Spyware that pretends to be an antivirus

By Dmitry Kalinin

Published: 2025-08-06 · Archived: 2026-04-05 21:22:06 UTC

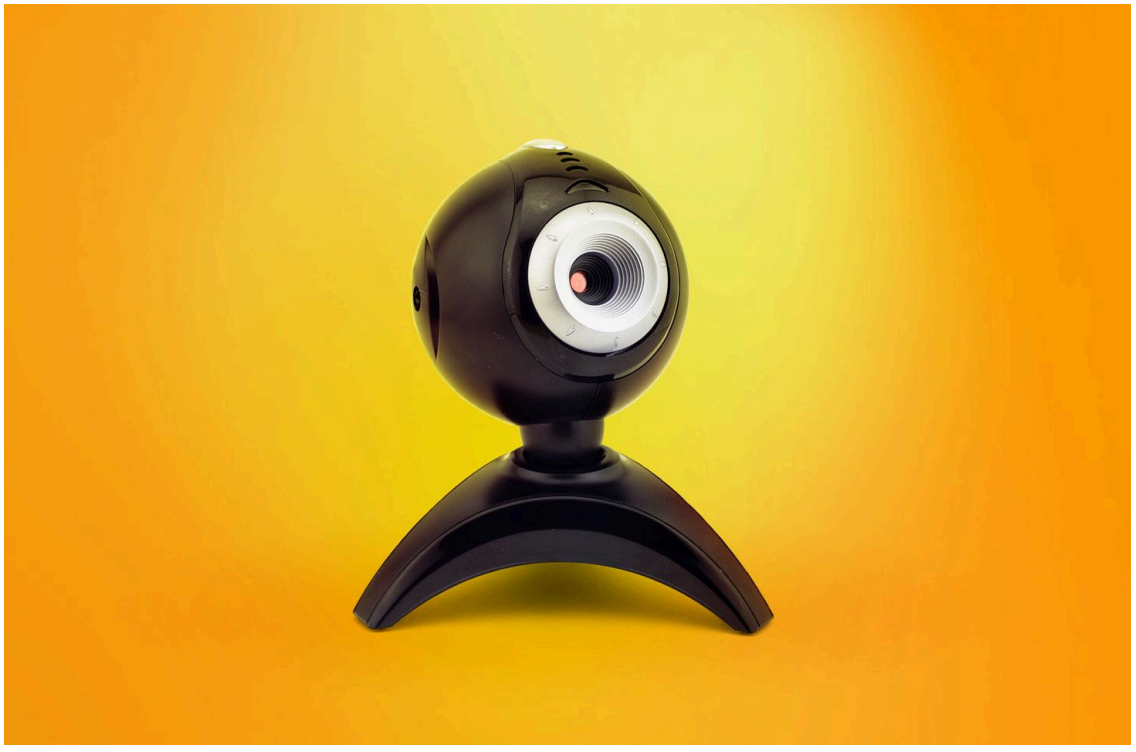
- Android

Android smartphone owners who use messengers are at risk.

- 

  Dmitry Kalinin

- August 6, 2025



In the pursuit of security, many folks are ready to install any app that promises reliable protection from malware and scammers. It's this fear that's skillfully used by the creators of new mobile spyware distributed through messengers under the guise of an antivirus. After installation, the fake antivirus imitates the work of a genuine one — scanning the device, and even giving a frightening number of "threats found". Of course no real threats are detected, while what it really does is simply spy on the owner of the infected smartphone.

How the new malware works and how to protect yourself from it is what we'll be telling you about today.

How the spyware gets into your phone

We've discovered a new malware campaign targeting Android users. It's been active since at least the end of February 2025. The spy gets into smartphones through messengers, not only under the guise of an antivirus, but also banking protection tools. It can look like this, for example:

- **"Hi, install this program here."** A potential victim can receive a message suggesting installing software from either a stranger, or a hacked account of a person in their contacts (which is how, for example, Telegram accounts are hijacked.
- **"Download the app in our channel".** New channels appear in Telegram every second, so it's quite possible that some of them may distribute malware under the guise of legitimate software.

After installation, the fake security app shows the number of detected threats on the device in order to force the user to provide all possible permissions supposedly to save the smartphone. In this way, the victim gives the app access to all personal data without realizing the real motives of the fake AV.

What LunaSpy can do

The capabilities of the spyware are constantly increasing. For example, the latest version we found has the ability to steal passwords from both browsers and messengers. This, by the way, is another reason to start using password managers if you haven't already done so. What else can LunaSpy do?

- Record audio and video from the microphone and camera.
- Read texts, the call log, and contact list.
- Run arbitrary shell commands.
- Track geolocation.
- Record the screen.

We also discovered malicious code responsible for stealing photos from the gallery, but it's not being used yet. All the information collected by the malware is sent to the attackers via command-and-control servers. What's surprising is that there are around 150 different domains and IP addresses associated with this spyware — all of them command-and-control servers.

How to protect your devices

We assume that this spyware is used by attackers as an auxiliary tool, so for now it doesn't compete with big players like SparkCat. Nevertheless, you should protect yourself from LunaSpy as best you can as you do with other threats.

- **Don't download apps from third-party sources.** We usually talk about the possible presence of malware in official stores and catalogs; however, this is a special case, so we'll supplement the standard recommendation with: never download APK files from messengers — even if they were sent to you by close friends. Better yet, disable the ability to install unknown applications.

- **Check which apps you give permission to.** Be wary if an antivirus or any other security solution requires too many permissions with no clear reason why it needs them.
- **Use Kaspersky for Android** to detect spyware and other malware in a timely manner.
- **Trust trusted developers.** If someone offers you to download a *"new super-accurate and secure"* antivirus that the internet seems to know nothing about, be very wary *and* opt for a proven solution.

> A bit more on spyware:
>
> - FinSpy: the ultimate spying tool
> - Spyware messengers on Google Play
> - Staying safe from Pegasus, Chrysaor and other APT mobile malware
> - LianSpy: new mobile spyware for Android
> - How to keep spies off your phone — in real life, not the movies

---

Source: https://www.kaspersky.com/blog/disguised-spy-for-android/54051/