It Could Be Harmful!

Spyware Installation Through Social Engineering Attacks in Italy

It Could Be Harmful! Spyware Installation Through Social Engineering Attacks in Italy

Original text in Italian

Potrebbe essere dannoso!

2025

brughiere.noblogs.org/post/2025/11/12/potrebbe-essere-dannoso

Translation and layout

No Trace Project

notrace.how/resources/#could-be-harmful

Note from the No Trace Project:

This text describes how Italian comrades were tricked into installing spyware on their phones through social engineering attacks involving fake technicians who claimed to work for mobile network operators. Based on our experience and the experience of other comrades, we believe the attacks described in this text:

- Were likely carried out by State actors, possibly local police forces or prosecutors.
- Very likely required the collaboration of mobile network operators, who would have remotely disconnected and then reconnected the line to make it seem as if the phone had connection issues, allowing the fake technician to credibly intervene.

This text is a reminder that the surveillance capabilities of repressive authorities are constrained by their resources, financial and otherwise. While intelligence agencies may have access to more sophisticated spyware that can be installed more reliably and stealthily, local police forces and prosecutors may have to rely on less sophisticated techniques.

This shows the importance of spreading awareness of social engineering attacks within our movements, so that other comrades do not fall for these tricks.

We have recently seen an increase in the use of spyware against politicians, companies, lawyers, and activists. We have reason to believe that similar software are being used in investigations against individuals associated with certain areas of the movement. Prosecutors are probably finding it easier to rely on external start-ups for software that, while not as sophisticated or expensive as Pegasus, Predator, Graphite, or Triangulation, still perform their snitching function of collecting information about their victims without their consent.

Recently, some comrades have experienced intrusions in their mobile devices. First, they suddenly and inexplicably lost Internet and telephone connectivity. At the same time, all outgoing calls were diverted to the mobile network operator's switchboard (or the operator was contacted for explanations). After a call with an assistant, who was either unaware or uninformed and reported probable connection issues, they were immediately contacted again by a different number claiming to be a technician from the network operator.

The technician signaled that the phone had not been updated. He then precisely and politely dictated all the steps to restore functionality, which included installing an app with the name and logo of the operator associated with the SIM card.

The installation steps show how intrusive the app is:

- First, Play Protect app analysis on the Play Store is disabled. This feature protects the device from potentially harmful apps and ensures that installed apps are safe and reliable.
- An SMS arrives with a link to a page that resembles the phone operator's website. You are then prompted to click a button that resembles the Google Play button to download the “update.”
- The file is downloaded, bypassing the Play Store, and opened from Downloads, despite warnings from the phone that are

all skipped. To complete the installation, you must change the phone settings to allow installation of apps from this source.

- The phone settings are then changed to grant access to the mobile network, allowing the phone operator's data connection to be used to send and receive information.
- Consent is given for the app to run in the background and start automatically when the phone is turned on. This allows it to continue to function even when it is not active on the screen.
- All permissions are granted to the app, including access to the camera, microphone, contacts, phone, SMS, calendar, location, files, etc.
- Battery optimization for the app is disabled in the settings so that its activity is not limited to save energy.
- The phone is restarted, and upon restarting, the green microphone symbol immediately appeared in the upper left corner. Then, it turned into a green dot and finally disappeared.
- To top it all off, an SMS arrived asking, "Are you satisfied with my service?"

After this process, it is plausible that all the phone's data (files, media, contacts, messages, etc.) was being forwarded to a remote server by the spyware app previously installed through deception, turning the phone into a real bug able to activate the microphone, camera, and geolocation, as well as to take screenshots.

Considering the identity of those affected and the capabilities of the attackers, it is not difficult to imagine the origin of this attack. Therefore, we urge you to pay attention to incidents of this kind, even though not all malware requires active installation by the phone owner, as was the case here.

This text describes how Italian comrades were tricked into installing spyware on their phones through social engineering attacks involving fake technicians who claimed to work for mobile network operators.

No Trace Project / No trace, no case. A collection of tools to help anarchists and other rebels **understand** the capabilities of their enemies, **undermine** surveillance efforts, and ultimately **act** without getting caught.