How to avoid turning your smartphone into a spyware zoo

By Leonid Grustniy

Published: 2018-05-14 · Archived: 2026-04-05 18:47:28 UTC

- Android

Do you follow the news? The news may also be following you. ZooPark spyware targets those partial to politics.

- May 14, 2018

Sometimes even a completely innocent-looking site with a good reputation can be harmful — criminals may find and exploit a vulnerability. For example, they can use the site for drive-by attacks, causing each visitor to download a file automatically (and unwittingly) as soon as they get to the site. For example, Android users interested in current events in the Middle East are at risk of getting a whole menagerie — ZooPark spyware — on their phones.

Kaspersky Lab has been following this malware since 2015, and it has learned a plethora of new tricks since then. The current, fourth version of this Trojan can steal almost any information from your smartphone, from contacts to call logs and info you enter by keyboard. Here is the list of data that ZooPark can collect and send to its owners:

- Contacts
- User account information

- Call history
- Call audio recordings
- Text messages
- Bookmarks and browser history
- Browser search history
- Device location
- Device information
- Information on installed apps
- Any files from the memory card
- Documents stored on the device
- Information entered using the on-screen keyboard
- Clipboard information
- App-stored data (for example, data from messaging apps such as Telegram, WhatsApp, and imo, or the Chrome browser)

In addition, ZooPark can take screenshots and photos, and record videos on command. For example, it can take a picture of the phone's owner from the front camera and send it to its command center.

Malware beasts and where to find them

ZooPark Trojan spyware is used for targeted attacks — in other words, it's not sent out randomly to ensnare just anyone; it aims for a specific audience. As we said, the criminals behind ZooPark target those who are interested in specific topics — in this case, Middle Eastern politics.

ZooPark spreads by two main channels: drive-by downloads and Telegram. In the latter case, for example, criminals offered an app on the Telegram channel for voting on the Kurdistan independence referendum.

Malefactors also hack some Web resources that are popular in certain countries or circles, making visitors automatically download an infected app that looks like something useful — for example, an official app for the news resource. Finally, in some cases, the malware pretends to be an "all-in-one" messenger. For more details about the technical aspects of ZooPark, see the post on Securelist.

Don't buy a zoo

To avoid falling prey to this kind of dangerous spyware, remember a few important rules that will help make your virtual life safer:

- Download apps only from trusted sources. Even better, use your device settings to disable the ability to install programs from third-party stores.
- Update your operating system and important apps as updates become available. Many safety issues can be solved by installing updated versions of software.
- Use mobile antivirus software to block suspicious links and apps. Kaspersky Internet Security for Android detects and neutralizes ZooPark.

Tips

Source: https://www.kaspersky.com/blog/zoopark-attacks/22389/