# Newly found Android malware records audio, tracks your location

bleepingcomputer.com/news/security/newly-found-android-malware-records-audio-tracks-your-location/

Bill Toulas

By
Bill Toulas

- April 1, 2022
- 03:41 PM
- 0

A previously unknown Android malware uses the same shared-hosting infrastructure previously seen used by the Russian APT group known as Turla, though attribution to the hacking group not possible.

Turla is a Russian state-supported hacking group known for using custom malware to target European and American systems, primarily for espionage.

The threat actors have recently been linked to the Sunburst backdoor used in the SolarWinds supply-chain attack in December 2020.

## New Android spyware discovered

Researchers from Lab52 identified a malicious APK [VirusTotal] named “Process Manager” that acts as Android spyware, uploading information to the threat actors.

While it is not clear how the spyware is distributed, once installed, Process Manager attempts to hide on an Android device using a gear-shaped icon, pretending to be a system component.

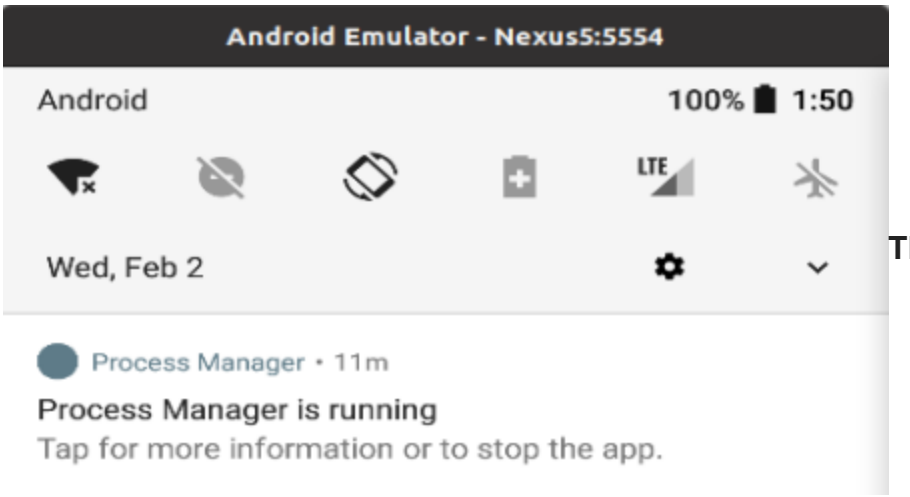
Upon its first launch, the app prompts the user to allow it to use the following 18 permissions:

- Access coarse location
- Access fine location
- Access network state
- Access WiFi state
- Camera
- Foreground service
- Internet
- Modify audio settings
- Read call log
- Read contacts
- Read external storage
- Write external storage
- Read phone state
- Read SMS
- Receive boot completed
- Record audio
- Send SMS
- Wake log

These permissions are a serious risk to privacy as it allows the app to get a device's location, send and read texts, access storage, take pictures with the camera, and record audio.

It is unclear if the malware abuses the Android Accessibility service to grant itself permissions or if it's tricking the user into approving a request.

After receiving the permissions, the spyware removes its icon and runs in the background with only a permanent notification indicating its presence.




**The permanent notification posing as a system service** *(Lab52)*

This aspect is quite strange for spyware that should usually strive to remain hidden from the victim, especially if this is the work of a sophisticated APT (advanced persistent threat) group.

The information collected by the device, including lists, logs, SMS, recordings, and event notifications, are sent in JSON format to the command and control server at 82.146.35[.]240, which is located in Russia.

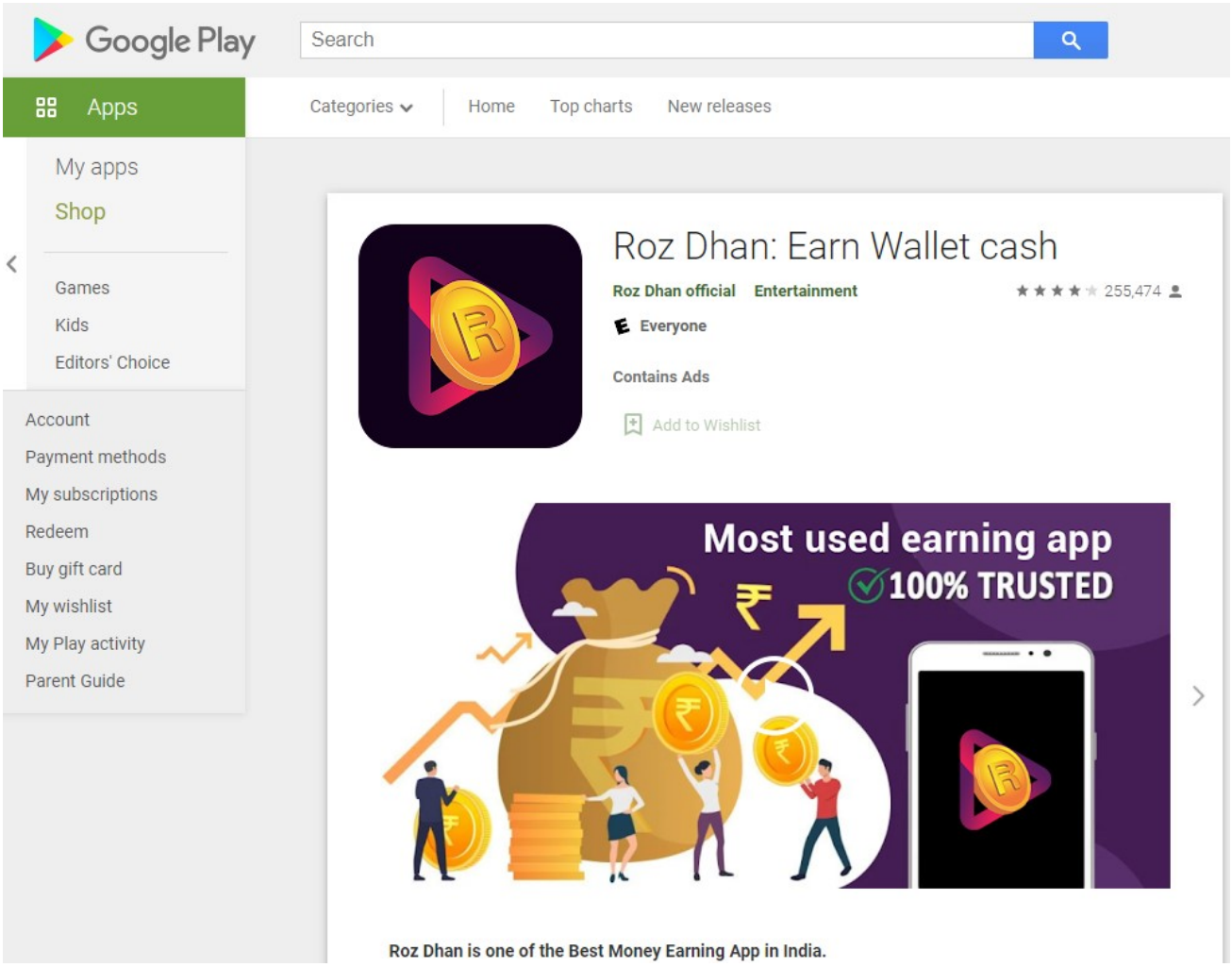

**Establishing C2 connection to send the stolen data** *(Lab52)*

The method of distribution for the APK is unknown, but if it is Turla, they commonly use social engineering, phishing, watering hole attacks, etc., so it could be anything.

## Strange case of abuse for profit

While researching the app, the Lab52 team also found that it downloads additional payloads to the device and found a case of an app fetched directly from the Play Store.

The app is named "Roz Dhan: Earn Wallet cash," and it's a popular (10,000,000 downloads) app featuring a money-generating referral system.




**Abused application on the Play Store**

The spyware reportedly downloads the APK via the app's referral system, likely to earn a commission, which is somewhat strange given that the particular actor is focused on cyber espionage.

This, in addition to the seemingly unsophisticated implementation of the Android spyware, leads us to believe that the C2 analyzed by Lab52 may be part of a shared infrastructure.

State actors are known for following this tactic, even if rarely, as it helps them obscure their trace and confuse analysts.

However, due to the low sophistication of the malware's threat capabilities and the use of referral-based monetization, the researchers do not believe this to be the work of a nation-state actor, like Turla.

"So in this report, we want to share our analysis on the capabilities of this piece of malware, although the attribution to Turla does not seem possible given its threat capabilities," explain the Lab52 researchers.

## Keep malware out

Users of Android devices are advised to review the app permissions they have granted, which should be fairly easy on versions from Android 10 and later, and revoke those that appear overly risky.

Also, starting from Android 12, the OS pushes indications when the camera or microphone is active, so if these appear orphaned, spyware is hiding in your device.

These tools are particularly dangerous when nesting inside IoTs that run older Android versions, generating money for their remote operators for prolonged periods without anyone realizing the compromise.

*Update 4/3/22: Article and title updated to show more clearly that the link with Turla APT is based on weak evidence.*

## Related Articles:

FluBot Android malware targets Finland in new SMS campaigns

Bearded Barbie hackers catfish high ranking Israeli officials

New ChromeLoader malware surge threatens browsers worldwide

New ERMAC 2.0 Android malware steals accounts, wallets from 467 apps

Popular Python and PHP libraries hijacked to steal AWS keys

- Eavesdrop
- Location
- Malware
- SMS
- Spyware
- Turla

Bill Toulas

Bill Toulas is a technology writer and infosec news reporter with over a decade of experience working on various online publications. An open source advocate and Linux enthusiast, is currently finding pleasure in following hacks, malware campaigns, and data breach incidents, as well as by exploring the intricate ways through which tech is swiftly transforming our lives.

- Previous Article
- Next Article

## You may also like: