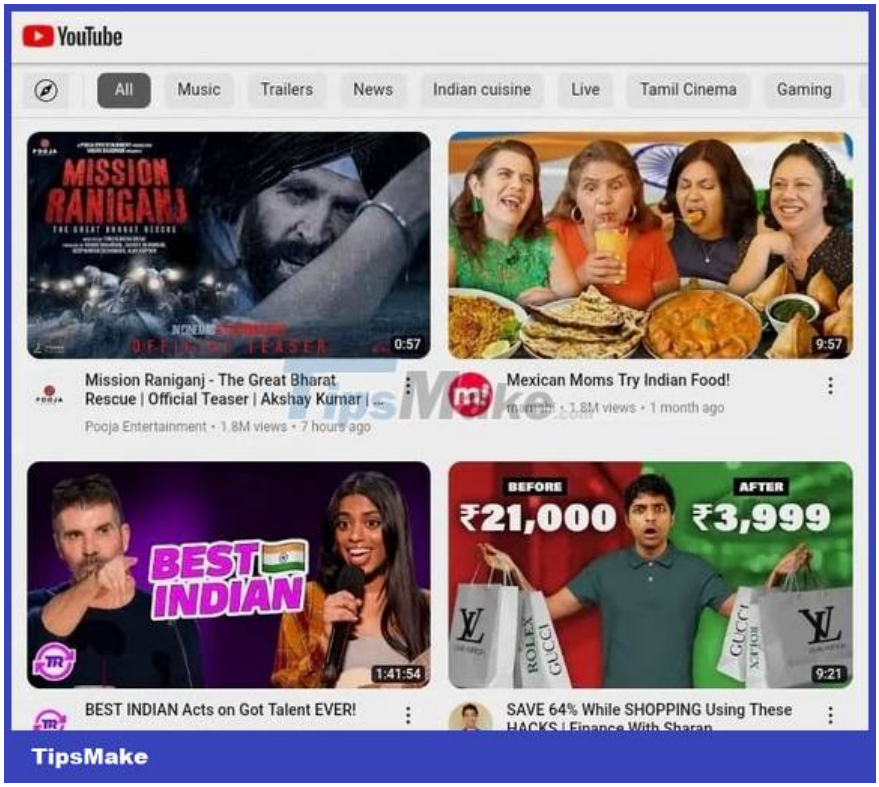
Detected 3 fake YouTube applications that secretly record and steal user information

Recently, researchers at SentinelLabs discovered 3 malicious applications impersonating YouTube designed to secretly record consumers, collecting an incredible amount of data.

Playing an important role in distributing these 3 fake YouTube applications is a cybercriminal group called Transparent Tribe (APT36).

Two of these malicious apps are called YouTube and the third is named Piya Sharma. 3 fake YouTube applications were distributed by Transparent Tribe (APT36) on social networking platforms and fake websites.



After the victim installs, the application will request permission to access the microphone, view and send SMS messages.

Basically, inside the 3 fake YouTube apps is CapraRAT malware, designed to steal personal information, GPS data, record audio, call logs, text messages, capture Screenshots, secret filming and system intervention.

After collecting stolen personal information, crooks will use it to carry out other fraudulent campaigns or resell it to third parties.

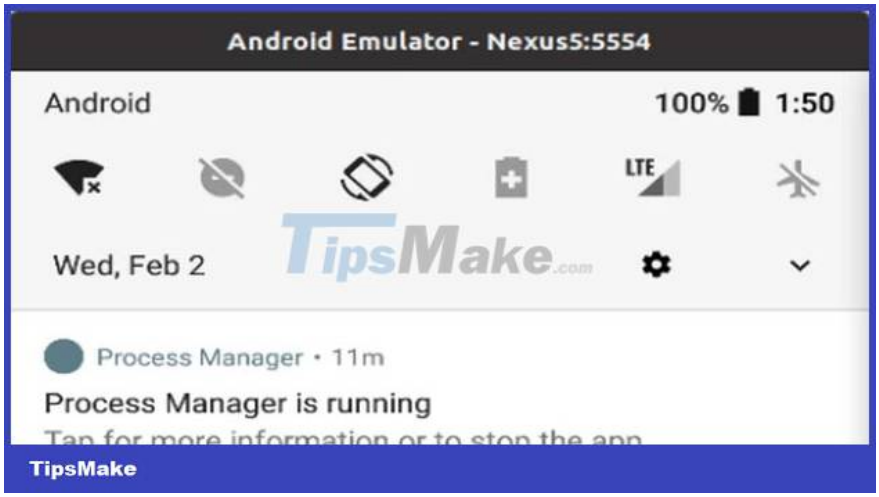
SentinelLabs recommends that users only download applications from trusted sources such as the Google Play store and carefully read the permissions requested by the application, to avoid becoming targets of fake applications. In addition, if you feel the application's requirements are unreasonable, stop installing immediately.

This is a malicious application that eavesdrops on users, please check your phone and remove it immediately

Researchers at Lab52 have discovered that Process Manager malware has the ability to record audio and track users' locations.

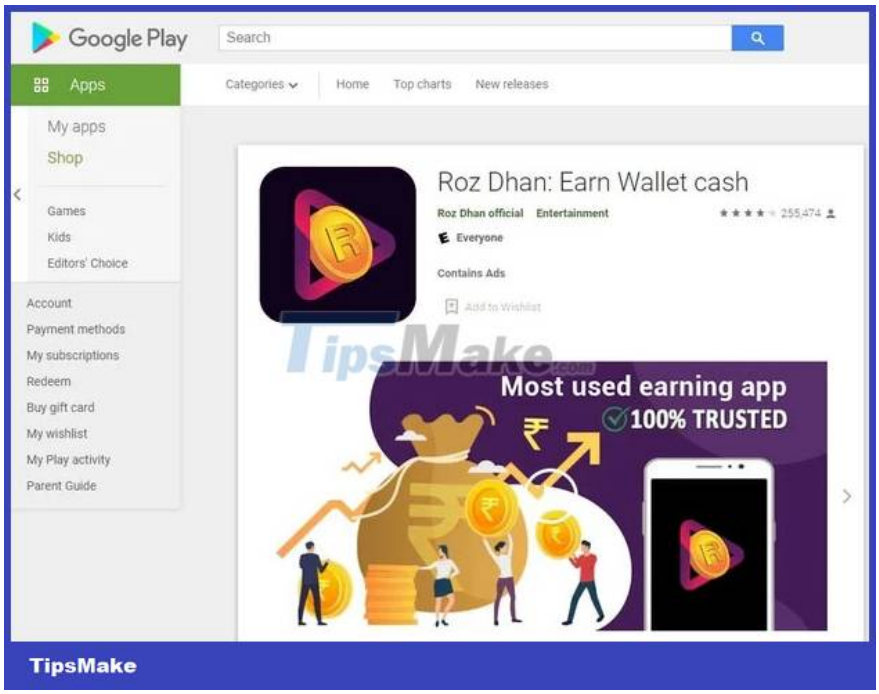
This application is hidden inside some applications on Google Play. Once installed, it will try to hide on the victim's device with a gear icon, making users mistakenly think that this is part of the system.

According to Lab52, this malicious code was previously linked to Turla, a famous hacker group believed to be supported by the Russian state. This group specializes in using custom malware to target European and American systems, mainly for espionage activities.



On first launch, this malicious application will request access to location, network status, camera, contacts, external memory, call logs, Foreground service, messages, recordings, etc. . to collect device location, send and read text, access memory, take photos/videos with the camera, and record audio.

After being granted the above permissions, this spyware will remove the icon from the screen and run silently in the background, making it very difficult for users to detect.



If you have accidentally installed it, please immediately remove this application by going to Settings -> Apps -> Manage apps, find the malicious application name - > press Uninstall.

You finished reading the article "**Detected 3 fake YouTube applications that secretly record and steal user information**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.