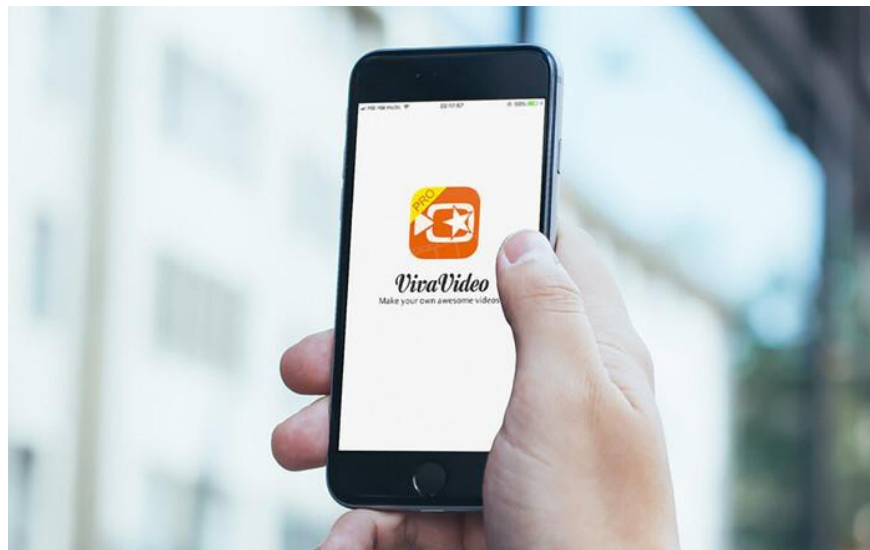


The famous VivaVideo editing app you need to remove right from your phone

According to a recently published report by Secure-D on Forbes, the VivaVideo app had a sneaky trick to generate illegal revenue.

A recently published report by Secure-D states that this security research firm has prevented about 20 million suspicious transactions on mobile devices, all derived from the VivaVideo app. for Android platforms.

The blocked transactions came from 19 countries, with the most being Brazil accounting for 11.5 million transactions, followed by Indonesia, Egypt, Thailand.... with a value of more than 27 million USD.

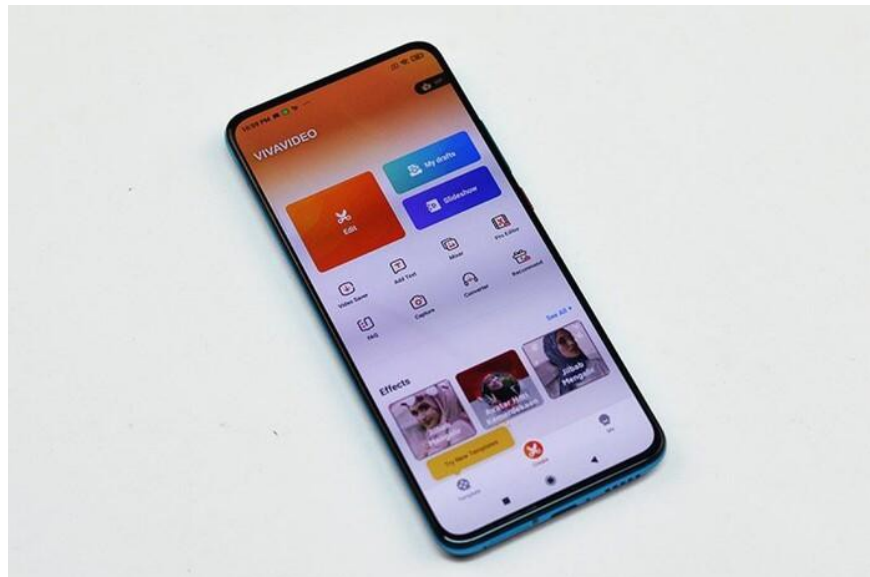


Secure-D experts have begun to question VivaVideo, when the application requires too many permissions when installed on a smartphone, including: access to the user's location, running in the background on the device. and many other system permissions... These are all unnecessary permissions with a regular video editing application.

Learn more about VivaVideo, Secure-D also discovered that this application uses 'tricks' to 'pickpocket' users without their knowledge.



Specifically, VivaVideo will allow users to download and use for free. However, during use, VivaVideo self-registers for paid services without the knowledge of the user, and cheats advertising to help bring revenue for VivaVideo's developers (according to data securely- D collected from early 2019 to present).



The app uses sophisticated tricks compared to other applications, making it difficult to track, the team said. When it detects that a monitoring application is available, it will stop suspicious behavior.

According to Upstream Systems, older versions of VivaVideo have been found to use Batmobi, the advertising platform's SDK, which has been banned by Google since 2018 for abuse of access to fraudulent ads.



Geoffrey Cleave, the head of Secure-D, said this behavior appeared on older versions of VivaVideo, with new versions, not yet able to conclude the application will behave similar or not.

At the same time, it is not known whether VivaVideo's illegal revenue-generating behavior has stopped, or that the VivaVideo developers have used another tactic to bypass Secure-D's tracking algorithm.

Notably, this is not the first time VivaVideo has been warned by security experts about suspicious activity.

In June, experts from VPNPro, a cybersecurity company, discovered that the VivaVideo application showed signs of tracking users when asking to override the permissions.



VPNPro experts recommend that users remove VivaVideo, as well as the applications developed by QuVideo from their device to avoid unnecessary risks.

In 2017, VivaVideo was also listed as spyware / malware by the Indian government.

On the Google Play Store, this app has more than 100 million downloads, 12 million reviews with an average star rating of 4.2. The app developer is QuVideo Inc., based in Hangzhou (China).

You finished reading the article "**The famous VivaVideo editing app you need to remove right from your phone**" 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.
