

# Android et ces 12 applications du Play Store sont infestées par un logiciel espion, désinstallez-les vite

Aymeric Geoffre-Rouland :

**Attention ! Des applications malveillantes se cachent sur Google Play dans des applications de messagerie, volant des données personnelles, interceptant des messages, et enregistrant même des appels.**

**Soyez prudent en téléchargeant des applications obscures.**



Le spyware VajraSpy se diffuse sur le PlayStore (image générée par IA)

- Des applications Android infectées par le malware VajraSpy ont été trouvées sur Google Play.
- Elles volent les données personnelles, interceptent les communications.
- Certaines sont encore disponibles sur le Play Store.

Après [une large campagne de malwares découverte sur le Play Store](#), des chercheurs d'ESET ont récemment découvert une nouvelle, impliquant **12 applications Android malveillantes** contenant le RAT VajraSpy.

Ces applications, déguisées en outils de messagerie ou d'actualités, ont été téléchargées plus de 1 400 fois, principalement depuis Google Play, mais aussi sur des boutiques tierces.

## Un logiciel espion se cache sous 12 applications Android : VajraSpy

Une fois installé, **VajraSpy vole des données personnelles** telles que les contacts et les messages, intercepte les communications cryptées d'applications comme WhatsApp et Signal, enregistre les appels téléphoniques et active même la caméra pour une surveillance subreptice.

Sa nature modulaire lui permet de s'adapter, l'étendue de ses capacités d'espionnage étant déterminée par les permissions accordées.

L'analyse d'ESET indique que la plupart des victimes se trouvent au Pakistan et en Inde, probablement attirées par des arnaques sentimentales pour installer les fausses applications de messagerie.

Une tactique très courante, utilisée par les cybercriminels pour **infiltrer les appareils**. Voici les applications Android infectées par VajraSpy.

### Disponibles sur Google Play (mais supprimées depuis) :

- Rifaqat رفاقت (actualités)
- Privee Talk (messagerie)
- MeetMe (messagerie)
- Let's Chat (messagerie)
- Quick Chat (messagerie)
- Chit Chat (messagerie)

### Disponibles uniquement en dehors de Google Play (bogus messaging apps) :

- Hello Chat
- YohooTalk
- TikTalk
- Nidus
- GlowChat
- Wave Chat

Bien que Google Play mette en place des **politiques plus strictes** pour dissuader les logiciels malveillants, les cybercriminels eux, continuent de trouver des **moyens de les contourner**.

Cet incident fait suite à des campagnes antérieures comme [l'adware d'octobre, qui a atteint 2 millions d'installations](#), et [le malware SpyLoan, téléchargé 12 millions de fois en 2023](#).

Un porte-parole de Google a réaffirmé son engagement à répondre aux problèmes de sécurité et de confidentialité et à prendre des mesures contre les violations des politiques. ESET et les experts en sécurité conseillent aux personnes qui utilisent Android **d'être prudents lorsqu'ils téléchargent des applications**, en particulier celles provenant de sources inconnues ou recommandées par des étrangers.

Tenez-vous-en **aux boutiques d'applications réputées**, examinez attentivement les permissions des applications avant de les accorder et restez vigilants face aux activités suspectes sur votre appareil.

D'autant plus que [ce n'est pas le premier logiciel espion à s'inviter sur Android](#).

### N'oubliez pas :

- Méfiez-vous des recommandations d'applications non sollicitées.

- Téléchargez des applications uniquement à partir de sources fiables.
- Faites attention aux permissions des applications avant de les accorder.
- Restez informé des menaces et des meilleures pratiques en matière de cybersécurité.

*Recherche et mise en page par:*

*Michel Cloutier*

*CIVBDL*

*20240205*

*"C'est ensemble qu'on avance"*