SonicSpy contamine plusieurs milliers d'apps Android

Des chercheurs de l'éditeur de solutions de sécurité mobile, Lookout, ont découvert au moins 3 applications Android sur le Play Store de Google contenant un logiciel espion, nommé SonicSpy, probablement créé par un développeur irakien

Les apps concernées sont Soniac, Hulk Messenger et Troy Chat. La première est une version modifiée de l'application de messagerie sécurisée Telegram. Seule Soniac était active quand les chercheurs ont détecté le logiciel espion. Des traces de code malveillant ont été trouvées dans deux autres applications. Mais elles ont été depuis retirées du carrousel applicatif de Google, probablement par le développeur lui-même.

Dans le détail, SonicSpy comprend 73 actions d'espionnage dont l'enregistrement discret des appels vocaux, la prise de photo à l'insu de l'utilisateur, l'envoi de SMS, récupérer des historiques d'appels, envoyer des données à un point d'accès WiFi, etc…

Infection au-delà, similitude en deçà

Le problème est que SonicSpy ne s'est pas contenté de se cantonner au Play Store de Google, mais a contaminé plusieurs milliers d'applications sur des magasins alternatifs. Les chercheurs ont fait une première estimation pour recenser plus de 4000 apps infectées par SonicSpy.

Dans leur analyse, les chercheurs de Lookout estiment que le développeur irakien est à l'origine d'un logiciel similaire SpyNote qui a sévit en 2016 et a été découvert par les spécialistes de Palo Alto Networks. Le *modus operandi* est proche en utilisant des services DNS dynamiques et s'attaquant au port non standard 2222.

A lire aussi :

SpyDealer, le malware qui espionne de fond en comble des smartphones Android

FalseGuide terrorise déjà 2 millions de smartphones Android