

# Un malware Android imite l'application Google Play dans le store

Un **nouveau malware** dont l'icône imite celle de l'application légitime **Google Play Store** a été découvert dans la logithèque officielle de Google par l'éditeur américain de solutions de sécurité **FireEye**. Ce programme malveillant utilise un serveur DNS dynamique et le protocole SSL (Gmail).

## Certificats et identifiants bancaires

Il existe une relation étroite entre **l'application principale** « **googl app stoy** », l'application jointe et **le programme malveillant** « **com.sdwiurse** » lui-même. Il peut agir en arrière-plan du terminal Android concerné pour recueillir des SMS, certificats et identifiants bancaires.

Lorsque le smartphone Android est infecté, **la fonction** « **désinstaller** » **est désactivée** et le programme continue de fonctionner à l'insu de l'utilisateur, explique FireEye dans un billet technique daté du 18 juin. Sur l'interface apparaissent des alertes en coréen (traduites en français cela peut donner « erreur programme » ou « c'est supprimé ») pour mieux tromper l'utilisateur. Les services peuvent être **arrêtés manuellement**, mais seront **relancés au redémarrage** du smartphone.

Pour limiter les détections lors du téléchargement de l'application, le malware utilise le chiffrement. Résultat, seuls **3 éditeurs d'antivirus sur 51** étaient parvenus à le détecter en fin de semaine dernière. D'après FireEye, une majorité de vendeurs utilise uniquement des algorithmes basés

sur les signatures pour détecter les malwares, et ne parviennent donc pas à détecter le contenu malveillant dissimulé dans des applications qui semblent basiques.

crédit photo © FireEye

---

**Lire aussi**

[Des malwares pré-installés sur des smartphones Android chinois](#)

[Le nombre de malwares Android a explosé en 2013](#)