Attention, Cheval de troie dans une Application sur Google Play découverte par Eset

Attention, Cheval de troie dans une Application sur Google Play découverte par Eset

Avant même la sortie sous Android de Prisma, une application populaire de retouche photos, Google Play Store s'était retrouvé inondé de fausses applications.

Les chercheurs d'ESET ont découvert de fausses applications imitant Prisma, dont plusieurs Chevaux de Troie dangereux. Dès l'avertissement d'ESET, le service sécurité de Google Play a retiré toutes les fausses applications du store officiel d'Android. Ces dernières auront tout de même atteint plus d'1,5 millions de téléchargements.
Prisma est un éditeur de photos unique publié par les laboratoires de Prisma. D'abord développé pour iOS, cette application a remporté d'excellents résultats de la part des utilisateurs d'iTunes et de l'App Store d'Apple. Les utilisateurs d'Android étaient à leurs tours impatients de la découvrir sur le Google Play (disponible depuis le 24 juillet 2016).
« La plupart des fausses applications de Prisma disponibles sur Google Play ne disposent pas d'une fonction retouche photo. A l'inverse, elles affichent uniquement des annonces, avertissements ou de faux sondages pour tromper l'utilisateur qui fournit des informations personnelles le concernant ; ou encore pour le faire souscrire à de faux services type SMS onéreux », commente Lukáš Štefanko, Malware Researcher chez ESET.
La plus dangereuse des fausses applications imitant Prisma et trouvée dans le Google Play est un Cheval de Troie téléchargeur détecté par ESET comme Android/TrojanDownloader.Agent.GY. Des informations sur les périphériques sont envoyées au serveur C&C, ce qui lui permet de télécharger sur demande des modules supplémentaires et de les exécuter afin de voler des données sensibles telles que le numéro de téléphone, l'opérateur, le pays, la langue etc.
A cause de ses capacités de téléchargement, la famille des malwares type Android/TrojanDownloader.-Agent.GY pose de sérieux risques pour les plus de 10.000 utilisateurs Android qui ont installé cette application dangereuse avant d'être retiré du Google Play Store.

Pour se protéger, Denis JACOPINI recommande l'application suivante :

Article original de Eset

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article