

### **G-Data : Une application Android malveillante reste au Google-Market**

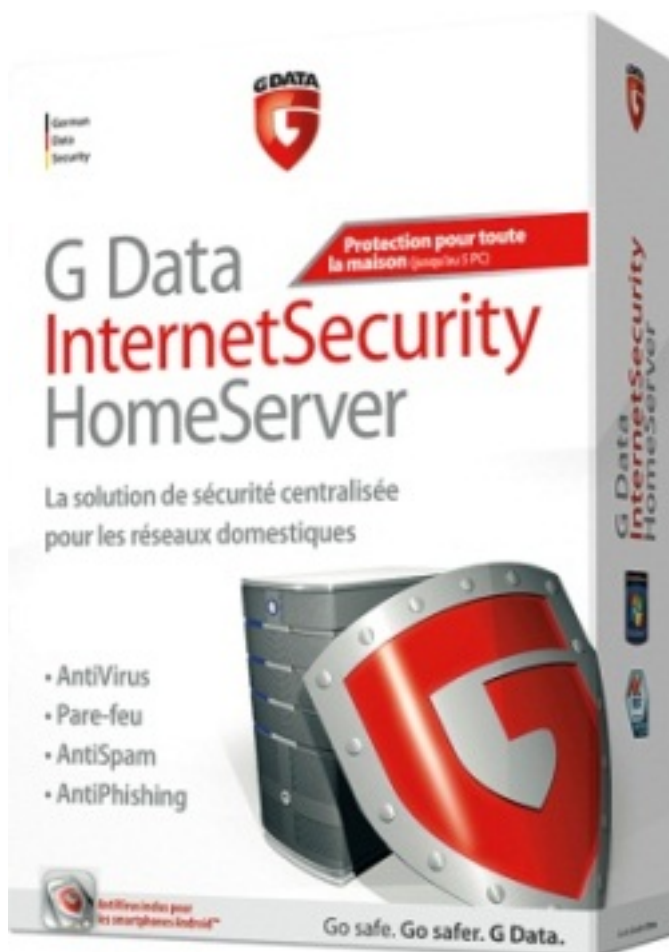
S curit 

Post  par : JerryG

Publi e le : 14/2/2012 11:00:00

**G-Data** qui scrute le Net et nos appareils communicants vient de faire une annonce assez  trange mais au combien salutaire pour les nomades. **Une application Android** est  t e du Google Market, car elle est consid r e comme **malveillante mais est ensuite de retour**. La fonctionnalit  dangereuse est rest e. La principale diff rence est le CLUF (Contrat de Licence Utilisateur Final). L' diteur de solutions antivirales s'interroge : "**Pr venir l'utilisateur est-il suffisant pour changer la donne ?**"

**Un logiciel est consid r  comme un malware** lorsque son but est, par exemple, de nuire   l'appareil ou de voler des informations, ce qui pourrait entra ner le vol d'identit  ou de fraude avec des p nalit s financi res sans le consentement de l'utilisateur. Mais il n'est pas toujours facile de trier le bon grain de l'ivraie. Le nombre d'applications qui diffament ou se moquent de l'utilisateur prennent une part croissante dans les menaces sur mobile. La difficult  de tracer une ligne claire entre un logiciel malveillant ou un  gitime est particuli rement difficile si la simple mention du comportement suppos  malveillant dans le contrat de licence ou le CLUF semble confirmer son droit d' tre publi  et de rester dans le Google Market. Jetons un coup d'oeil   une affaire en cours.



 tape 1: SndApps.A

Le malware en question, Android.Trojan.SndApps.A a été découvert le 4 juillet 2011 par Xuxian Jiang, alors professeur assistant au NCSU. Il s'adresse aux appareils mobiles Android et était disponible sur le Google Market. Une fois installé par l'utilisateur, le code malveillant ajoute des services afin d'être capable de déclencher certains processus malveillants au démarrage du système. L'utilisateur ne dispose d'aucune influence sur ces services.

Les applications porteuses de ce code sont très simples. L'application affiche juste une image d'avertisseur sonore. Ainsi, quand on le touche, joue le son correspondant. Les autres applications comme coussin-pâteur, antimoustique, etc. fonctionnent de la même façon.

Chaque application installée tente de faire installer les applications similaires du même développeur à l'utilisateur. L'autre comportement encore plus suspect des applications de ce développeur est le vol de données personnelles telles que les contacts, le numéro de téléphone et le numéro IMEI du smartphone. Ces données sont transmises, en clair, au serveur de Typ3-Studios, ce qui ajoute à l'impression qu'il s'agit bien d'un logiciel malveillant. Après la découverte de Jiang, les équipes de sécurité du Google Market ont retiré ces applications du marché.

### Étape 2 : Deuxième tentative... et succès

Fin août 2011, Typ3-Studios a publié une nouvelle série d'applications, très semblable à celles décrites précédemment. Seule la couleur de fond des icônes a été changée. Elles montrent le même comportement que les versions potentiellement malveillantes, mais n'ont pas encore été retirées du Market de Google, (statut 13/02/2012).

### Pourquoi ces applications n'ont-elles pas été à nouveau retirées?

Dans la version Android.Riskware.SndApps.B, la seule indication d'un changement est le contrat de licence utilisateur final ajouté (en abrégé : CLUF). Son retour à l'existence est annoncé par un avis simple dans le «Quoi de neuf» de Google Market. Là, on peut lire : *"S'il vous plaît, lisez la nouvelle politique de confidentialité et les conditions d'utilisation dans le menu de l'application."* En outre, la permission d'insérer le service de publicité au démarrage du système a été ajoutée. L'interprétation de ce comportement comme malveillant semble maintenant entravée par le fait qu'il soit simplement mentionné - en particulier lorsque l'utilisateur approuve cette situation.

Mais, le CLUF de toutes les applications mentionnées n'est visible que si l'utilisateur appuie sur la touche Menu du smartphone. L'utilisation des applications étant seulement de jouer un son par pression sur l'écran il est évident que la majorité des utilisateurs ne verront jamais ce contrat de licence - ils sont implicitement d'accord sur ce CLUF en utilisant l'application.



