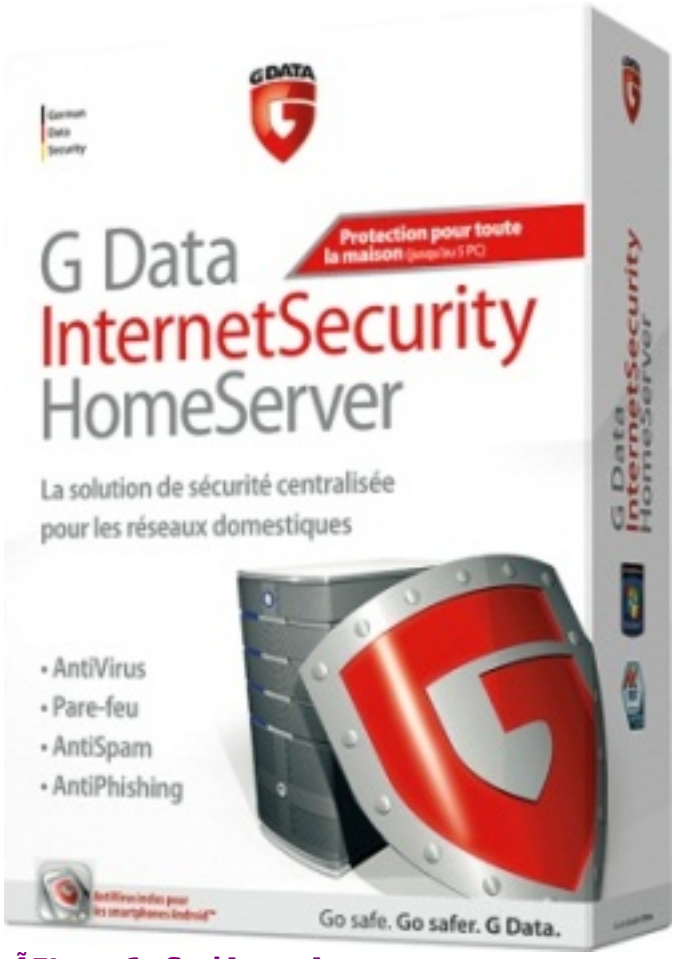
G-Data : Une application Android malveillante reste au Google-Market
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 14/2/2012 11:00:00

G-Data qui scrute le Net et nos appareils communicants vient de faire une annonce assez Ã©trange mais au combien salutaire pour les nomades. **Une application Android** est Ã´tÃ©e du Google Market, car elle est considÃ©rÃ©e comme **malveillante mais est ensuite de retour**. La fonctionnalitÃ© dangereuse est restÃ©e. La principale diffÃ©rence est le CLUF (Contrat de Licence Utilisateur Final). L'Ã©diteur de solutions antivirales s'interroge : " ***PrÃ©venir l'utilisateur est-il suffisant pour changer la donne ?***"

Un logiciel est considÃ©rÃ© comme un malware lorsque son but est, par exemple, de nuire Ã l'appareil ou de voler des informations, ce qui pourrait entraÃ®ner le vol d'identitÃ© ou de fraude avec des pÃ©nalitÃ©s financiÃ¨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 difficultÃ© de tracer une ligne claire entre un logiciel malveillant ou un lÃ©gitime est particuliÃ¨rement difficile si la simple mention du comportement supposÃ© malveillant dans le contrat de licence ou le CLUF semble confirmer son droit d'Ãªtre publiÃ© et de rester dans le Google Market. Jetons un coup d'oeil Ã une affaire en cours.



Ã tape 1: SndApps.A

Le malware en question, Android.Trojan.SndApps.A a Ã©tÃ© dÃ©couvert le 4 juillet 2011 par Xuxian Jiang, alors professeur assistant au NCSU. Il s'adresse aux appareils mobiles Android et Ã©tait disponible sur le Google Market. Une fois installÃ© par l'utilisateur, le code malveillant ajoute des services afin dâ□□Ãªtre capable de dÃ©marrer certains processus malveillants au dÃ©marrage du systÃ¨me. L'utilisateur ne dispose d'aucune influence sur ces services.

Les applications porteuses de ce code sont trÃ¨s simples. L'application affiche juste une image dâ□□avertisseur sonore Ã air qui, quand on le touche, joue le son correspondant. Les autres applications comme coussin-pÃ©teur, antimoustique, etc. fonctionnent de la mÃªme faÃ§on.

Chaque application installÃ©e tente de faire installer les applications similaires du mÃªme dÃ©veloppeur Ã lâ□□utilisateur. Lâ□□autre comportement encore plus suspect des applications de ce dÃ©veloppeur est le vol de donnÃ©es personnelles telles que les contacts, le numÃ©ro de tÃ©lÃ©phone et le numÃ©ro IMEI du smartphone. Ces donnÃ©es sont transmises, en clair, au serveur de Typ3-Studios, ce qui ajoute Ã l'impression quâ□□il s'agit bien dâ□□un logiciel malveillant. AprÃ¨s la dÃ©couverte de Jiang, les Ã©quipes de sÃ©curitÃ© du Google Market ont retirÃ© ces applications du marchÃ©.

Ã□tape 2 : DeuxiÃ¨me tentative... et succÃ¨s

Fin aoÃ»t 2011, Typ3-Studios a publiÃ© une nouvelle sÃ©rie d'applications, trÃ¨s semblable Ã celles dÃ©crites prÃ©cÃ©demment. Seule la couleur de fond des icÃ´nes a Ã©tÃ© changÃ©e. Elles montrent le mÃªme comportement que les versions potentiellement malveillantes, mais nâ□□ont pas encore Ã©tÃ© Ã´tÃ©es du Market de Google, (statut 13/02/2012).

Pourquoi ces applications nâ□□ont-elles pas Ã©tÃ© Ã nouveau retirÃ©es?

Dans la version Android.Riskware.SndApps.B, la seule indication d'un changement est le contrat de licence utilisateur final ajoutÃ©e (en abrÃ©gÃ©: CLUF). Son retour Ã l'existence est annoncÃ© par un avis simple dans le Â«Quoi de neufÂ» de Google Market. LÃ , on peut lire : "*S'il vous plaÃ®t, lisez la nouvelle politique de confidentialitÃ© et les conditions d'utilisation dans le menu de lâ□□application.*" En outre, la permission dâ□□insÃ©rer le service de publicitÃ© au dÃ©marrage du systÃ¨me a Ã©tÃ© ajoutÃ©e. Lâ□□interprÃ©tation de ce comportement comme malveillant semble maintenant entravÃ©e par le fait quâ□□il soit simplement mentionnÃ© - en particulier lorsque l'utilisateur approuve cette situation.

Mais, le CLUF de toutes les applications mentionnÃ©es n'est visible que si l'utilisateur appuie sur la touche Menu du smartphone. L'utilisation des applications Ã©tant seulement de jouer un son par pression sur lâ□□Ã©cran il est trÃ¨s Ã©vident que la majoritÃ© des utilisateurs ne verront jamais ce contrat de licence - ils sont implicitement d'accord sur ce CLUF en utilisant l'application.

Le dÃ©but du CLUF se lit comme suit: "*En utilisant cette application mobile (lâ□□Â« applicationÂ»), vous acceptez d'Ãªtre liÃ© par la prÃ©sente Politique de confidentialitÃ© et les conditions d'utilisation.*" La simple existence dâ□□un CLUF semble donc Ãªtre suffisant Ã Google pour laisser passer cette application- du moins, c'est ce que cette situation laisse penser.

Un autre point que les dÃ©veloppeurs ont dÃ» changer pour ne pas se faire expulser Ã nouveau est le chiffrement de la transmission des donnÃ©es utilisateur.

Les applications de Typ3-Studios sont aujourdâ□□hui disponibles sur le Google Market. Lâ□□application Â« coussin pÃ©teur Â» a, par exemple, Ã©tÃ© tÃ©lÃ©chargÃ©e plus de 10 000 fois.

Conclusion: Malware ou Riskware ?

La classification des logiciels devient de plus en plus difficile, surtout lorsque l'utilisateur accepte des autorisations douteuses.

La seule existence d'un CLUF ne devrait pas suffire Ã lÃ©gitimer un comportement suspect. Autre tendance douteuse : le CLUF n'est pas facilement accessible pour l'utilisateur. Une application qui inclut des autorisations et un CLUF qui sont au-delÃ du cas d'utilisation de l'application nâ□□est gÃ©nÃ©ralement pas exempte de tout reproche. Dans de telles situations, lâ□□appellation Riskware doit Ãªtre utilisÃ©e afin dâ□□attirer l'attention de l'utilisateur.

Ce que vous devez garder Ã l'esprit lorsque vous installez une application

N'utilisez que des sources dignes de confiance pour installer le logiciel. Dans le Google Market, lire les commentaires afin de vous tenir informÃ©.

Le Google Market affiche Ã©galement les autorisations de l'application souhaitent obtenir pour fonctionner. Ã□valuer si vous voulez attribuer ces autorisations demandÃ©es. Les logiciels de sÃ©curitÃ© comme G Data MobileSecurity pour Android peuvent afficher ces autorisations, mÃªme aprÃ¨s l'installation.

Vous trouverez les solutions G-Data chez GS2i.