G-Data : Checker, Fausses applications Facebook
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 11/6/2012 13:30:00

Le G-Data SecurityLabs dÃ©cortique un cas concret et apporte quelques Ã©clairages sur ces attaques,**le cas Checker**. Qui nâ□□a jamais rencontrÃ© une fausse application sur Facebook ?

Un ami publie une vidÃ©o Â« incroyable Â» sur son mur ou souhaite partager avec vous une application Â« extraordinaireÂ». Mais avant mÃªme que vous nâ□□ayez eu le temps de vous rendre compte de votre erreur, en cliquant sur ce message vous avez Ã votre tour partagÃ© cette fausse bonne information Ã lâ□□ensemble de vos amis. Quel est le but de ces fausses applications ? Sont-elles dangereuses ?

La plupart des attaques menÃ©es ont une portÃ©e Ã©conomique. En sâ□□appuyant sur les rÃ©seaux publicitaires les concepteurs de ces fausses applications ont trouvÃ© un moyen simple de gagner rapidement beaucoup dâ□□argent sans nÃ©cessairement nuire Ã l'utilisateur, du moins pas directement. Dans le cas Â« Checker Â» Ã©tudiÃ©, G Data SecurityLabs a dÃ©couvert une approche particuliÃ¨rement sophistiquÃ©e.

Tout commence avec un message sur le Mur : Un de vos amis possÃ¨de une application capable de vÃ©rifier qui de ses contacts consultent son profil. Une application forcÃ©ment trÃ¨s intÃ©ressante et enviable (non autorisÃ©e par Facebook. **ici**).

Ã□ dÃ©faut de diriger sur ladite application, lâ□□URL raccourcie conduit Ã une adresse Internet

dont la seule fonction est de vÃ©rifier le pays d'origine du visiteur. Selon le rÃ©sultat, le visiteur est alors dirigÃ© dans une longue chaÃ®ne de redirection vers de nombreux services ad intÃ©grÃ©s dans des iFrames. Chaque Â« visite Â» automatique sur ces sites permet Ã lâ□□attaquant de gagner de l'argent.

Selon les pays, diffÃ©rentes pages sont affichÃ©es Ã des frÃ©quences diverses. La page Internet justforfunapps est un exemple de pages affichÃ©es. Celle-ci est chargÃ©e de publicitÃ©s pour divers produits et services web. Heureusement, aucun lien intÃ©grÃ© nâ□□est malveillant, mais les attaquants peuvent rediriger le trafic vers un site Web dangereux dÃ¨s quâ□□ils le souhaitent.

Sur les autres sites ciblÃ©s, jeux de loterie, chÃ¨que-cadeau et rÃ©ductions diverses sont proposÃ©s. Des offres pour lesquelles il faut bien entendu saisir ses coordonnÃ©es personnelles (numÃ©ro de tÃ©lÃ©phone mobile, adresse e-mail, etc.). Certaines loteries invitent aussi lâ□□internaute Ã envoyer plusieurs SMS surtaxÃ©s.

Mode de propagation

Dans le cas de lâ□□application "Checker" testÃ©e, son installation est proposÃ©e lorsque la victime clique sur lâ□□image de la soi-disant interface affichÃ©e sur le mur de son ami. Une demande de validation des droits liÃ©s Ã lâ□□utilisation de lâ□□application est alors demandÃ©e. Une fois les autorisations accordÃ©es, "Checker" publie automatiquement lâ□□image de sa fausse interface sur le mur et attend ses futures victimes : soit elles cliquent sur le lien proposÃ© et entre dans la chaine de publicitÃ©s, soit elles cliquent sur lâ□□image et installent la fausse application. Dans les deux cas, lâ□□action des internautes contribue directement ou indirectement Ã lâ□□enrichissement de lâ□□attaquant.

Les solutions G-Data sont disponible chez GS2i.

Visitez le site de GS2i