Bitdefender : La croissance des risques de sÃ©curitÃ© liÃ©e aux rÃ©seaux sociaux
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 9/7/2012 14:00:00

Les rÃ©seaux sociaux ne sont pas nouveaux dans lâ□□Ã¨re Internet mais peu de vigilance leur est encore accordÃ©e, dâ□□un point de vue sÃ©curitÃ©. Le plus Ã©tonnant est que cela semble Ãªtre le cas autant pour les utilisateurs que pour les opÃ©rateurs de rÃ©seaux sociaux eux-mÃªmes, confirme **Bitdefender**.

Un exemple rÃ©cent : au dÃ©but du mois de Juin, plus de 6,5 millions de mots de passe utilisateurs ont Ã©chappÃ© Ã la vigilance de Linkedin et se sont trouvÃ©s diffusÃ©s sur des serveurs underground russes. Lâ□□enquÃªte est en cours. LinkedIn a rÃ©agi en envoyant des e-mails Ã leurs utilisateurs pour les inciter fortement Ã changer leur mot de passe, ce qui a entraÃ®nÃ© finalement un risque supplÃ©mentaire, Ã©tant donnÃ© quâ□□il est possible pour LinkedIn dâ□□associer plus dâ□□une adresse pour un utilisateur.

Selon **Alexandru Catalin Cosoi**, Directeur de recherche en sÃ©curitÃ© chez Bitdefender : Â« *le mail conseillant de rÃ©initialiser son mot de passe sembleavoir Ã©tÃ© envoyÃ© - alÃ©atoirement - Ã des adresses e-mail avec lesquelles les utilisateurs concernÃ©s Ã©taient certes liÃ©s, Ã leurs employeurs actuels ou passÃ©s, mais qui nâ□□avaient jamais Ã©tÃ© associÃ©es par les utilisateurs Ã leur compte LinkedIn. Nous pouvons donc supposer que lâ□□association a Ã©tÃ© rÃ©alisÃ©e en rassemblant des adresses, Ã partir des â□□invitations Ã se connecterâ□□ de LinkedIn* Â».

Les auteurs de logiciels malveillants ont aussi commencÃ© Ã tirer avantage de la popularitÃ© de LinkedIn, avec de faux e-mails, ayant lâ□□apparencede provenir du rÃ©seau social professionnel. Ainsi, des escroqueries obsolÃ¨tes connues sur Facebook, sont maintenant rÃ©pandues sur LinkedIn, persuadant des utilisateurs dâ□□exÃ©cuter des piÃ¨ces jointes malveillantes sur leurs ordinateurs.

Les lecteurs et utilisateurs ne doivent pas penser que LinkedIn est une exception. Ils sont simplement les derniÃ¨res victimes de ce type dâ□□attaque. Dâ□□autres rÃ©seaux sociaux tels que Facebook, Twitter ou encore Foursquare, dÃ©pensent de lâ□□Ã©nergie sur des questions de

sÃ©curitÃ© qui leur sont propres.

Ce type de problÃ¨me de sÃ©curitÃ© n'inspire pas vraiment confiance, et ne donne pas envie de lier fortement lâidentitÃ© des entreprises et lâimage des marques dans lâunivers des rÃ©seaux sociaux. Mais lâalternative de rompre lâaccÃ¨s, bien que tentant, nâest pas vraiment possible, en particulier pour les entreprises qui ont dÃ©jÃ intÃ©grÃ© les rÃ©seaux sociaux dans leur stratÃ©gie de vente et de marketing.

Pour **Alexandru Catalin Cosoi** : Â« *il reste une alternative, trouver le juste milieu entre lâexposition au risque, le coÃ»t et la commoditÃ©. Une bonne chose pour commencer serait de sensibiliser les utilisateurs Ã la sÃ©curitÃ© et de leur fournir une solution qui peut filtrer les liens quâils reÃ§oivent de leurs amis des rÃ©seaux sociaux, surveiller les paramÃ¨tres de confidentialitÃ© et empÃªcher les donnÃ©es critiques, tels que les mots de passe ou les numÃ©ros de sÃ©curitÃ© sociale dâÃªtre envoyÃ©s depuis un ordinateur, soit par un virus soit par des actions involontaires de son propriÃ©taire* Â».