BitDefender : Danger, Un Trojan cible les utilisateurs de Facebook
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 19/3/2010 0:00:00

Un faux message de modification de mot de passe est envoyÃ© de la part de FacebookÂ®

BitDefenderÂ®,Ã©diteur de solutions de sÃ©curitÃ© antimalwares, annonce aujourdâ□□hui quâ□□une vague de **diffusion de malware utilisant FacebookÂ® comme appÃ¢t** a dÃ©butÃ© hier soir. Sous lâ□□apparence dâ□□un email officiel Ã©manant de FacebookÂ®, les utilisateurs sont prÃ©venus du fait quâ□□ils doivent modifier leurs mots de passe pour des raisons de sÃ©curitÃ©. Les destinataires de cette fausse alerte sont supposÃ©s ouvrir une piÃ¨ce jointe au format .zip pour dÃ©couvrir leurs nouveaux identifiants.

A la place dâ□□un nouveau mot de passe, le fichier compressÃ© cache le cheval de Troie â□□ **Trojan.Dropper.Oficla.G**â□□. Ce Trojan contient en fait des codes malveillants ou des logiciels indÃ©sirables quâ□□il dÃ©pose et installe sur les PC. La plupart du temps, ce cheval de Troie installe une porte dÃ©robÃ©e ou Â« backdoor Â» qui permet aux pirates de disposer dâ□□un accÃ¨s distant clandestin aux machines infectÃ©es. Cette backdoor peut Ã©galement Ãªtre utilisÃ©e par les cybercriminels pour installer dâ□□autres codes malveillants sur les PC.

Selon le centre de surveillance des Laboratoires BitDefender, la diffusion des messages de spam incluant le code malveillant a dÃ©butÃ© dans la soirÃ©e du 17 mars 2010. Depuis, les vagues de spam atteignent des proportions impressionnantes atteignant parfois lâ□□envoi de 200 spams toutes les demi-heures.

De plus, lâ□□outil de surveillance BitDefender de diffusion des malwares indique le dÃ©but dâ□□une diffusion massive du cheval de Troie Trojan.Dropper.Oficla.G. Bien que ce phÃ©nomÃ¨ne ne fasse que commencer, cela ne semble plus Ãªtre quâ□□une question de temps avant que les cybercriminels ne contrÃ´lent un nombre consÃ©quent dâ□□ordinateurs.

Les prÃ©visions indiquent que le taux dâ□□infection va sÃ»rement Â« exploser Â» compte tenu de lâ□□efficacitÃ© des techniques dâ□□ingÃ©nierie sociale utilisÃ©es par ce stratagÃ¨me. FacebookÂ® est en effet un rÃ©seau social trÃ¨s en vogue et se connecter pour dialoguer et utiliser ses applications trÃ¨s populaires est devenu une habitude quotidienne pour de nombreuses personnes. Quelle que soient leurs motivations pour se connecter Ã ce rÃ©seau social, le prÃ©tendu email de changement de mot de passe les amÃ¨nera tous au mÃªme rÃ©sultat : ouvrir

le fichier pour y jeter un Å□il et Ãªtre infectÃ© au bout du compte.

Pour ne pas courir de risque, BitDefender recommande de ne jamais ouvrir les emails provenant de contacts inconnus et dâ□□installer et de mettre Ã jour une solution de sÃ©curitÃ© complÃ¨te et efficace.