

BitDefender : Jeux Vidéo et réseaux sociaux, Spams et Phishing en hausse
Sécurité

Posté par : JerryG

Publié le : 9/4/2010 0:00:00

Les applications de jeux sur les **réseaux sociaux** font augmenter le nombre de **spams et de phishing de plus de 50%**. L'étude de BitDefender révèle que des profils d'utilisateurs, l'appartenance à des groupes et le fait d'avoir des amis en commun donnent plus de crédibilité aux fausses identités

BitDefender®, Éditeur de solutions de sécurité antimalwares a présenté les résultats d'une étude sur l'impact que peut avoir la pratique de jeux sur les réseaux sociaux sur les données personnelles.

Pour obtenir les scores les plus élevés, les applications de jeux présentes sur les réseaux sociaux requièrent que les utilisateurs réunissent le plus grand nombre possible d'amis et de « supporters » autour d'un même jeu. Ceci amène les joueurs à développer des communautés de joueurs, des groupes et des pages de fans qui facilitent l'interaction entre les joueurs.



Les pirates à l'origine des campagnes de spams et de phishing exploitent également la tendance du « social gaming » en créant de faux profils et en utilisant des robots pour envoyer du spam à des groupes, comme le montre l'étude présentée par BitDefender lors de la MIT Spam Conference. Contrairement aux techniques de spams classiques qui utilisent le réseautage social, au sein duquel les spammeurs tentent de séduire les utilisateurs pour être admis dans leur cercle d'amis, les faux profils liés aux jeux sociaux sont volontairement ajoutés sans trop regarder par les utilisateurs qui cherchent avant tout à élargir la

communauté de joueurs autour de leurs jeux favoris. La suppression automatique de ces faux comptes est par conséquent quasi impossible à faire automatiquement compte tenu du fait que l'action effectuée par les spammeurs n'est pas prévisible en elle-même.

L'habitude de valider également que les faux comptes qui ont le plus de succès sont ceux qui imitent au mieux les véritables profils, avec de nombreuses informations et photos de leur supposé « utilisateur ». Au cours d'une expérience portant sur l'acceptation de ces profils, les chercheurs de BitDefender ont créé trois faux profils : l'un sans photo et ne contenant que peu de renseignements, l'autre avec une image et quelques informations et le troisième avec de très nombreuses informations et photos. Les trois profils ont rejoint des groupes portant sur des thèmes généraux. Une heure après avoir commencé à ajouter des « amis » à chaque profil, leur cercle d'amis est élargi avec 23 connexions pour le premier profil, 47 pour le deuxième et 53 pour le troisième.

L'expérience a ensuite été faite sur des groupes de jeux sociaux, le nombre d'utilisateurs souhaitant ajouter ces personnes inconnues a alors considérablement augmenté. En 24 heures, 85 utilisateurs ont ainsi accepté la demande provenant du premier profil, 108 celle du deuxième et 111 celle du troisième.

Ainsi, comme le souligne George Petre, Responsable de l'habitude des menaces chez BitDefender et auteur de cette étude, « les utilisateurs sont plus enclins à accepter des spammeurs dans leur liste d'amis dans un réseau social que dans tout autre environnement de communication en ligne. »

Les conséquences en termes de sécurité sont nombreuses : consolidation et progression de la puissance de nuisance des spammeurs, vol de données et d'identité, piratage de comptes et diffusion de malwares. Une URL raccourcie postée sans explication sur chaque faux profil a été suivie par 24% des « amis » de ces trois comptes, alors qu'ils ignoraient qu'elle avait publié et où elle conduisait.

George Petre ajoute que *"cette acceptation aveugle permet aux spammeurs et pirates utilisant des techniques d'ingénierie sociale de se rapprocher des utilisateurs de façon bien plus efficace que tout autre type de e-mail ou d'escroquerie. De plus, nous avons constaté que dans le cadre des réseaux sociaux, les utilisateurs peuvent plus facilement être piégés pour ajouter des spammeurs à leur profil. Facebook est tant le réseau social le plus en vogue en ce moment est aussi le réseau le plus exposé à ce type d'attaques."*

Afin de ne pas participer aux développements de ces menaces, nous recommandons donc bien sûr aux adeptes des jeux sociaux de faire preuve de la plus grande vigilance s'ils souhaitent élargir leur cercle d'amis.

[Pour plus d'informations concernant les produits BitDefender](#)