Les cybercriminels utilisent Twitter pour infecter les internautes
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 11/6/2009 0:00:00

Les pirates crÃ©ent des comptes sur Twitter puis publient des milliers de commentaires sur â□□PhishTube Broadcastâ□□ pour apparaÃ®tre parmi les thÃ¨mes les plus populaires. Ces commentaires contiennent des liens vers des pages web malveillantes conÃ§ues pour propager le faux antivirus PrivacyCenter.
Cette nouvelle attaque dâ□□un des rÃ©seaux les plus populaires du Web 2.0 fait suite aux attaques de Digg.com, et YouTube, entre autres.

PandaLabs, le laboratoire d'analyse et dÃ©tection des malwares de Panda Security, a dÃ©celÃ© une nouvelle menace visant les utilisateurs de Twitter. Pour cette attaque, les cybercriminels ont crÃ©Ã© des centaines de comptes Twitter et publiÃ© des milliers de commentaires sur le sujet de â□□PhishTube Broadcastâ□□, en rÃ©fÃ©rence au groupe de rock amÃ©ricain Phish.

Â

Â

En procÃ©dant de la sorte, les pirates nâ□□ont dâ□□autre but que de gagner un maximum dâ□□argent.

Â« *Nous avons averti derniÃ¨rement d'une augmentation des techniques malveillantes de rÃ©fÃ©rencement sur les moteurs de recherche ("BlackHat SEO"), notamment pour vendre des fausses solutions antivirus. Dans le cas de cette attaque, les pirates ne visent pas les moteurs de recherche mais le mÃ©canisme de classement de Twitter en faisant apparaÃ®tre les liens malveillants dans la liste des sujets populaires. Les utilisateurs de Twitter intÃ©ressÃ©s par le sujet exploitÃ© par les pirates se retrouvent face Ã des milliers de commentaires malveillants parmi les commentaires lÃ©gitimes* Â», explique **Luis Corrons**, le directeur technique de PandaLabs.

Â« *Avec ses millions d'utilisateurs, ce rÃ©seau est une cible trÃ¨s attractive pour les cybercriminels et nous pouvons nous attendre Ã ce qu'il soit de nouveau attaquÃ© Ã l'avenir.* Â»

L'exploitation de Twitter par les pirates est Ã rapprocher des autres attaques subies par les rÃ©seaux populaires du Web 2.0 tels que les attaques de **Digg.com**Â ou de **YouTube**Â rapportÃ©es par PandaLabs.

Pour plus dâ□□informations