Les cybercriminels utilisent Twitter pour infecter les internautes

- **Les pirates créent des comptes sur Twitter puis publient des milliers de commentaires sur « PhishTube Broadcast » pour apparaître parmi les thèmes les plus populaires.**

- **Ces commentaires contiennent des liens vers des pages web malveillantes conçues pour propager le faux antivirus PrivacyCenter.**

- **Cette nouvelle attaque d'un des réseaux les plus populaires du Web 2.0 fait suite aux attaques de Digg.com, et YouTube, entre autres.**

Paris, le 10 juin 2009

PandaLabs, le laboratoire d'analyse et détection des malwares de Panda Security, a décelé une nouvelle menace visant les utilisateurs de Twitter. Pour cette attaque, les cybercriminels ont créé des centaines de comptes Twitter et publié des milliers de commentaires sur le sujet de « PhishTube Broadcast », en référence au groupe de rock américain Phish. Par ce moyen, ils s'assurent d'apparaître dans la liste des sujets les plus commentés. Ils obtiennent ainsi une visibilité importante avec de nombreux utilisateurs qui visualisent leurs commentaires.

La liste des sujets les plus commentés (« Trending Topics ») est affichée sur l'interface de tous les utilisateurs de Twitter, présentant les sujets dont on parle le plus sur le réseau. En cliquant sur un de ces thèmes, l'utilisateur arrive sur une page affichant tous les tweets relatifs au thème en question.

Dans ce cas, les utilisateurs qui cliquent sur « PhishTube Broadcast » verront tous les commentaires malveillants publiés via les comptes créés par les pirates. Ces commentaires incluent des liens vers de fausses pages pornographiques. En cliquant sur n'importe lequel élément de ces pages, l'internaute infecte son ordinateur avec une copie du faux antivirus PrivacyCenter.

Un faux antivirus est un type d'adware conçu pour imiter un véritable antivirus et effectuer une fausse analyse du PC. A l'issue de cette l'analyse, PrivacyCenter informe l'utilisateur que son ordinateur est infecté par un logiciel malveillant. L'objectif est de faire croire aux utilisateurs qu'ils sont infectés puis de leur proposer de désinfecter la prétendue menace en achetant une version "premium" du faux antivirus. En procédant de la sorte, les pirates n'ont d'autre but que de gagner un maximum d'argent.

« Nous avons averti dernièrement d'une augmentation des techniques malveillantes de référencement 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 mécanisme de classement de Twitter en faisant apparaître les liens malveillants dans la liste des sujets populaires. Les utilisateurs de Twitter intéressés par le sujet exploité par les pirates se retrouvent face à des milliers de commentaires malveillants parmi les commentaires légitimes », explique Luis Corrons, le directeur technique de PandaLabs. « Avec ses millions d'utilisateurs, ce réseau est une cible très attractive pour les cybercriminels et nous pouvons nous attendre à ce qu'il soit de nouveau attaqué à l'avenir. »

L'exploitation de Twitter par les pirates est à rapprocher des autres attaques subies par les réseaux populaires du Web 2.0 tels que les attaques de Digg.com (http://www.pandasecurity.com/homeusers/media/press-releases/viewnews?noticia=9556) ou de YouTube (http://www.pandasecurity.com/france/homeusers/media/press-releases/viewnews?noticia=9699) rapportées par PandaLabs.

Pour plus d'informations, consultez le blog de PandaLabs à l'adresse : http://pandalabs.pandasecurity.com/archive/Rogueware-Campaigns-now-blending-into-Twitter-Trends.aspx

Des illustrations à l'adresse http://www.flickr.com/photos/panda_security/tags/malicioustwitter/

A propos de PandaLabs

Depuis 1990, la mission de PandaLabs est d'analyser les nouvelles menaces le plus rapidement possible pour assurer une totale sécurité à nos clients. Pour cela, PandaLabs a développé un système automatisé et innovant qui analyse et traite les milliers de nouveaux échantillons reçus chaque jour et renvoie automatiquement un verdict (logiciel malveillant ou inoffensif). Ce système repose sur l'Intelligence Collective Antimalware, le nouveau modèle de sécurité de Panda Security, qui détecte même les codes malveillants capables de passer au travers des autres solutions de sécurité.

Actuellement, 94 % des malwares détectés par PandaLabs sont analysés par l'Intelligence Collective Antimalware. Cette analyse automatique est complétée par le travail de plusieurs équipes spécialisées dans chaque type spécifique de malware (virus, vers, chevaux de Troie, logiciels espions, phishing, spam, rootkits, etc.) qui travaillent 24 heures sur 24 et 7 jours sur 7 pour offrir une garantie maximale. Grâce à ce système, Panda peut offrir à ses clients des solutions plus sûres, plus simples et consommant moins de ressources.

Pour plus d'informations, visitez le blog de PandaLabs : http://www.pandalabs.com