Le meilleur moyen de pirater quelqu'un ? Prétendre que vous êtes Facebook

Les résultats de la nouvelle recherche des Websense Security Labs montrent que les cybercriminels créent de plus en plus de faux sites copiant les réseaux sociaux afin de diffuser leurs attaques, et ciblent également les utilisateurs au bureau

Paris, le 14 mai 2009— Websense, Inc. (NASDAQ: WBSN) révèle aujourd'hui les résultats des recherches conduites par ses laboratoires de sécurité, les Websense Security Labs™. Il en ressort une tendance croissante au clonage de noms de domaines, avec en perspective pour les cybercriminels de cibler un nombre très importants d'utilisateurs des réseaux sociaux, et en particulier les habitués de Facebook, MySpace et Twitter.

Les cybercriminels utilisent de plus en plus des noms de domaine comportant des termes comme Facebook, MySpace et Twitter, sans aucun lien avec les sites réels. Ils cherchent ainsi par la ruse à mener des internautes peu méfiants à visiter des sites Web leurres et les inciter à fournir des informations confidentielles ou à télécharger un logiciel malveillant. Les laboratoires de recherche Websense indiquent qu'un échantillon d'analyse provenant de sa base de données d'URLs présente plus de 200 000 sites fictifs clonant des sites réels ont été développés, et dont les URLs contiennent toutes le terme Facebook, MySpace ou Twitter. Les exemples suivants s'inspirent de noms de site découverts : unblock.facebookproxy.com, buy.viagra.twitter.1234.com ou hotbabesofmyspace999.com (attention, il s'agit simplement d'exemples de noms de site similaires à ceux que les chercheurs ont découverts).

Les résultats de la recherche révèlent également que les cybercriminels ont fait ce qu'il fallait pour créer des clones permettant de contourner les dispositifs de sécurité mis en place par les entreprises. Un grand nombre de noms de domaines clonés sont des sites qui permettent de contourner le proxy de l'entreprise pour tenter d'échapper aux technologies de filtrage Web classiques.

Les cybercriminels ont su tirer parti de la forte augmentation du nombre de jeunes utilisateurs « accros » aux réseaux sociaux et entrant dans la vie active, ainsi que de la croissance de 276 % de Facebook sur la tranche d'âge 35-54 ans au cours des six derniers mois. Ainsi, le nom Facebook a été le nom de domaine le plus souvent utilisé pour duper les internautes. Les laboratoires de sécurité de Websense ont en effet recensé plus de 150 000 URLs reconnues comme leurres pendant la période étudiée.

« Ces nouvelles menaces mettent en perspective un futur où les cybercriminels vont continuer à cibler Facebook, MySpace et Twitter ainsi que d'autres sites de réseau social, et ce pour trois raisons », souligne Charles Renert, Directeur des Études chez Websense. « Ces sites Web sont populaires, du coup les fraudeurs peuvent viser de nombreuses personnes ; ces dernières se fiant au contenu des sites en questions, notamment parce qu'elles pensent qu'il provient d'autres personnes de leur

réseau. En outre, il faut rappeler que n'importe qui peut créer et publier du contenu sur ces sites, ils s'avèrent donc faciles à compromettre. Le filtrage Web classique n'est pas efficace pour protéger les utilisateurs contre les menaces que présentent les sites de confiance, et pour traquer les fraudeurs qui génèrent de nouvelles URLs quasi instantanément afin d'éviter la détection. Seule une analyse en temps réel du contenu Web peut empêcher que les utilisateurs soient victimes de ces attaques ».

Ce n'est pas la première fois que les utilisateurs de Facebook sont la cible des cybercriminels. Fin avril, les laboratoires Websense ont détecté une campagne de phishing visant les utilisateurs de Facebook. L'arnaque, baptisée « FBStarter » par les chercheurs en sécurité, redirigeait les utilisateurs vers une page de phishing imitant la page de connexion de Facebook. En indiquant leurs noms d'utilisateur et mots de passe, les internautes fournissaient aux cybercriminels les informations nécessaires pour accéder à leurs comptes et spammer leurs amis.

Les données compilées à partir du réseau Websense Threatseeker™ montrent que les sites web qui autorisent le contenu créé par l'utilisateur représentent la majorité des 50 diffuseurs de contenu malveillant les plus actifs. Et, 70 % de ces sites ont renfermé des logiciels malveillants au cours des six derniers mois, ainsi que du spam malveillant et le clonage d'URLs et de noms de domaine.

A propos de Websense, Inc.

Websense, Inc. (NASDAQ : WBSN), leader mondial des technologies intégrées de sécurité Web et de protection des courriels et des données, offre l'Essential Information Protection™ à plus de 44 millions de salariés du monde entier. Distribués au travers d'un réseau mondial de partenaires, les logiciels et les solutions de sécurité hébergées Websense aident les entreprises à bloquer les codes malveillants, à prévenir la perte d'informations confidentielles et à appliquer des règles de sécurité et d'accès Internet. Pour en savoir plus, consultez www.websense.com.