Alerte d’ESET sur la toute dernière attaque sur Facebook

le 16 février 2011

Les Pavillons-sous-Bois, ESET, spécialiste de la conception et du développement de logiciels de sécurité, annonce que des utilisateurs de Facebook viennent récemment d’être exposés à un groupe de vers, comprenant Win32/Yimfoca.AA et Win32/Fbphotofake. Le ver Win32/Yimfoca.AA s'est même placé dans les 10 premiers virus observés par le moteur de détection ThreatSense.Net d’ESET dans beaucoup de pays européens, y compris l'Autriche, l'Italie, la République Tchèque et la Slovaquie, pendant les dernières semaines.

Selon Marek Polesensky, chercheur de Malware chez ESET, **le ver Yimfoca exploite la messagerie instantanée de Facebook** pour attaquer, tandis que Fbphotofake est un ver de réseau social qui diffuse son code et d’autres menaces à travers des spams sur Facebook. Polesensky ajoute: "Yimfoca sert de porte dérobée qui peut être commandée à distance et peut également se propager via d’autres logiciels de messagerie instantanée comme Skype, MSN ou Yahoo Messenger " En plus, Yimfoca peut télécharger et exécuter d’autres codes malveillants mis en ligne - comprenant un faux logiciel d'antivirus, un code chargé de modifier les paramètres de sécurité ou encore de désactiver le pare-feu. Le ver Fbphotofake diffuse principalement du spam via Facebook. Les utilisateurs doivent veiller à faire attention et à ne pas ouvrir les fichiers attachés soupçonneux et inconnus, ou cliquer sur des liens douteux.

Suite à ces récentes attaques de malwares, David Harley, chercheur analyste chez ESET, a précisé que **la transmission de messages Facebook est de plus en plus exploitée** par l’arnaque de la lettre pseudo-officielle de Nigériens. " Il s’agit d’une tentative d’escroquerie maquillée sous forme de chantage émotif " précise Harley. Il conseille aux utilisateurs " de veiller à être certain de l’identité de l'expéditeur et du contenu du message Facebook ".

Randy Abrams, Directeur de la formation technique chez ESET aux USA, note quant à lui « qu’une partie du problème tient au fait que la culture Facebook est anti-sécuritaire et que c'est donc un obstacle difficile à surmonter pour les professionnels de la sécurité "

Dernière attaques Facebook

- Le vers Win32/Yimfoca.AA s’est diffusé pendant les derniers mois et s’est positionné parmi les 10 premières menaces constatées dans de nombreux pays européen à travers le moteur ThreatSense.Net.
- Fbphotofake propage du spam via Facebook. Pour se prémunir de ces deux vers, les utilisateurs doivent veiller à ne pas ouvrir de fichiers incertains et cliquer sur des liens douteux.
- L’arnaque de type Nigerian letter est en train de se diffuser via des messages Facebook.
- Des mises à jour et de l’information peuvent être consultées sur le site : http://www.facebook.com/security.

À propos de ThreatSense.Net®

ThreatSense.Net® est un système Cloud computing de collecte de malwares utilisant des données recueillies sur les postes de travail qui emploient les solutions ESET dans le monde entier. Ce système d’observation et de détection permanente fournit un flux d’information en continu aux experts du laboratoire d’analyse des virus d’ESET afin de leur dresser un portrait précis et en temps réel sur la nature et la portée des infiltrations globales. L'analyse en profondeur des menaces, des vecteurs d'attaque et des configurations permet à ESET d’ajuster le traitement heuristique et toutes les mises à jour de la base de signatures afin de protéger ses utilisateurs contre des menaces à venir.

A propos d'ESET

La société ESET est spécialisée dans la conception et le développement de logiciels de sécurité offrant une protection globale contre les menaces évolutives qui sévissent dans les environnements informatiques. Pionnier en matière de détection proactive des menaces, ESET est aujourd'hui le leader dans ce domaine. ESET a développé un vaste réseau mondial de partenariats, y compris avec des entreprises telles que Canon, Dell et Microsoft. ESET possède des bureaux à Bratislava (Slovaquie), Bristol (Royaume-Unis), Buenos Aires (Argentine), San Diego (USA), Prague (République Tchèque), et est représenté dans plus de 110 pays. Pour plus d'informations, veuillez visiter les sites Internet :www.eset-nod32.fr ou www.athena-gs.com