À Montrouge, le jeudi 11 février 2010

Un cheval de Troie, une idée de cadeau originale pour la Saint-Valentin

Et si vous receviez un cheval de troie pour la Saint-Valentin ?

À l approche de la Saint-Valentin, certains résultats de moteurs de recherche à la requête « cute Valentines day ideas » (« idées de cadeaux pour la Saint-Valentin ») sont utilisés pour diffuser des malwares.

Les statistiques montrent que ces termes ont été très employés ces jours-ci pour effectuer des recherches sur Internet, et il n est donc pas étonnant que les cybercriminels tentent eux aussi de tirer profit de cette atmosphère romantique. Concrètement, la simple recherche sur Internet d une « idée » pour faire plaisir à l élu(e) de son c ur à l occasion de la Saint-Valentin peut entraîner le téléchargement de malwares sur le système des utilisateurs.

Les malwares aiment les traditions, surtout quand elles favorisent leur diffusion : lorsque les utilisateurs cliquent sur un lien vers un site Web à l'apparence légitime dans la page de résultats de leur recherche, ils sont automatiquement

redirigés vers un site Web qui infecte leur système avec un faux antivirus identifié par BitDefender sous le nom de « Trojan.Fakeav.YZ ».

Trojan.Fakeav.YZ a ensuite un comportement similaire à celui d'autres faux antivirus : la fenêtre du navigateur est automatiquement réduite alors qu'un message d'avertissement s'affiche, signalant aux utilisateurs la présence de nombreuses infections sur leur ordinateur et leur recommandant d'installer une solution de sécurité.

Que l'utilisateur clique sur le bouton « OK » ou sur « Annuler » dans l'une des fenêtres pop-up à l'écran, le résultat est le même : il lance un faux processus d'analyse s'affichant dans la fenêtre du navigateur restaurée. Ce simulacre d'analyse en temps réel détecte de multiples malwares sur le système alors que d'autres fausses fenêtres pop-up incitent l'utilisateur à télécharger le programme malveillant. À chaque « analyse », le nombre d'infections détectées augmente, afin de convaincre les utilisateurs de la nécessité d'enregistrer le faux programme antivirus. Une fois installé, il modifie le contenu de plusieurs fichiers systèmes et déclenche l'affichage de nombreuses fenêtres pop-up avertissant de problèmes système et d'infections imaginaires. Il demande aussi constamment à l'utilisateur d'acheter ou de renouveler une licence.

Vous pouvez voir ici les actions de ce « joli cadeau » : http://www.youtube.com/watch?v=4duTeuDOGLo

Afin de protéger vos systèmes et données pour éviter de les compromettre, veuillez suivre les cinq conseils ci-dessous :

- Installez et activez une solution pare-feu et antimalware fiable ainsi qu'un filtre antispam, comme celles proposées parBitDefender.
- Mettez à jour votre antimalware, votre pare-feu et votre filtre antispam aussi souvent que possible avec les dernières définitions devirus et signatures de fichiers et d'applications suspectes.
- Analysez votre système fréquemment
- Vérifiez régulièrement votre système d'exploitation : téléchargez et installez les dernières mises à jour de sécurité et les outils permettant de supprimer des malwares, ainsi que les autres patches et fixes disponibles.
- Ne téléchargez pas et n'enregistrez pas de fichiers provenant de sources inconnues ; même s'ils proviennent d'une source fiable, évitez d'ouvrir et de copier des fichiers sur votre système sans avoir lancé auparavant une analyse antimalware complète.

À propos de BitDefender®

BitDefender est la société créatrice de l'une des gammes de solutions de sécurité la plus complète et la plus certifiée au niveau international reconnues comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en

matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les solutions de sécurité BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont disponibles via le Centre de presse. Retrouvez également sur le sitewww.malwarecity.fr les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.

À propos des Editions Profil

Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et de contrôle parental Parental Filter 2, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.