Le vendredi 6 mars 2009

Les laboratoires BitDefender analysent l'exploitation d'une nouvelle faille Adobe PDF

Les spammeurs et les voleurs d'informations trouvent tous les jours de nouvelles manières d'exploiter cette vulnérabilité

BitDefender ® analyse l'utilisation de la dernière faille touchant le format PDF d'Adobe, découverte pour la toute première fois le 4 novembre 2008.

L'analyse BitDefender a démontré que les principaux dangers qui affectent l'utilisateur comprennent différents malwares :

1. Backdoor.Poisonivy.GK est une porte dérobée qui permet au spammeur de se connecter à distance à l'ordinateur infecté et d'exécuter des commandes non autorisées. Il surveille et enregistre également toutes les applications et les versions des applications que la victime utilise.

2. Trojan.Spammer.Tedroo.BA est un cheval de Troie qui transforme un ordinateur infecté en un ordinateur envoyant du spam.

3. **Trojan.Spy.Goldun.NEP,** lui surveille les fenêtres Internet Explorer et vole les informations d'authentification des utilisateurs pour le système de paiement en ligne e-gold.

Pour plus de sécurité et afin d'éviter de telles atteintes à leur vie privée, nous recommandons aux utilisateurs de mettre à jour leurs solutions de sécurité, ainsi que d'installer toutes les mises à jour de sécurité Adobe existantes.

Depuis la diffusion de la mise à jour de sécurité Adobe, on sait qu'Adobe Reader 8 et Adobe Acrobat 8 (versions antérieures à la 8.1.3) sont sujets à de multiples dénis de service et exploits. Ces informations essentielles n'ont pas échappé non plus ni aux spammeurs, ni aux voleurs d'informations.

Le 6 novembre, la faille sur la fonction "util.printf()"d'Adobe était publiée et le lendemain, le premier cheval de Troie était repéré dans des spams et sur des sites Internet malicieux. Détecté par BitDefender comme **Exploit.PDF.A,** le code JavaScrit à l'intérieur du PDF tentait de télécharger d'autres malwares à partir de l'adresse : http://adxdnet.n[removed]un.php après une exploitation réussie. Le code de commandes était encodé en caractères ASCII en clair et exécuté 5 secondes après l'ouverture du document.

Plusieurs variantes de ce PDF malicieux sont apparues dans les mois suivants, modifiant le code d'exploitation et la charge utile. Des versions plus récentes contiennent du code crypté. Une exploitation de faille pour la fonction "**Collab.collectEmailInfo()"** a également été ajoutée afin d'augmenter le taux d'infection.

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 site www.malwarecity.com 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 Parental Filter, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.