Le jeudi 11 juin 2009

BitDefender découvre des scammeurs imitant des sites de paiement en ligne pour obtenir des informations personnelles de leurs victimes

Des malwares furtifs redirigent les navigateurs Internet vers de faux sites Internet

Les chercheurs BitDefender® confirment que les services de paiement en ligne font toujours partie des dix identités les plus souvent usurpées dans le monde du spam et du phishing, conformément au dernier rapport BitDefender sur l'état des e-menaces

La dernière campagne de phishing ciblant les utilisateurs de services bancaires et de paiements en ligne comporte plusieurs éléments caractéristiques propres aux malwares. D'abord, le message non sollicité diffusant le malware prétend proposer la meilleure Solution Antivirus Open Source et demande aux utilisateurs de visiter une page Web où ils peuvent télécharger le produit.

Pourtant, une fois que l'utilisateur a cliqué sur le lien, il ne reçoit pas la suite de sécurité promise, mais un faux exécutable, *setup.exe*, une archive auto-extractible qui s'exécute bien comme telle. Son but est de remplacer le contenu du répertoire *C:\WINDOWS\System32\drivers\etc* et de modifier le comportement du navigateur Web, en chargeant automatiquement des pages Web spécialement conçues à des fins de phishing imitant des sites de paiement en ligne tels que PayPal, Abbey ou Halifax.

Puis, à chaque fois que l'utilisateur tape dans son navigateur une adresse appartenant à l'une de ces institutions financières, il est automatiquement redirigé vers les fausses pages. Ses données d'authentification (nom d'utilisateur, mot de passe, code de sécurité) et d'autres données sensibles (nom, prénom, adresse e-mail, adresse postale, numéro et date d'expiration de la carte, code de vérification de la carte et même, le code confidentiel) sont récupérées via des scripts PHP. Toutes les autres options du menu disponibles sur les pages redirigent l'utilisateur vers les sections appropriées des véritables sites Web.

L'analyse a révélé que ces fausses pages Web se chargeaient à partir de domaines enregistrés en Chine et en Corée.

« La situation économique actuelle a inévitablement conduit à la prolifération des délits informatiques » explique Vlad Valceanu, Directeur de la Recherche Antispam des Laboratoires BitDefender. « Les dernières tendances observées par BitDefender révèlent plusieurs aspects alarmants : d'abord, depuis le début de l'année, les scams et les actes de phishing suivent une courbe ascendante. Ensuite, la complexité et l'agressivité de ces attaques ont augmenté considérablement ainsi que le nombre de victimes de ces attaques. Les utilisateurs doivent non seulement faire plus attention aux e-mails qu'ils reçoivent, mais il est également important qu'ils installent une solution de sécurité fiable sur leurs systèmes, afin d'éviter de prochaines attaques ».

Pour être informé au sujet des e-menaces inscrivez-vous aux flux RSS BitDefender.

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.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 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.