Communiqué de presse

À Montrouge, mardi 26 janvier 2010

Des auteurs de virus créent « Win32.Worm.Zimuse »,
un code malveillant qui endommage le disque dur des ordinateurs

Un faux test de QI combine en fait virus, rootkit et ver dans une formule fatale

BitDefender®, éditeur de solutions de sécurité antimalwares, a identifié aujourd'hui une nouvelle menace informatique alliant le comportement destructeur des virus aux mécanismes de diffusion des vers. Il existe deux variantes connues de ce virus, qui s'introduit dans l'ordinateur sous la forme d'un innocent test de QI.

Une fois exécuté, le ver crée entre sept et onze copies de lui-même (selon la variante) dans des zones sensibles du système de Windows.

Win32.Worm.Zimuse.A est un malware extrêmement dangereux. Contrairement à la plupart des vers, Win32.Worm.Zimuse.A peut causer d'importantes pertes de données car il écrase les 50 premiers kilo-octets de la zone d'amorçage du disque dur (Master Boot Record) - une zone essentielle du disque dur.

Afin de s'exécuter à chaque amorçage de Windows, le ver définit l'entrée de registre suivante :
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]"Dump"="%programfiles%\Dump\Dump.exe

Il crée également deux fichiers pilotes : %system%\drivers\Mstart.sys et %system%\drivers\Mseu.sys

Les versions 64 bits de Windows Vista et Windows 7 requérant des pilotes avec une signature numérique, le ver ne peut y installer ces fichiers.

Malheureusement, lors des premières étapes de l'infection, il est presque impossible aux utilisateurs de découvrir que leur système est victime d'une menace informatique. Suite à l'infection, après un certain nombre de jours (40 jours pour la variante A et 20 jours pour la variante B), l'ordinateur affiche un message d'erreur

affirmant qu'un problème a eu lieu en raison de contenu malveillant présent dans les paquets IP provenant d'une URL particulière. L'utilisateur est ensuite invité à restaurer le système en appuyant sur « OK ». Le redémarrage qui a lieu à la suite de ce message, endommage le disque dur de l'ordinateur en raison de la corruption du secteur d'amorçage. Pour voir une vidéo présentant les étapes d'une attaque de Win32.Worm.Zimuse.A, veuillez cliquer ici.

Afin de profiter d'Internet en toute sécurité, BitDefender recommande d'installer et de mettre à jour régulièrement une suite antimalware complète avec une protection antivirus, antispam, antiphishing et pare-feu. Nous recommandons la plus grande vigilance aux utilisateurs lorsqu'il leur est demandé d'ouvrir des fichiers provenant d'emplacements inconnus.

Marc Blanchard, épidémiologiste et Directeur des Laboratoires Editions Profil pour BitDefender en France ajoute :
" Le Worm Zimuse fait partie des malwares dit 'hautement destructeur'. Il en existe peu en circulation, les hackers ayant plutôt tendance à exploiter les machines des utilisateurs de manière invisible, mais ce type de menace est néanmoins émergeant ces dernières semaines. Leurs principes de fonctionnement ne laissent aucune chance à l'utilisateur une fois la destruction programmée. De plus, du fait que le secteur d'amorçage du disque dur Master Boot Record est touché, un reformatage dit de haut niveau ne suffira pas à retirer ce malware. Il faudra, alors, procéder à un reformatage du disque dur dit « d'usine », ce qui n'est pas toujours évident à mettre en place pour un utilisateur standard. Seule solution pour éviter ce type d'attaque, installer une protection antivirale proactive AVANT que le malware puisse opérer son action de destruction."

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 reconnue 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. Pour plus d'informations, visitez : www.bitdefender.fr

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.