BitDefender : La parade contre Win32.Worm.Zimuse, qui attaque le disque dur
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 27/1/2010 0:00:00

Un faux test de QI combine en fait virus, rootkit et ver dans une formule fatale. BitDefenderÂ®, Ã©diteur de solutions de sÃ©curitÃ© antimalwares, a identifiÃ© aujourd'hui une nouvelle menace informatique alliant le comportement destructeur des virus aux mÃ©canismes 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 exÃ©cutÃ©, le ver crÃ©e entre sept et onze copies de lui-mÃªme (selon la variante) dans des zones sensibles du systÃ¨me de Windows.

Win32.Worm.Zimuse.A est un malware extrÃªmement dangereux. Contrairement Ã la plupart des vers, Win32.Worm.Zimuse.A peut causer d'importantes pertes de donnÃ©es car il Ã©crase les 50 premiers kilo-octets de la zone d'amorÃ§age du disque dur (Master Boot Record) - une zone essentielle du disque dur.

Afin de s'exÃ©cuter Ã chaque amorÃ§age de Windows, le ver dÃ©finit l'entrÃ©e de registre suivante :

[HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersionRun]"Dump"="%programfiles%DumpDump.exe

Il crÃ©e Ã©galement deux fichiers pilotes : %system%driversMstart.sys et %system%driversMseu.sys

Les versions 64 bits de Windows Vista et Windows 7 requÃ©rant des pilotes avec une signature numÃ©rique, le ver ne peut y installer ces fichiers.

Malheureusement, lors des premiÃ¨res Ã©tapes de l'infection, il est presque impossible aux utilisateurs de dÃ©couvrir que leur systÃ¨me est victime d'une menace informatique. Suite Ã l'infection, aprÃ¨s 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 problÃ¨me a eu lieu en raison de contenu malveillant prÃ©sent dans les paquets IP provenant d'une URL particuliÃ¨re. L'utilisateur est ensuite invitÃ© Ã restaurer le systÃ¨me en appuyant sur Â« OK Â». Le redÃ©marrage qui a lieu

Ã la suite de ce message, endommage le disque dur de l'ordinateur en raison de la corruption du secteur d'amorÃ§age.

Pour voir une vidÃ©o prÃ©sentant les Ã©tapes d'une attaque de Win32.Worm.Zimuse.A.

Afin de profiter d'Internet en toute sÃ©curitÃ©, BitDefender recommande d'installer et de mettre Ã jour rÃ©guliÃ¨rement une suite antimalware complÃ¨te avec une protection antivirus, antispam, antiphishing et pare-feu. Nous recommandons la plus grande vigilance aux utilisateurs lorsqu'il leur est demandÃ© d'ouvrir des fichiers provenant d'emplacements inconnus.

Marc Blanchard, Ã©pidÃ©miologiste 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 plutÃ´t tendance Ã exploiter les machines des utilisateurs de maniÃ¨re invisible, mais ce type de menace est nÃ©anmoins Ã©mergeant ces derniÃ¨res semaines. Leurs principes de fonctionnement ne laissent aucune chance Ã l'utilisateur une fois la destruction programmÃ©e. De plus, du fait que le secteur dâ□□amorÃ§age du disque dur Master Boot Record est touchÃ©, un reformatage dit de haut niveau ne suffira pas Ã retirer ce malware. Il faudra, alors, procÃ©der Ã un reformatage du disque dur dit Â« d'usine Â», ce qui n'est pas toujours Ã©vident Ã mettre en place pour un utilisateur standard. Seule solution pour Ã©viter ce type dâ□□attaque, installer une protection antivirale proactive AVANT que le malware puisse opÃ©rer son action de destruction.*"

Suite Ã la diffusion croissante du malware Win32.Worm.Zimuse qui sâ□□attaque aux disques durs des personnes qui en sont victimes, BitDefenderÂ®, Ã©diteur de solutions de sÃ©curitÃ© antimalware, met Ã la disposition de tous les internautes un outil de dÃ©sinfection gratuit disponible :

Sur le site webÂ Â ou directement en **tÃ©lÃ©chargeant l'Outil de dÃ©sinfection**

Pour se prÃ©munir de se type de menace et Ã©viter les dÃ©sinfections Ã postÃ©riori, BitDefender recommande de disposer dâ□□une solution de sÃ©curitÃ© proactive rÃ©guliÃ¨rement mise Ã jour.