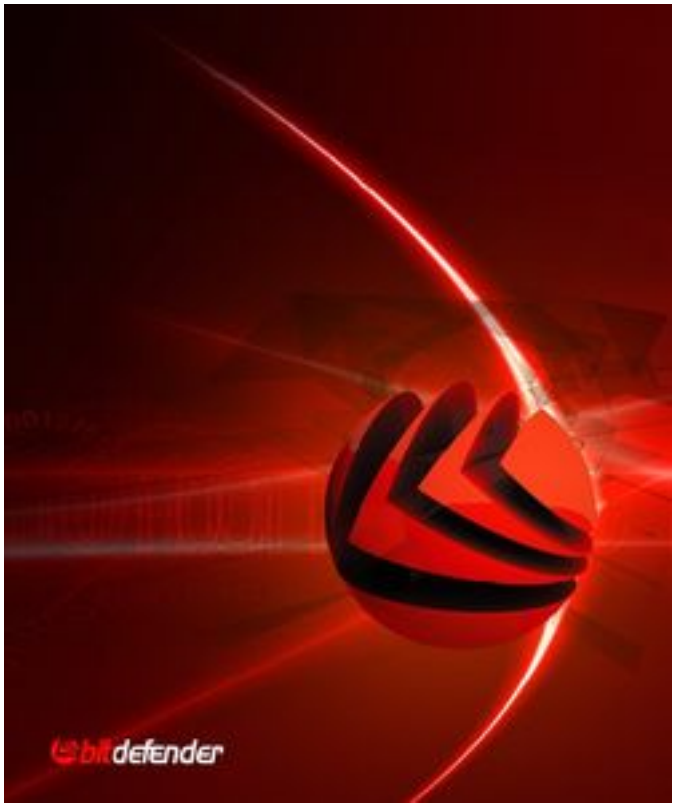
BitDefender : le ver Conficker ou Downadup, maitrisÃ©
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 16/2/2009 0:00:00

On apprenait rÃ©cemment que Microsoft offrait une rÃ©compense pour la tÃªte du crÃ©ateur du ***ver Conficker ou Downadup***, qui cause bien des soucis sur les PC des internautes innocents et bien ***les chercheurs de BitDefender ont dÃ©jÃ mis au point un antidote.***
Win32.Worm.Downadup, un ver informatique qui se rÃ©pand en utilisant une vulnÃ©rabilitÃ© du service serveur Windows RPC a Ã©tÃ© dÃ©tectÃ© par BitDefenderÂ®. Ce ver (aussi appelÃ© Conficker ou Kido) n'est pas nouveau en soi.

Il est apparu pour la premiÃ¨re fois fin Novembre 2008, exploitant la vulnÃ©rabilitÃ© MS08-067 pour se rÃ©pandre facilement Ã travers les rÃ©seaux locaux et installer des programmes malveillants (programmes rogues) sur les ordinateurs infectÃ©s.



Â

Fin dÃ©cembre, les Laboratoires BitDefender avaient dÃ©couvert une nouvelle version de ce ver appelÃ©e Win32.Worm.Downadup.B. Le malware prÃ©sente de nouvelles caractÃ©ristiques, outre son mode de propagation et des signes d'amÃ©lioration.

Le ver utilise des clÃ©s USB pour se diffuser. Il se copie dans un dossier alÃ©atoire Ã l'intÃ©rieur du rÃ©pertoire RECYCLER (utilisÃ© par la corbeille pour stocker les fichiers supprimÃ©s) et crÃ©e un fichier autorun.inf dans le dossier racine du lecteur infectÃ©. Le ver s'exÃ©cute alors automatiquement si le lancement automatique est autorisÃ©.

Le ver a Ã©galement corrigÃ© certaines fonctions TCP afin de bloquer l'accÃ¨s aux sites Internet liÃ©s Ã la sÃ©curitÃ© informatique en filtrant certaines chaÃ®nes de caractÃ¨res contenues dans chaque adresse. Cela le rend encore plus difficile Ã Ã©liminer puisqu'il est presque impossible de recueillir des informations Ã son sujet Ã partir d'un ordinateur infectÃ©.

Â

De plus, il supprime certains droits d'accÃ¨s de l'utilisateur afin de protÃ©ger ses fichiers.

Le ver est Ã©galement conÃ§u de faÃ§on Ã ne pas Ãªtre dÃ©tectÃ© par les antivirus : il travaille avec des interfaces API rarement utilisÃ©es afin d'Ã©viter les technologies de virtualisation. Il empÃªche les mises Ã jour Windows et certains trafics rÃ©seau, en optimisant les caractÃ©ristiques de Vista pour faciliter sa propagation.

Win32.Worm.Downadup.B a un algorithme de gÃ©nÃ©ration de noms de domaine similaire Ã celui trouvÃ© dans des botnets comme Rustock. Il compose 250 domaines par jour et vÃ©rifie certains d'entre eux pour effectuer des mises Ã jour ou tÃ©lÃ©charger et installer d'autres fichiers.

En raison de ses caractÃ©ristiques (un systÃ¨me extrÃªmement rÃ©cent, une bonne protection) et car beaucoup de gens ne font pas de mises Ã jours rÃ©guliÃ¨res de leur antivirus, ce ver pourrait devenir un rival aux botnets existants comme Storm ou Srizbi.

Pour plus d'informations techniques, vous pouvez consulter le **blog Malwarecity** (Malwarecity Blog) et la description de ce ver informatique (dÃ©scription du ver).

Un outil de suppression est Ã©galement disponible sur le site

Â