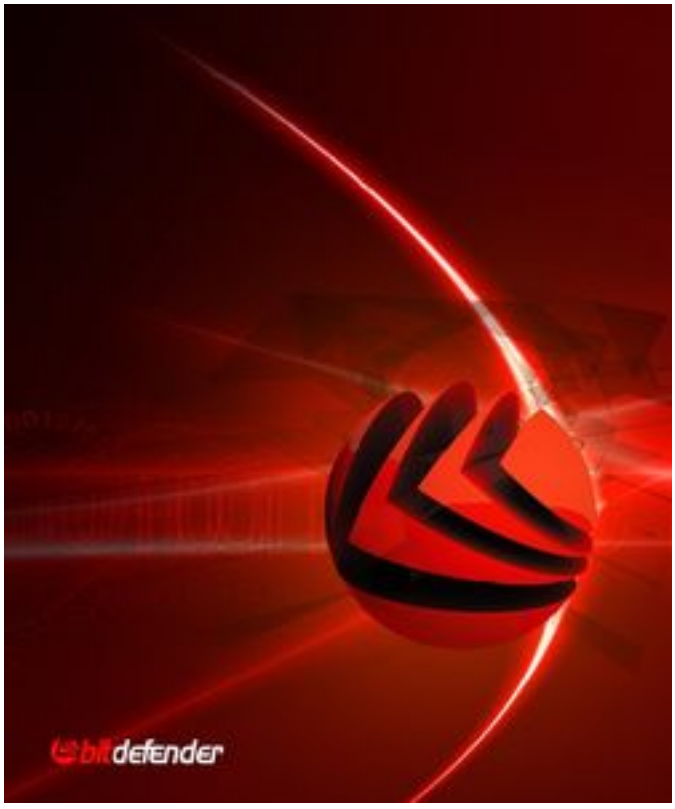
BitDefender : 1 er Ã proposer un outil pour dÃ©sinfecter Downadup
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 12/3/2009 0:00:00

BitDefender annonce qu'une nouvelle variante du ver Downadup se rÃ©pand largement sur Internet
BitDefenderÂ®, lâ□□un des fournisseurs les plus rÃ©compensÃ©s de solutions antivirus et de sÃ©curitÃ© des donnÃ©es a dÃ©tectÃ© une nouvelle version, plus agressive, du virus Downadup, qui se diffuse en utilisant une vulnÃ©rabilitÃ© de Windows RPC Server Service sous le nom de Win32.Worm.Downadup.C.

Cette nouvelle version rÃ©siste mieux Ã la dÃ©sinfection que les prÃ©cÃ©dentes. Une fois le systÃ¨me corrompu, le ver dÃ©sactive Windows Update et bloque l'accÃ¨s Ã la plupart des sites Internet anti-virus afin d'empÃªcher l'utilisateur de dÃ©sinfecter son ordinateur.



BitDefender est le premier Ã proposer **un outil gratuit qui dÃ©sinfecte toutes les versions de Downadup et qui est disponible dÃ¨s maintenant Ã l'adresse suivante** . Ce domaine est le premier Ã fournir un outil permettant de supprimer ce ver qui ne soit pas bloquÃ© par l'e-menace.

Le ver par lui-mÃªme n'est pas nouveau, il est apparu pour la premiÃ¨re fois fin Novembre 2008, et est connu sous les noms de Conficker ou Kido. Ce ver exploite Ã©galement la vulnÃ©rabilitÃ© dÃ©crite dans le bulletin de sÃ©curitÃ© Microsoft MS08-067.

Une fois l'exploitation rÃ©ussie, il installe des logiciels Â« rogues Â» sur l'ordinateur infectÃ©.

Â« ***Les laboratoires BitDefender observent de plus en plus une augmentation du nombre de vers, tel que Downadup, ayant un algorithme mathÃ©matique gÃ©nÃ©rant des sÃ©quences Ã partir de la date du jour*** Â» a expliquÃ© Vlad Valceanu, spÃ©cialiste des malwares pour BitDefender.

Â« ***Les vers produisent ensuite un nombre fixe de noms de domaines tous les jours et recherchent des mises Ã jour. Cela permet aux crÃ©ateurs de malwares et aux cybercriminels de rÃ©aliser facilement une nouvelle version du ver ou de lui donner une nouvelle charge utile, puisqu'ils n'ont qu'Ã enregistrer l'un des domaines et Ã tÃ©lÃ©charger ensuite les fichiers*** Â».
Â