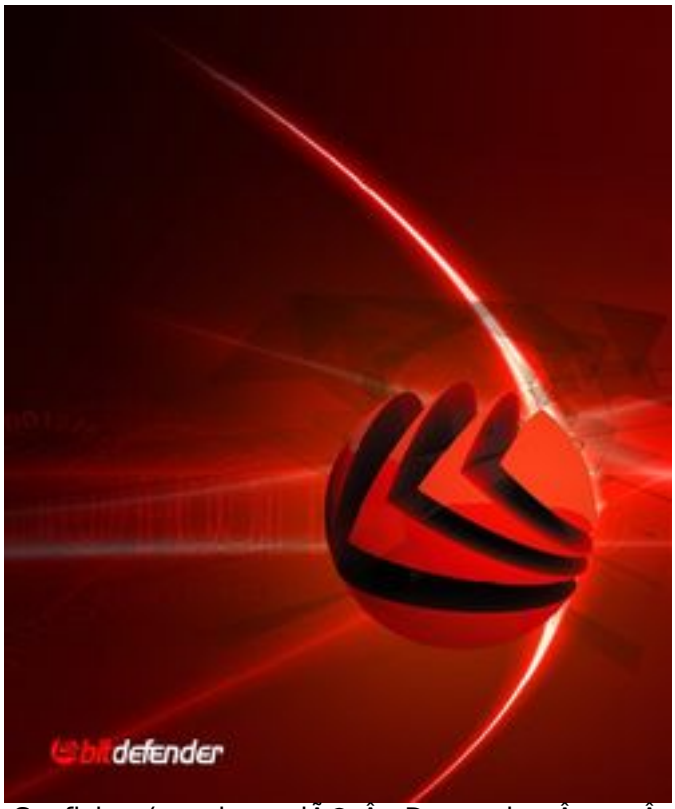
BitDefender publie le livre blanc Â« Conficker â Un an aprÃ¨s Â»
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 17/12/2009 0:00:00

Â« **Conficker â Un an aprÃ¨s** Â» ou comment **le ver Conficker** sâest diffusÃ© depuis 2008 et comment il pourrait devenir une menace encore plus importante en 2010

BitDefender, Ã©diteur de solutions de sÃ©curitÃ© antimalwares, a annoncÃ© aujourdâhui la publication de Â« Conficker â Un an aprÃ¨s Â», un livre blanc traitant de la premiÃ¨re apparition du ver Conficker en novembre 2008, des dommages quâil a causÃ©s et de la faÃ§on dont il pourrait se diffuser en 2010. Conficker est un malware bien conÃ§u au potentiel de destruction important en raison de son ingÃ©nieux systÃ¨me de mises Ã jour. Le livre blanc de BitDefender, Â« Conficker â Un an aprÃ¨s Â», donne Ã©galement des conseils aux lecteurs pour protÃ©ger leurs systÃ¨mes contre ce ver.



Conficker (aussi appelÃ© Â« Downadup Â» ou Â« Kido Â») est un ver de rÃ©seau qui exploite les vulnÃ©rabilitÃ©s de MicrosoftÂ® WindowsÂ® pour se diffuser. Le principal objectif de Conficker est de compromettre autant de machines que possible en exploitant une vulnÃ©rabilitÃ© du Service Serveur RPC de Microsoft Windows, dÃ©crite dans le Bulletin de SÃ©curitÃ© de Microsoft MS08-067. **La vulnÃ©rabilitÃ© permet Ã un attaquant dâexÃ©cuter du code Ã distance sur une machine non protÃ©gÃ©e.**

De nombreuses variantes du ver Conficker ont Ã©tÃ© crÃ©Ã©es depuis son apparition. Certaines utilisent la fonction Autorun (exÃ©cution automatique) pour les supports et disques amovibles (tels que les pÃ©riphÃ©riques de stockage et clÃ©s USB) pour se diffuser, alors que dâautres profitent de mots de passe non sÃ©curisÃ©s pour infiltrer des rÃ©seaux. Une autre variante

dÃ©sactive Microsoft Windows Update et bloque lâaccÃ¨s Ã la plupart des sites Web antimalwares, ce qui empÃªche les utilisateurs de procÃ©der Ã des mises Ã jour de sÃ©curitÃ© manuelles ou automatiques.

Conficker continue Ã causer des dÃ©gÃ¢ts, malgrÃ© la rÃ©compense de 250 000 $ promise par Microsoft en Ã©change dâinformations permettant de dÃ©couvrir qui se cache derriÃ¨re ce ver. Les chercheurs des laboratoires **BitDefender estiment que Conficker deviendra une menace encore plus importante en 2010** en recourant aux techniques suivantes :

â¢ Neutralisation des systÃ¨mes de dÃ©fense â Conficker neutralisera complÃ¨tement les systÃ¨mes de dÃ©fense et laissera de dangereuses brÃ¨ches de sÃ©curitÃ© sur le rÃ©seau de lâutilisateur.

â¢ DÃ©ni de service distribuÃ© â En paralysant des ordinateurs sur Internet, Conficker les empÃªchera dâaccÃ©der Ã certains sites Internet pendant de longues pÃ©riodes.

â¢ Fraudes au clic â Conficker sera utilisÃ© pour visiter certains sites Web et pour Â« cliquer Â» automatiquement sur des banniÃ¨res publicitaires afin de gÃ©nÃ©rer des gains financiers.

â¢ Enregistreurs de frappes, surveillance du trafic rÃ©seau et vols dâidentitÃ© Ã grande Ã©chelle â Conficker, comme de nombreux botnets, sera programmÃ© pour surveiller les frappes des victimes et utilisera ces informations pour accÃ©der Ã leurs informations confidentielles.

â¢ Envoi de spam â Conficker recueillera des adresses e-mail, qui seront utilisÃ©es pour envoyer de grandes quantitÃ©s de spam Ã dâautres ordinateurs.

Pour accÃ©der au livre blanc de BitDefender, Â« **Conficker â Un an aprÃ¨s** Â». **Pour Ã©couter le podcast de Catalin Cosoi**, directeur des laboratoires de recherches BitDefender en anglais Â« **Conficker âOne year Ahead** Â»

Catalin Cosoi donne quelques conseils aux auditeurs pour maintenir leurs systÃ¨mes hors de portÃ©e de Conficker et des autres malwares.

En voici quelques uns :

â¢ Maintenez Ã jour votre systÃ¨me dâexploitation : tÃ©lÃ©chargez et installez les derniÃ¨res mises Ã jour de sÃ©curitÃ© ainsi que les outils de suppression de malwares et les patches ou correctifs disponibles.

â¢ Mettez Ã jour votre solution antimalware, votre pare-feu et votre filtre antispam aussi souvent que possible avec les derniÃ¨res dÃ©finitions de virus et les signatures de

fichiers/dâ□□applications suspects.

â□¢ Installez et activez une solution antimalware fiable et protÃ©gÃ©e par un mot de passe avec pare-feu, filtre antispam, et contrÃ´le parental

â□¢ Analysez rÃ©guliÃ¨rement votre systÃ¨me.

â□¢ Informez-vous au sujet des e-menaces et de la sÃ©curitÃ© informatique.

Ã□ propos de BitDefenderÂ®

BitDefender est la sociÃ©tÃ© crÃ©atrice de lâ□□une des gammes de solutions de sÃ©curitÃ© la plus complÃ¨te et la plus certifiÃ©e au niveau international reconnue comme Ã©tant parmi les plus rapides et les plus efficaces du marchÃ©. Depuis sa crÃ©ation en 2001, BitDefender nâ□□a cessÃ© dâ□□Ã©lever le niveau et dâ□□Ã©tablir de nouveaux standards en matiÃ¨re de protection proactive des menaces. Chaque jour, BitDefender protÃ¨ge des dizaines de millions de particuliers et de professionnels Ã travers le monde â□□ en leur garantissant une utilisation sereine et sÃ©curisÃ©e de lâ□□univers informatique. Les solutions de sÃ©curitÃ© BitDefender sont distribuÃ©es dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiÃ©s. Dans les pays francophones, BitDefender est Ã©ditÃ© en exclusivitÃ© par Ã□ditions Profil.

Pour plus dâ□□informations

Ã□ propos des Editions Profil

Editions Profil, sociÃ©tÃ© indÃ©pendante crÃ©Ã©e en 1989, dÃ©veloppe, Ã©dite et diffuse des logiciels sur diffÃ©rents secteurs dâ□□activitÃ©s, professionnel et grand public. Lâ□□Ã©diteur a constituÃ© un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivitÃ©. Editions Profil sâ□□est plus particuliÃ¨rement spÃ©cialisÃ©e ces derniÃ¨res annÃ©es dans l'Ã©dition et la distribution d'outils de sÃ©curitÃ© informatique et la protection des donnÃ©es en gÃ©nÃ©ral. Editions Profil Ã©dite notamment les solutions de sÃ©curitÃ© BitDefender et de contrÃ´le parental Parental Filter 2, ainsi que les solutions Farstone et diffuse les solutions de rÃ©cupÃ©ration de donnÃ©es et de gestion de serveurs MS Exchange de Kroll-Ontrack.