

BitDefender, Faux Upgrade Advisor Windows7, Vrai Trojan

S curit 

Post  par : JerryG

Publi e le : 11/5/2010 15:00:00

Un message d  « aide  » propose aux destinataires de v rifier la **compatibilit  de leur PC avec Windows  7** en t  chargeant et en ex cutant une version modifi e du logiciel Windows  7 Upgrade Advisor, qui contient **un cheval de Troie**

Les cybercriminels sont r put s pour leur propension   exploiter l  nt r t pour les nouveaut s technologiques. Les syst mes d exploitation et leurs d veloppements r cents servent ainsi souvent d  app ts, permettant de g n rer des gains illicites.

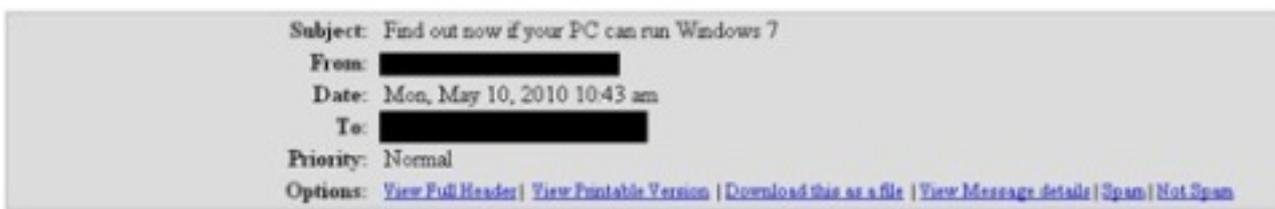


Windows  7, la derni re version de Microsoft   Windows  sortie en octobre 2009, ne pouvait pas  chapper longtemps aux cr ateurs de malwares qui profitent de l  impatience des utilisateurs   l  installer sur leur PC.

Ce type de   r ssite   ne peut d pendre uniquement du facteur chance, un peu d organisation est n cessaire. Voici le mode op ratoire mis en place par les cybercriminels cette fois-ci : un e-mail offre une    aide d sint ress e  » aux utilisateurs de Windows et leur recommande de t  charger Windows  7 Upgrade Advisor. Ce logiciel doit leur permettre de savoir si les ressources de leur syst me sont suffisantes pour installer le nouveau syst me d exploitation. Pour cela, il leur suffit d  ouvrir le fichier .zip en pi ce jointe.

Fig. 1 L  e-mail invitant   v rifier la compatibilit  avec Windows  7

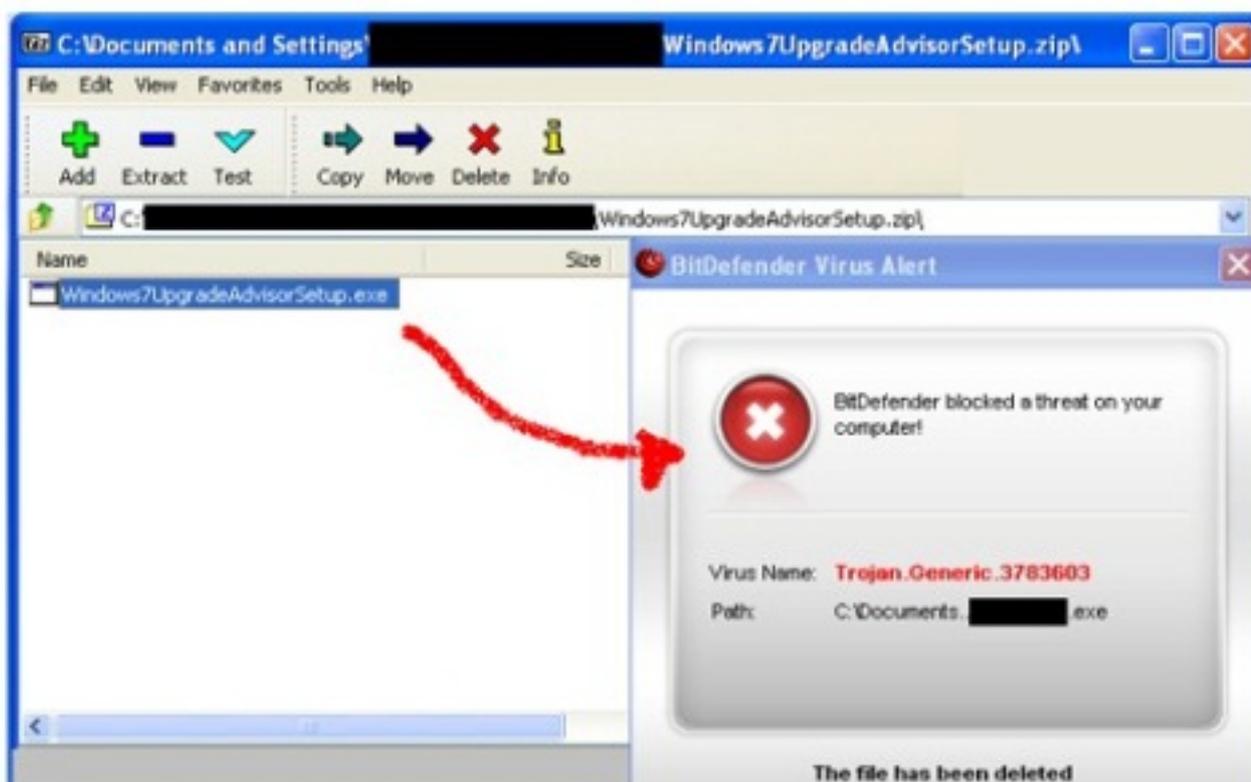
Cependant, le fichier zip ne contient pas l  outil de v rification de compatibilit  en question mais le Trojan.Generic.3783603. Ce malware contient des logiciels malveillants ou potentiellement ind sirables qu  il d pose et installe sur le syst me. Souvent, il installe une backdoor qui permet un acc s distant et clandestin au syst me infect .



Cette porte d'entrée peut ensuite être utilisée par des cybercriminels pour télécharger et installer d'autres logiciels malveillants ou potentiellement indésirables sur l'ordinateur compromis.

Fig. 2 Détection de Trojan.Generic.3783603

Les taux d'infection relevés par le Système de Reporting des Virus en Temps Réel de BitDefender indiquent une diffusion massive de Trojan.Generic.3783603. Bien que ce phénomène ne soit tout récent, il semble que ce ne soit qu'une question de temps avant que les cybercriminels ne prennent le contrôle d'un nombre élevé de machines. Les taux d'infection devraient également augmenter fortement en raison de l'augmentation de l'ingénierie sociale de ce mécanisme, en l'occurrence la référence au système d'exploitation de Microsoft Windows extrêmement populaire.



Afin de profiter d'Internet en toute sécurité, **BitDefender vous recommande de ne jamais ouvrir les pièces jointes** envoyées par des personnes inconnues, et d'installer et de mettre à jour une solution antimalware complète. Pour ne pas prendre de risque, veuillez télécharger le logiciel dont vous avez vraiment besoin depuis le site web officiel de son éditeur.

Tous les noms de produits et d'entreprises mentionnés dans ce document le sont à titre

purement informatif et sont la propriété, et éventuellement les marques, de leurs propriétaires respectifs.

[Pour plus d'informations concernant les produits BitDefender](#)