BitDefender : Hacker ou ne pas Hacker les comptes MSN
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 2/6/2010 0:00:00

Une invitation envoyÃ©e en masse proposant un outil permettant de **pirater soi-mÃªme des comptes,** menace les utilisateurs de **Windows Live Messenger**

Cet e-mail, qui constitue la premiÃ¨re Ã©tape dâ□□un plan frauduleux de rÃ©cupÃ©ration de donnÃ©es, restera trÃ¨s probablement dans les archives de lâ□□histoire du cybercrime tant il Ã©claire sur le comportement humain. Suffit-il dâ□□affirmer que quelque chose est illÃ©gal, pour que personne ne le fasse, ou est ce le contraire ?

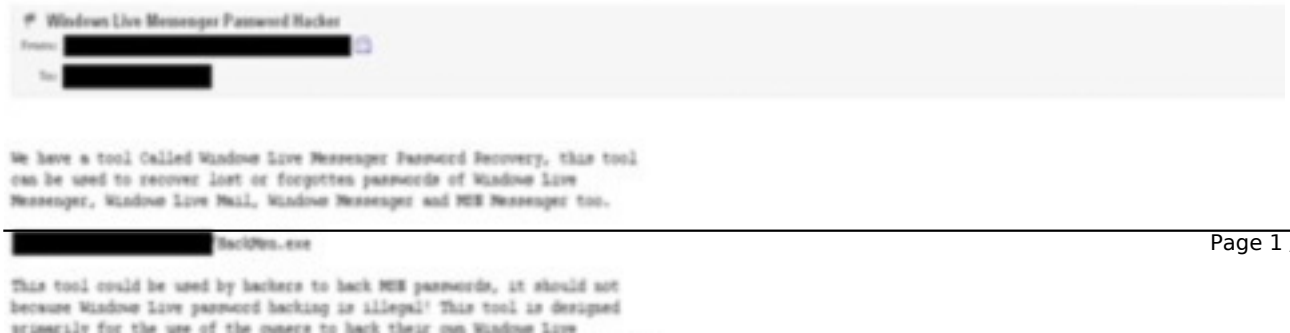
Câ□□est ainsi que le soi-disant outil sâ□□attribue une lÃ©gitimitÃ© bien fragile en affirmant : Â« *Cet outil pourrait Ãªtre employÃ© par des hackers pour pirater des mots de passe MSN, mais ne devrait pas Ãªtre utilisÃ© Ã ces fins car le piratage de mots de passe de Windows Live est illÃ©gal !* [â□¦] Â».

De mÃªme que les efforts du loup pour se faire passer pour une brebis dans la bergerie sont vains, cet outil affirme, sans convaincre, quâ□□il est destinÃ© aux Â« [â□¦] utilisateurs de MSN souhaitant pirater leurs propres comptes MSN [â□¦] Â» et aux Â« chercheurs Â».

Fig. 1 Le message initial appelant Ã la confiance sous prÃ©texte quâ□□il vous met en garde contre les pirates !

La logique de ce message est toutefois dÃ©routante. La rÃ©fÃ©rence finale Ã lâ□□outil pouvant Ãªtre utilisÃ© dans des situations oÃ¹ il est possible Â« de se connecter sans avoir Ã saisir son mot de passe Â» ajoute Ã son cÃ´tÃ© surnaturel.

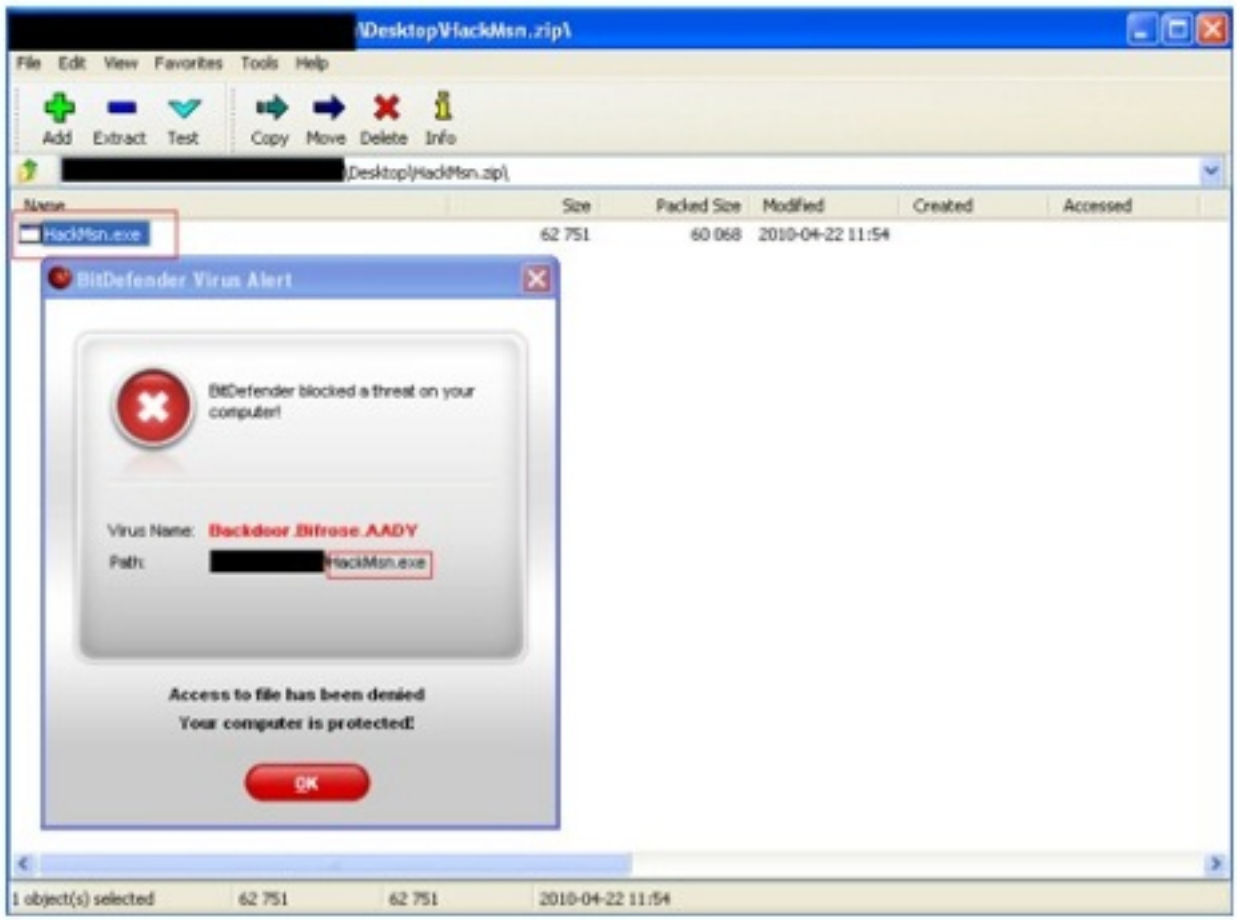
Lâ□□analyse approfondie du sens des e-mails que vous recevez nâ□□est sans doute pas votre passe temps favori, mais prÃ©tendre que lâ□□on souhaite faciliter la rÃ©cupÃ©ration de mots de passe perdus devrait prÃªter Ã sourire dans un contexte oÃ¹ lâ□□on nâ□□est jamais trop prudent face au risque de vol de donnÃ©es.



A ce stade seules des versions anglaises ont Ã©tÃ© dÃ©tectÃ©es ce qui les rend assez facile Ã Ã©viter, mais il est probable que des dÃ©clinaisons dans dâ□□autres langues de cette Â« campagne Â» suivent sous peu.

Lâ□□analyse de lâ□□e-mail mise Ã part, le lien fourni dans le message est censÃ© permettre de tÃ©lÃ©charger lâ□□outil promis. Et câ□□est Ã ce moment que HackMsn.exe rÃ©vÃ¨le qui il est rÃ©ellement : une backdoor.

Fig. 2. La backdoor dÃ©couverte par les Laboratoires BitDefender



IdentifiÃ© par BitDefender sous le nom de Â« **Backdoor.Bifrose.AADY** Â», ce code malveillant affecte les plateformes Windows. Le malware sâ□□injecte dans le processus explorer.exe et ouvre une backdoor qui permet aux pirates dâ□□accÃ©der au systÃ¨me et dâ□□en prendre le contrÃ´le. Backdoor.Bifrose.AADY tente Ã©galement de lire les clÃ©s et les numÃ©ros de sÃ©rie de plusieurs logiciels installÃ©s sur lâ□□ordinateur affectÃ©, enregistre les mots de passe dâ□□ICQ, de Messenger, des comptes de courrier Ã©lectronique POP3, et essaie d'accÃ©der aux sauvegardes protÃ©gÃ©es.

Une solution de sÃ©curitÃ© Ã jour et une bonne vigilance de la part des utilisateurs sera le meilleur obstacle Ã la diffusion de ce type de malware.

Pour plus dâ□□informations concernant **les produits BitDefender**