Communiqué de presse

À Montrouge, le mardi 1 juin 2010

Hacker ou ne pas Hacker les comptes MSN

Une invitation envoyée en masse proposant un outil permettant de pirater soi-même des comptes, menace les utilisateurs de Windows Live Messenger

Cet e-mail, qui constitue la première étape d'un plan frauduleux de récupération de données, restera très probablement dans les archives de l'histoire du cybercrime tant il éclaire sur le comportement humain. Suffit-il d'affirmer que quelque chose est illégal, pour que personne ne le fasse, ou est ce le contraire ? C'est ainsi que le soi-disant outil s'attribue une légitimité bien fragile en affirmant : « Cet outil pourrait être employé par des hackers pour pirater des mots de passe MSN, mais ne devrait pas être utilisé à ces fins car le piratage de mots de passe de Windows Live est illégal ! […] ».

De même que les efforts du loup pour se faire passer pour une brebis dans la bergerie sont vains, cet outil affirme, sans convaincre, qu'il est destiné aux « […] utilisateurs de MSN souhaitant pirater leurs propres comptes MSN […] » et aux « chercheurs ».

Fig. 1 Le message initial appelant à la confiance sous prétexte qu'il vous met en garde contre les pirates !

La logique de ce message est toutefois déroutante. La référence finale à l'outil pouvant être utilisé dans des situations où il est possible « de se connecter sans avoir à saisir son mot de passe » ajoute à son côté surnaturel. L'analyse approfondie du sens des e-mails que vous recevez n'est sans doute pas votre passe temps favori, mais prétendre que l'on souhaite faciliter la récupération de mots de passe perdus devrait prêter à sourire dans un contexte où l'on n'est jamais trop prudent face au risque de vol de données. A ce stade seules des versions anglaises ont été détectées ce qui les rend assez facile à éviter, mais il est probable que des déclinaisons dans d'autres langues de cette « campagne » suivent sous peu.

L’analyse de l’e-mail mise à part, le lien fourni dans le message est censé permettre de télécharger l’outil promis. Et c’est à ce moment que HackMsn.exe révèle qui il est réellement : une backdoor.

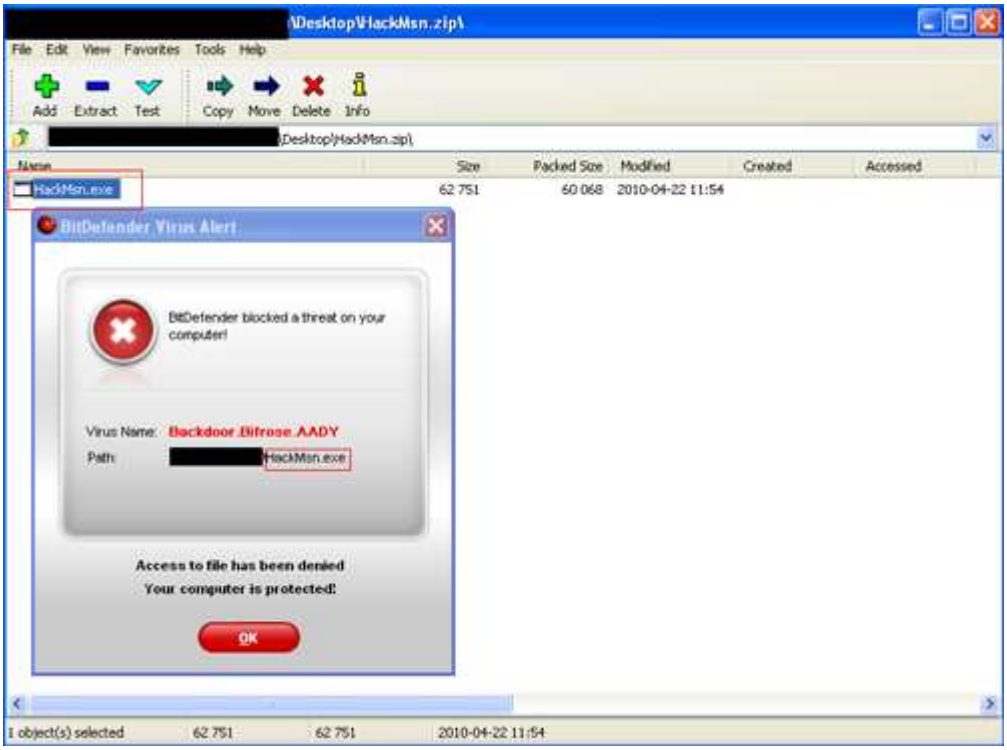

Fig. 2. La backdoor découverte par les Laboratoires BitDefender

Identifié par BitDefender sous le nom de « Backdoor.Bifrose.AADY », ce code malveillant affecte les plateformes Windows. Le malware s’injecte dans le processus explorer.exe et ouvre une backdoor qui permet aux pirates d’accéder au système et d’en prendre le contrôle. Backdoor.Bifrose.AADY tente également de lire les clés et les numéros de série de plusieurs logiciels installés sur l’ordinateur affecté, enregistre les mots de passe d’ICQ, de Messenger, des comptes de courrier électronique POP3, et essaie d'accéder aux sauvegardes protégées.

Une solution de sécurité à jour et une bonne vigilance de la part des utilisateurs sera le meilleur obstacle à la diffusion de ce type de malware.

Pour plus d’informations concernant les produits BitDefender, vous pouvez consulter www.BitDefender.fr et pour retrouver BitDefender en ligne et rester au fait de l’actualité des e-menaces :

- Flux RSS
- Facebook
- Twitter
- La communauté Malwarecity

À propos de BitDefender®

*BitDefender est la société créatrice de l'une des gammes de **solutions de sécurité** les plus complètes et les plus certifiées au niveau international, reconnues comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les **solutions de sécurité** BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont disponibles via le **Centre de presse**. Retrouvez également sur le site **www.malwarecity.fr** les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.*

À propos des Editions Profil

Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et de contrôle parental Parental Filter 2, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.