SÃ©curitÃ© : ESET, 7 rÃ¨gles de sÃ©curitÃ© pour sa messagerie instantanÃ©e
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 29/11/2010 13:30:00

ESET, spÃ©cialiste de la conception et du dÃ©veloppement de logiciels de sÃ©curitÃ©, annonce avoir identifiÃ© il y a quelques jours, un ver informatique inconnu qui a contraint Microsoft Ã suspendre temporairement les liens actifs dans **Live Messenger 2009** afin d'Ã©viter la propagation de ce ver particuliÃ¨rement agressif.

La messagerie instantanÃ©e est une voie trÃ¨s efficace pour permettre aux malwares de rester actif et de perdurer. Et, pendant ce temps, les cybercriminels perfectionnent leurs techniques pour leurrer les victimes potentielles afin de les entraÃ®ner Ã visiter des hyperliens malveillants.

Â« *C'est une mesure Ã©tonnante de la part de Microsoft car la diffusion de vers, Ã travers la messagerie instantanÃ©e (IM), tel que Skype, Yahoo!, Messenger et Microsoft Live Messenger, ne constitue pas une nouveautÃ©. Par exemple, le vers AimVen a Ã©tÃ© dÃ©couvert en 2003 et visait la plate-forme America Online Instant Messenger,* Â» commente **Pierre-Marc Bureau**, senior analyste chez ESET, qui vient rÃ©cemment de s'exprimer sur le thÃ¨me "Best Newcomer in the Antivirus industry" lors du Virus Bulletin Conference 2010 qui s'est tenu Ã Vancouver au Canada.

Â« *La faÃ§on d'opÃ©rer de ce type d'attaque est simple,* Â» explique **Pierre-Marc Bureau.** Â« *Tout d'abord la victime reÃ§oit un message qui contient un hyperlien de l'un de ses contacts, puis il clique dessus et il est ainsi infectÃ©.* Â» Le ver peut Ã©galement employer la gÃ©o-localisation afin d'utiliser la langue de la victime et associer ainsi des nouvelles ou Ã©vÃ¨nements relatifs au pays de cette victime afin de tromper sa vigilance. Ces techniques sophistiquÃ©es peuvent duper mÃªme les utilisateurs les plus prudents.

Les fonctions de suppression de donnÃ©es Ã distance ou de vÃ©rification de la carte SIM, en cas de vol d'appareils notamment, seront particuliÃ¨rement apprÃ©ciÃ©es par les responsables de la sÃ©curitÃ© des systÃ¨mes d'information d'entreprises (RSSI).

ESET a Ã©tabli sept rÃ¨gles d'or de sÃ©curitÃ© lorsque l'on utilise la messagerie instantanÃ©e :

1. Le fait d'ouvrir des images, tÃ©lÃ©charger des fichiers ou cliquer sur des liens devrait Ãªtre Ã©vitÃ© Ã tout prix lorsque l'on ne connaÃ®t pas la source. N'ouvrez pas de fichiers suspicieux ou de liens mÃªme s'ils viennent de vos connaissances, essayez de vÃ©rifier avec la personne concernÃ©e, l'origine de la piÃ¨ce jointe.

2. Ne rÃ©pondez pas aux messages de personnes que vous ne connaissez pas. Si quelqu'un que vous n'identifiez pas vous envoie une demande pour s'enregistrer dans vos contacts, refusez-la si vous n'Ãªtes pas certain de l'identitÃ© du contact.

3. Des messages non dÃ©sirÃ©s doivent Ãªtre bloquÃ©s - le blocage du Spam ou de messages provenant de personnes inconnues peut facilement Ãªtre Ã©vitÃ©. La plupart des logiciels de messagerie instantanÃ©e proposent de crÃ©er sa propre liste de contacts.

4. Ne pas dÃ©poser d'informations sensibles ou privÃ©es dans la messagerie instantanÃ©e, et notamment pour tout ce qui concerne les numÃ©ros de carte de crÃ©dit, des donnÃ©es bancaires, des mots de passe, ou encore des donnÃ©es qui vous identifient personnellement, comme des numÃ©ros de tÃ©lÃ©phone ou des adresses. Vous devriez Ã©galement Ã©viter de partager des informations sur vos contacts IM ou e-mail.

5. Votre messagerie instantanÃ©e devrait Ã©galement avoir un mot de passe non intuitif et diffÃ©rent de tous les autres employÃ©s sur de multiples connexions. Utilisez toujours des mots de passe diffÃ©rents pour chaque service en ligne. Ne rÃ©utilisez pas votre mot de passe. Si vous ouvrez une session sur un ordinateur partagÃ© ou dans un domaine public, assurez-vous que le dispositif de procÃ©dure de connexion automatique est bien contrÃ´lÃ©.

6. Ã□vitez des rencontres avec des inconnus que vous avez contactÃ©s en ligne Ã travers la messagerie instantanÃ©e. Si vous dÃ©cidez de rencontrer la personne dans la vraie vie, soyez trÃ¨s prudent, faites-vous accompagner par un proche.

7. Ã□teignez votre webcam, si vous ne l'utilisez pas, car certains malwares permettent Ã des criminels ou Ã des inconnus de vous espionner Ã travers votre propre webcam. Si vous avez une camera intÃ©grÃ©e, contrÃ´lez toujours si le voyant lumineux est bien Ã©teint quand vous ne l'utilisez pas.

Vous trouverez les solutions de protection Eset chez notre partenaire, **EptiSoft, le Magasin en ligne** spÃ©cialisÃ© dans la vente de produits dÃ©matÃ©rialisÃ©s et **c'est Ã cette adresse**

Â