# Un ver redoutable infecte la messagerie instantanée : ESET propose 7 règles de sécurité.

**Le 26 Novembre 2010**

**Les Pavillons-sous-Bois**le 26 novembre 2010, **ESET**, spécialiste de la conception et du développement de logiciels de sécurité, annonce avoir identifié il y a quelques jours, un ver informatique inconnu qui a contraint Microsoft à suspendre temporairement les liens actifs dans Live Messenger 2009 afin d'éviter la propagation de ce ver particulièrement agressif. La messagerie instantanée est une voie très 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 entraîner à visiter des hyperliens malveillants.

« C'est une mesure étonnante de la part de Microsoft car la diffusion de vers, à travers la messagerie instantanée (IM), tel que Skype, Yahoo!, Messenger et Microsoft Live Messenger, ne constitue pas une nouveauté. Par exemple, le vers AimVen a été découvert en 2003 et visait la plate-forme America Online Instant Messenger, » commente Pierre-Marc Bureau, senior analyste chez **ESET**, qui vient récemment de s'exprimer sur le thème "Best Newcomer in the Antivirus industry" lors du Virus Bulletin Conference 2010 qui s'est tenu à Vancouver au Canada.

« La façon d'opérer de ce type d'attaque est simple, » explique Pierre-Marc Bureau. « Tout d'abord la victime reçoit un message qui contient un hyperlien de l'un de ses contacts, puis il clique dessus et il est ainsi infecté. » « Le ver peut également employer la géo-localisation afin d'utiliser la langue de la victime et associer ainsi des nouvelles ou évènements relatifs au pays de cette victime afin de tromper sa vigilance. Ces techniques sophistiquées peuvent duper même les utilisateurs les plus prudents. alors primordiale dans un tel contexte. Les fonctions de suppression de données à distance ou de vérification de la carte SIM, en cas de vol d'appareils notamment, seront particulièrement appréciées par les responsables de la sécurité des systèmes d'information d'entreprises (RSSI).

**ESET a établi sept règles d'or de sécurité lorsque l'on utilise la messagerie instantanée :**

**1. Le fait d'ouvrir des images, télécharger des fichiers ou cliquer sur des liens devrait être évité à tout prix lorsque l'on ne connaît pas la source.**
N'ouvrez pas de fichiers suspicieux ou de liens même s'ils viennent de vos connaissances, essayez de vérifier avec la personne concernée, l'origine de la pièce jointe.

**2. Ne répondez 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'êtes pas certain de l'identité du contact.

**3. Des messages non désirés doivent être bloqués.**
le blocage du Spam ou de messages provenant de personnes inconnues peut facilement être évité. La plupart des logiciels de messagerie instantanée proposent de créer sa propre liste de contacts.

**4. Ne pas déposer d'informations sensibles ou privées dans la messagerie instantanée,**
et notamment pour tout ce qui concerne les numéros de carte de crédit, des données bancaires, des mots de passe, ou encore des données qui vous identifient personnellement, comme des numéros de téléphone ou des adresses. Vous devriez également éviter de partager des informations sur vos contacts IM ou e-mail.

**5. Votre messagerie instantanée devrait également avoir un mot de passe non intuitif et différent de tous les autres employés sur de multiples connexions.**
Utilisez toujours des mots de passe différents pour chaque service en ligne. Ne réutilisez pas votre mot de passe. Si vous ouvrez une session sur un ordinateur partagé ou dans un domaine public, assurez-vous que le dispositif de procédure de connexion automatique est bien contrôlé.

**6. Évitez des rencontres avec des inconnus que vous avez contactés en ligne à travers la messagerie instantanée.**
Si vous décidez de rencontrer la personne dans la vraie vie, soyez très prudent, faites-vous accompagner par un proche.

**7. Éteignez votre webcam, si vous ne l'utilisez pas,**
car certains malwares permettent à des criminels ou à des inconnus de vous espionner à travers votre propre webcam. Si vous avez une camera intégrée, contrôlez toujours si le voyant lumineux est bien éteint quand vous ne l'utilisez pas.

**A propos d'ESET**

La société ESET est spécialisée dans la conception et le développement de logiciels de sécurité offrant une protection globale contre les menaces évolutives qui sévissent dans les environnements informatiques. Pionnier en matière de détection proactive des menaces, ESET est aujourd'hui le leader dans ce domaine. ESET a développé un vaste réseau mondial de partenariats, y compris avec des entreprises telles que Canon, Dell et Microsoft. ESET possède des bureaux à Bratislava (Slovaquie), Bristol (Royaume-Unis), Buenos Aires (Argentine), San Diego (USA), Prague (République Tchèque), et est représenté dans plus de 110 pays. Pour plus d'informations, veuillez visiter les sites Internet :www.eset-nod32.fr ou www.athena-gs.com