Une mise à jour douteuse dans un e-mailing!

3 - les News

Publié par: RédacChef

Publié le : 21/10/2005 19:10:00

S'agit-il

d'une

faille de

sécurité ?

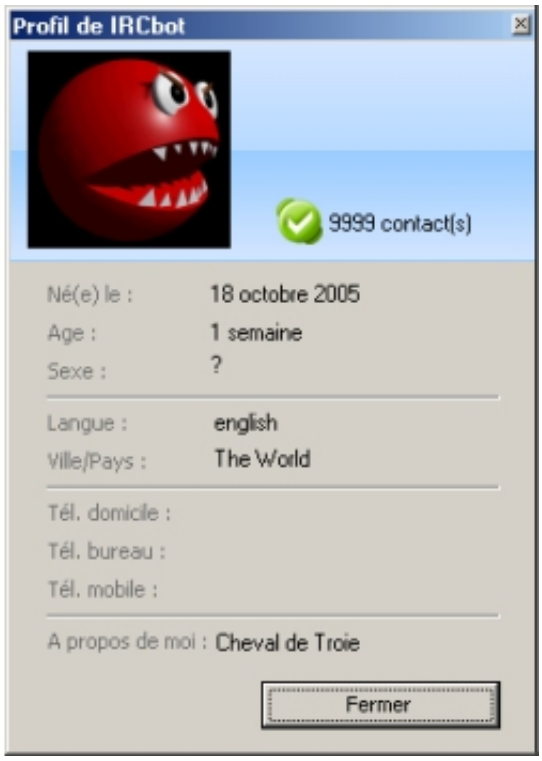
Cette semaine, dans notre forum, nous avons commenté la distribution d'un courrier suspect avec l'entête de Skype. Doit-on conclure à une faiblesse de la sécurité Skype? La réponse est NON ! Le code malware qui accompagne ce courrier n'exploite aucune faille de sécurité du logiciel Skype.

La popularité du logiciel Skype avec plus de 50 millions d'utilisateurs en fait une cible potentielle pour les créateurs malveillants de code viral. Aucun système n'est sécurisé à 100%, cependant, il faut reconnaître que le programme Skype est plutôt bien verrouillé et si vous désirez en savoir davantage vous pouvez consulter le Centre de Sécurité Skype. Certains concepteurs de programmes malveillants préfèrent donc se servir de la forte notoriété de Skype plutôt que de rechercher une faiblesse sécuritaire dans le code de Skype. Dès lors, le maillon faible dans la chaîne de sécurité, c'est l'utilisateur lui-même.

Les éditeurs n'envoient jamais de mises à jour par pièce-jointe dans un email ! Qu'on se le dise !

Ce malware utilise un e-mailing avec une usurpation d'identité de l'expéditeur. Ce genre de procédé n'est pas nouveau .... Il existait déjà depuis longtemps avec les identités empruntées de Microsoft, Norton, IBM, Kapersky et d'autres marques mondialement connues ... La seule nouveauté, c'est l'utilisation du nom de Skype cette fois-ci. Si l'on tente d'ouvrir la pièce jointe, une fenêtre apparaît avec un message *Installation error* ou *The file could not be opened*. C'est un leurre pour faire croire que rien ne s'est passé. En fait le cheval de Troie est bien installé dans le répertoire du système

avec un fichier *remote.exe*, et aussi dans la base de registre. Il s'agit d'un code troyen connu Fanbot ou IRCbot.
voir le site Sophos.



Jaanus, responsable du blog Skype disait:

(traduction de notre rédaction)

" *Skype n'envoie jamais des mises à jour de logiciel par e-mail. Nous envoyons seulement des informations concernant vos commandes si vous avez acheté quelque chose chez nous et aussi si vous avez opté pour recevoir les e-mail de Skype ..., nous envoyons des circulaires et des invitations d'études. Mais c'est tout! Ainsi si vous recevez un e-mail de mise à jour du logiciel Skype, effacez-le SVP et dites aux autres de faire de même.*

Skype utilise des signatures électroniques pour aider les utilisateurs à vérifier la validité des mises à jour. Vous pouvez vérifier l'authenticité du logiciel Skype confirmant que sa signature électronique est valide. Les instructions pour vérifier la signature électronique du logiciel Skype sont décrites dans le Guide de l'Administrateur de Skype."

Néanmoins, si vous détectez un évènement douteux dans le logiciel Skype, vous pouvez faire votre rapport au Centre de Sécurité Skype :

security@skype.net