Skype recueillait des informations sur les PC de ses utilisateurs à leur insu

- Informatique - Sécurité Informatique -

Date de mise en ligne : dimanche 4 mars 2007

L'éditeur du logiciel voix sur IP a reconnu qu'il prélevait le numéro de série de la carte mère du PC des utilisateurs. Il a mis fin à cette pratique.

Skype s'est rapidement imposée comme la solution de téléphonie Internet (VoIP) la plus populaire. L'éditeur affiche désormais plus de 170 millions d'inscrits à son service. Et ce malgré les inquiétudes sur une "boîte noire".

Les protocoles de communication de Skype sont en effet cryptés selon des algorithmes secrets et les spécialistes ne peuvent vérifier l'existence de porte dérobée volontaire ou non qui permettrait un espionnage des utilisateurs. A tel point qu'en 2005, le ministère délégué à l'Enseignement Supérieur et à la Recherche a décidé d'interdire le logiciel de téléphonie dans les universités et centres R&D qui lui sont rattachés.

Ce n'est pas la découverte révélée début février par le blog Pagetable.com dans la version de Skype diffusée depuis décembre 2006 qui va rassurer les internautes. A l'origine, une simple erreur d'exécution du fichier 1.com de Skype sous la version 64 bits de Windows.

Intrigué, un informaticien a analysé ce fichier avec un débogueur (logiciel permettant de suivre à la loupe le déroulement d'un programme au coeur de la machine) et s'aperçoit que le contenu du BIOS du PC, dont le numéro de série de la carte mère habituellement, est lu par Skype. Voilà qui tombe mal pour la société qui affiche sur la page d'accueil de son site Internet "No Spyware - Adware - Malware" (pas de logiciel d'espionnage, de publicité intrusive ou de logiciels malveillants).

La faute à un plug-in d'un éditeur tiers

Dans une contribution sur son blog en date du 8 février (et réactualisé le 9 février), Kurt Sauer, directeur de la sécurité de Skype (Chief Security Officer), rejette la faute sur un plug-in développé par un éditeur tiers du nom d'Easybits qui "inclut une forme de gestion des droits numériques [...] et qui tente d'identifier de manière unique sur quel ordinateur physique il est en train de tourner."

Toujours selon le Mr Sécurité de Skype, "c'est assez normal de regarder les données qui permettent d'identifier de façon unique une plate-forme et il n'y a rien de secret à lire les paramètres du matériel depuis le BIOS". Le réprésentant de l'éditeur précise : "Les appels de fonction pour lire le BIOS sont publics et sont accessibles à tout logiciel fonctionnant sur votre ordinateur."

Sauf que la plupart des logiciels installés sur un ordinateur ne sont généralement pas des outils de communication se servant d'Internet. Pis, il est difficile de contrôler le trafic de Skype qui, aux yeux d'un administrateur informatique, utilise le même canal qu'un surf sur le Web pour contourner les pare-feux.

Une nouvelle version qui ne lit plus les données BIOS

Skype tente de rassurer : "En adéquation avec nos accords sur la confidentialité, Skype n'accède pas à ces informations. Elles ne sont utilisées que par le logiciel EasyBits pour s'assurer que l'utilisation du plug-in est conforme."

Et si ce n'était pas suffisant, le société Skype justifie un " dysfonctionnement" avec ses nouvelles plates-formes pour mettre à disposition une nouvelle version "qui ne lit plus les données inscrites sur le BIOS". Mais les doutes subsistent : y-a-t-il d'autres données prélevées par Skype à l'insu de ses utilisateurs ?

Certaines sociétés préféreront donc opter pour un logiciel VoIP dont le statut open source permet de vérifier les flux de données échangés avec les correspondants. De son côté, avec beaucoup d'opportunisme, la société Arkoon, qui fabrique des solutions de protection des réseaux des entreprises, avait émis mi-férier un communiqué dans lequel elle mettait en avant ses appliances FAST360 permettant de bloquer le trafic de Skype et assimilés.

Post-scriptum :

http://www.vnunet.fr/fr/vnunet/news...