

Extrait du Spyworld Actu

<http://mail.spyworld.fr/spip.php?article6189>

Le chiffrement de Skype résiste à la police allemande

- Renseignement - International -



Date de mise en ligne : vendredi 23 novembre 2007

Spyworld Actu

La police allemande s'est dite incapable de déchiffrer le chiffrement utilisé dans le client VoIP Skype, ce qui l'empêche de surveiller les appels des criminels potentiels et des terroristes.

Pour rappel, Skype est un logiciel de téléphonie IP permettant à ses utilisateurs de passer des appels gratuits de PC à PC ou bien payants vers des lignes fixes, tout en restant sur son ordinateur. D'après Joerg Ziercke, président de la BKA (Police Fédérale allemande), " le chiffrement avec ce logiciel de téléphonie IP... nous pose des difficultés ".

" Nous ne pouvons le décrypter. C'est pourquoi nous envisageons de surveiller la source des télécommunications - c'est-à-dire aller à la source avant le chiffrement ou après son déchiffrement. ", a déclaré Ziercke. Les experts informatiques ont déclaré que les communications sur Skype et sur les autres logiciels se basant sur la VoIP (voice over internet protocol, voix sur IP) étaient difficiles à intercepter car ils fonctionnent par la fraction des données voix par de petits paquets en les faisant transiter à travers des milliers de tuyaux au lieu de les faire circuler d'un point à un autre, ont indiqué les autorités allemandes. Skype s'appuie en effet sur la technologie peer-to-peer afin d'acheminer les communications.

Pour l'heure, l'Allemagne n'a pas encore demandé à Skype de divulguer des informations sur les clés du chiffrement des télécommunications entre ses membres ni de laisser des portes dérobées pour les organes du gouvernement. Pour autant, il s'agit selon Ziercke d'un besoin essentiel pour les autorités policières allemandes de pouvoir rechercher en ligne les ordinateurs de terroristes potentiels et les infecter d'un logiciel espion, [ce dont nous vous parlions dans une précédente actualité.](#)

Cette décision n'est pas vraiment bien vue outre-Rhin, des inquiétudes naissant quant à la fréquence de l'utilisation de tels procédés pour tracer le terrorisme, ce à quoi Ziercke a répondu que ce ne serait utilisé qu'en de rares exceptions.

Post-scriptum :

<http://www.generation-nt.com/skype-...>