Alerte : un trojan sème la discorde sur Live Messenger

D'après l'éditeur de sécurité Aladdin, déjà près de **11.000 PC** ont été touchés par ce maudit canasson qui a le don de se propager sur la Toile au triple galop.

Ce spécialiste de la mutation est un Bot IRC qui se diffuse en proposant le téléchargement d'un fichier ZIP. Selon l'éditeur, la menace est encore très sérieuse, et à l'écriture de ce papier, elle continue de grossir heure après heure.

Sa force est la duperie. Il propose en effet à un contact une image qui en réalité contient le code malveillant. Mais le fichier provenant d'une source qui est en apparence fiable, la majorité des utilisateurs ont la fâcheuse tendance à l'accepter.

Pourtant, il faut rappeler qu'il s'agit d'un comportement à risque, et il vaut mieux vérifier à deux fois avant d'accepter, par exemple en passant un rapide coup de téléphone à l'expéditeur. Il est également recommandé par Microsoft de régulièrement changer son mot de passe.

Un Trojan qui fonctionne comme un couteau suisse

Le fichier utilisé est une nouvelle forme de trojan IRC (Internet Relay Chat) qui a commencé à se diffuser le dimanche 18 novembre et qui en l'espace de trois jours a déjà contaminé près de 11.000 machines.

Il est utilisé par les hackers pour agrandir leurs réseaux de machines zombies puisqu'il a la capacité de se propager à l'ensemble des contacts de la première cible.

Ces attaques sont coordonnées par un channel IRC qui totalise 500 commands bots (toutes sont des machines zombies!) sur lequel les ingénieurs d'eSafe (le laboratoire de Aladdin) ont placé des sondes.

Précisons que le fichier utilisé dans ces attaques est un document compressé en .zip. Il utilise différents noms qui font référence à des photos. Le code malveillant une fois installé a pour mission de scanner d'autres programmes afin de trouver de nouvelles cibles.

Si ce genre d'attaque n'est pas nouveau -puisque le vecteur est une solution de messagerie instantanée en l'occurrence Windows Live Messenger- il a la capacité de scanner les réseaux de machines virtuelles.

Ce cheval de Troie a d'ailleurs été baptisé *« le couteau suisse pour cybercriminels »* par Aladdin, une métaphore de « génie »…