07 juillet 2011
Protégez-vous

Attention au pire virus informatique de l'histoire

Kaspersky Labs vient d'annoncer la découverte du virus le plus dangereux de l'histoire. Qualifié d'«indestructible», il aurait déjà infesté 4,5 millions d'ordinateurs. Les conseils de sécurité de l'un des responsables de Kaspersky.

Avec Nicolas Brulez

Atlantico : Kaspersky Labs vient d'annoncer la découverte du plus grand virus de l'histoire : s'agit-il d'une exagération ?

Nicolas Brulez : Il y a eu beaucoup d'interprétations de l'annonce de Kaspersky Lab.**TLD 4 est sans aucun doute un des programmes malveillants les plus complexes de l'histoire.** Il est très difficile à analyser. Dans notre annonce nous parlions « d'indestructivité ».

Le malware n'est pas « indestructible », mais le botnet est très difficile à éradiquer en partie à cause du Réseau Peer 2 Peer et du protocole chiffré utilisé pour communiquer avec les serveurs de contrôle.

De quel type de virus s'agit-il ?

TDL-4 est un logiciel malveillant de type « bootkit », qui est capable d'infecter ce que l'on appelle la « zone d'amorce » du disque dur : **lors du démarrage de l'ordinateur, le programme malveillant se lance avant le système d'exploitation, ce qui lui permet de rester invisible aux yeux de nombreuses applications de sécurité.**

L'une de ses spécificités réside dans le fait qu'il fonctionne aussi sous les systèmes d'exploitation 64 bits, jusqu'à présent considérés comme sécurisés contre ce genre de virus.

Le TDL4 utilise un protocole chiffré pour communiquer avec les serveurs des personnes qui le contrôlent, mais il utilise surtout **le réseau Peer 2 peer KAD [*qu'utilisent la plupart des logiciels de téléchargement illégal populaires, ndlr*] pour infecter d'autres ordinateurs distants.**

A quoi sert-il ?

Sa finalité est la génération de clics sur des bannières publicitaires afin de générer de l'argent pour ses créateurs.

Il peut également permettre aux pirates d'utiliser les ordinateurs infectés comme « proxy », c'est-à-dire des ordinateurs « tampons » qui leur permettent d'agir sans dévoiler leur propre identité.

Enfin, les criminels peuvent être rémunérés au nombre d'installation de TDL4 à l'aide d'un système d'affiliation : **entre 20 et 200 dollars pour 1000 nouvelles victimes, en fonction de leur pays.**

Les utilisateurs français sont-ils menacés ?

De par les vecteurs d'infections massifs utilisés (sites pornographiques, d'hébergement de fichiers, de vidéos ou de cracks), les utilisateurs français sont aussi concernés.

Les pays europens rapportent beaucoup d'argent grâce aux programmes d'affiliation : c'est une motivation pour les criminels qui cherchent à optimiser les gains.

Comment se protéger ?

La protection de l'ordinateur commence par une bonne éducation des utilisateurs. Les comportements à risques tel que le téléchargement de cracks sont à proscrire. **Il est important de maintenir son système d'exploitation à jour, mais également les applications tierces** telles que le JAVA, le lecteur flash ou encore le lecteur PDF, qui sont responsables de nombreuses infections lors d'un surf classique (sites compromis, liens malveillants, etc.).

Il est bien sûr important de maintenir un antivirus à jour.

Enfin, un cas d'infection, il est possible de **télécharger gratuitement l'outil TDSS Killer, capable de détecter et d'éradiquer TDL4.**