Le malware TDL4 poursuit sa propagation

Selon le chercheur Nicolas Brulez de Kaspersky Labs, les internautes ont tout intérêt à prendre le téléchargement illégal avec des pincettes. Les amateurs de P2P pourraient voir leur machine infectée par TDL4, un malware difficilement détectable et qualifié d'indestructible. L'un des virus les plus coriaces de l'histoire informatique pourrait bientôt faire ses débuts dans l'Hexagone. Il succèderait à l'illustre I Love You, à Sasser ou encore au fameux virus pakistanais.

C'est ce que prétend un représentant de Kaspersky Labs. A en croire ses propos, TDL4, continue sa progression. Il s'est déjà « invité » sur près de 5 millions d'ordinateurs à travers le monde. De type bootkit, ce malware est d'autant plus difficile à éradiquer qu'il s'intègre au secteur d'amorçage du disque de démarrage. En d'autres termes, il est chargé en mémoire avant même le système d'exploitation, et réside tout au long du cycle de fonctionnement de la machine dans laquelle il s'est logé.

Invisible de la plupart des programmes, dont les antivirus, TDL4 s'exécute aussi bien sur des plateformes 32 bits que 64 bits, précise *ITespresso.fr*. Sa propagation s'effectue par la voie des réseaux P2P. Un protocole chiffré permet aux pirates de prendre un contrôle partiel des ordinateurs infectés. La véritable finalité de la démarche se cantonne toutefois à la génération de clics automatiques sur des bannières publicitaires. Une solution lucrative pour les créateurs de TDL4.

Au chapitre des recommandations émises par Kaspersky, l'éditeur rappelle de mettre à jour son OS, les composants tiers (Flash, Java…) et l'antivirus. Télécharger le patch TDSS Killer peut également résoudre le problème. Prévenir valant toujours mieux que guérir, l'éditeur de logiciels de sécurité recommande d'éviter les sites de vidéos, de cracks et de contenus pornographiques illégaux.