Les hackers prennent en otage le système de mise à jour de Microsoft

Les cybercriminels utilisent de façon détournée, le système de transfert de fichiers *« made in Redmond »* afin d'éviter les filtres des firewalls, annoncent des ingénieurs de Symantec…

Le BITS (ndlr : Background Intelligent Transfer Service) est utilisé par les OS de Microsoft pour délivrer correctement les patchs à ses clients. Ce système a fait ses premiers pas avec Windows XP, il est également présent dans Windows Serveur 2003 et Windows Vista.

Il s'agit d'un système de transfert de fichiers asynchrone. Les utilisateurs téléchargent les uns après les autres et si la connexion est coupée, ce système résume le téléchargement de façon automatique.

« Il s'agit d'un composant de l'OS très pratique et si l'on considère qu'il supporte le langage HTTP et qu'il peut également être programmé via COM API, il s'agit de l'outil parfait pour faire télécharger n'importe quoi, n'importe quand à Windows » déclare Elia Florio, ingénieur chez l'éditeur de sécurité. *« Y compris des fichiers malveillants ».*

D'après Florio, certains concepteurs de Trojan commencent à utiliser BITS pour télécharger du code sur un poste déjà infecté. *« Ils font cela pour une raison simple, BITS fait partie intégrante du système d'exploitation il est donc considéré comme fiable par le pare-feu qui le laisse agir à sa guise. »*

Les malwares, en particulier les Trojans, commencent par ouvrir une backdoor sur le PC cible de façon à pouvoir y injecter du code ou un keylogger. Pour cela, le cheval de Troie doit être en mesure de contourner le pare-feu. Généralement, les méthodes utilisées par ces malwares sont brutales et elles provoquent des alarmes.

« C'est ingénieux et nouveau », déclare Oliver Friedrichs, directeur du security response group de Symantec. *« Les attaquants détournent un composant de Windows pour éviter de se faire détecter par le pare-feu, c'est très malin et en même temps très dangereux . »*

« Utiliser BITS est totalement bénéfique pour les hackers qui savent qu'il s'agit d'un système fiable, gratuit, et qu'ils n'ont plus besoin d'écrire eux même le code pour la mise à jour des Trojans. »

Selon Florio : *« il est impossible d'empêcher l'utilisation de BITS dans la mesure ou il n'est pas facile de savoir ce que BITS peut ou ne peut pas télécharger. Il est probable qu'il faudrait rendre l'interface de BITS moins accessible. Ou du moins, il serait opportun de limiter le nombre d'URLs autorisées. »*