

Une « Backdoor » dans Windows 7 ?

Cela existe depuis 15 ans... à la demande de la NSA

Lundi 23 Novembre 2009



La NSA étatsunienne sait de quoi elle parle, en 1995, dans le cadre de la préparation des lois CDA et Network Surveillance, elle avait obtenu de Microsoft qu'ils intègrent une "porte dérobée" dans leur système d'exploitation afin de que les services secrets U.S. puissent venir fouiller dans l'ordinateur à distance et que la NSA puisse décoder la clé d'encryptage utilisée par l'utilisateur pour protéger ses communications.

A l'époque cette mesure était – déjà – justifiée au nom de la lutte contre le terrorisme... on traquait alors les « groupes miliciens » qui avaient soi-disant fait sauter le bâtiment fédéral de Oklahoma-City et voulaient assassiner Bill Clinton.

En 1998, à la conférence Crypto98, un groupe de chercheurs avait révélé que les DLL intitulés ADVAPI et NSAKKEY, installés par défaut dans toutes les copies de Windows, étaient en fait un « rootkit » de la NSA.

http://www.theforbiddenknowledge.com/hardtruth/nsa_backdoor_windows.htm

[Silicon.fr - 20/11/2009]

Après la [faille non-patchée](#) découverte sur Windows 7, cette fois un chercheur en sécurité de la très sérieuse NSA (National Security Agency) américaine explique que **l'OS de Microsoft n'est pas totalement sécurisé.**

Microsoft a donc réagi dans les colonnes de *Computerworld* en **réfutant l'idée de la présence de portes dérobées (backdoor)**. Une position qui n'étonne aucunement l'ensemble des chercheurs en sécurité. Cela étant, il serait plus qu'étonnant que Microsoft ait délibérément caché cette porte et engagé ainsi sa réputation.

Pour information, les portes dérobées sont un des moyens les plus utilisées par les cyber-espions. Ces derniers utilisent des chevaux de Troie appelés *trojans* qui permettent d'ouvrir des «portes de service» qui donnent accès aux données de l'ordinateur depuis l'extérieur.

Selon **Mikko Hyppönen**, directeur des laboratoires de recherche de F-Secure, il s'agit là du moyen principal de piratage. « *La porte de service se lance immédiatement et se cache dans le système, souvent à l'aide de techniques de*

*rootkits. Il établit une connexion depuis l'ordinateur infecté vers une adresse réseau spécifique située quelque part dans le monde. Avec l'aide de cette porte de service, le **cybercriminel accède aux informations situées sur l'ordinateur cible**, ainsi qu'aux informations situées dans le réseau local auquel la cible accède. »*

Ainsi la position extrême s'avère être celle de **se déconnecter du Web**, certains postes contenant des informations critiques. Une solution radicale... mais inapplicable aujourd'hui face à la réalité des besoins de communication en ligne.

http://www.silicon.fr/fr/news/2009/11/20/windows_7_embarque_t_il_une_porte_derobee

Source:<http://libertesinternets.wordpress.com>

Backdoor = Porte dérobée