Portes derobées

Dans un logiciel, une **Porte dérobée** est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel. L'introduction d'une porte dérobée dans un logiciel à l'insu de son utilisateur transforme le logiciel en cheval de Troie. (voir : Porte dérobée).

Pourquoi les éditeurs de logiciels privateurs implantent-ils des portes dérobées dans leurs logiciels ? Les objectifs sont multiples. Il y a :

- L'espionnage [1)]
- L'altération les données [2)]
- L'altération préférences de l'utilisateur [3)]
- L'installation, la suppression ou la désactivation des programmes [4)]
- L'acquisition du contrôle total (porte dérobée universelle) [5)], [6)]

Il y a encore d'autres raisons. Par exemple, l'implantation involontaire (faille de sécurité) ou pour des raisons encore inconnue.

Les éditeurs de logiciels privateurs utilise l'argument sécuritaire pour justifier l'implantation de ces portes dérobées. Hors, la présence même de ces portes dérobée est en soit une faille de sécurité et elles vous rendent, de facto, complètement vulnérable et démuni vis-à-vis de ces éditeurs.

Notes et références

- https://www.gnu.org/proprietary/proprietary-back-doors.fr.html sur les portes dérobées du logiciel privateur.
- **[en]** https://www.eff.org/deeplinks/2015/02/who-really-owns-your-drones pour d'autres exemples.

[1)], [5)]
En violation, selon les cas, aux articles 272, 273, 274 ou 301 du code pénal suisse - 311.0.
[2)], [3)], [4)], [6)]
En violation de l'art. 143bis du code pénal suisse - 311.0.