https://laurentbloch.org/BlogLB/Le-rootkit-de-Sony

Le rootkit de Sony

- Zinformatiques - Sécurité du système d'information -

Date de mise en ligne : mardi 14 mars 2006

Nous ne saurions entreprendre le tour d'horizon de la malfaisance informatique sans évoquer une affaire où le scandale le dispute au ridicule. Le 31 octobre 2005, le spécialiste reconnu des systèmes Windows Mark E. Russinovich publiait sous le titre Sony, Rootkits and Digital Rights Management Gone Too Far un article dans la revue en ligne Sysinternals où il racontait la mésaventure suivante.

Il testait sur son ordinateur le logiciel de détection d'intrusion *RootkitRevealer* (RKR). Un rootkit est un programme ou un ensemble de programmes qui permettent à un pirate de maintenir dans la durée un accès frauduleux à un système informatique, généralement par l'ouverture de portes dérobées et par des modifications vicieuses du système, et RKR est destiné à détecter de telles attaques.

Que révéla RKR à Russinovich ? un répertoire caché, plusieurs pilotes de périphériques cachés, et un programme caché. Russinovich, auteur notamment de l'ouvrage de référence *Windows internals : Windows 2000, Windows XP & Windows Server 2003* [1], n'est pas précisément un utilisateur naïf et il applique des règles de sécurité scrupuleuses. Étonné de se voir ainsi piraté, il mobilisa toute sa science des structures internes de Windows et des outils d'analyse pour percer ce mystère (les détails sont exposés dans l'article http://www.sysinternals.com/blog/20...), et quelle ne fut pas sa surprise en découvrant que le rootkit incriminé était un logiciel commercial arborant fièrement la marque de la compagnie qui l'avait développé, *First 4 Internet*. Cette compagnie avait créé un ensemble de logiciels destinés à implémenter une technologie nommée XCP, dont la fonction est d'exercer des contrôles d'accès sur les CD musicaux enregistrés du commerce selon les spécifications du protocole *Digital Rights Management* (DRM). *First 4 Internet* avait vendu sa technologie à plusieurs compagnies, dont Sony, et en constatant cela Russinovich se rappela avoir acheté peu de temps auparavant un CD Sony qui ne pouvait être joué qu'au moyen du logiciel inscrit sur le CD lui-même, et qui ne pouvait être recopié que trois fois. C'est ce que l'on appelle un CD au contenu protégé contre les copies.

En fait, lorsque le CD était joué sur un ordinateur, le logiciel inscrit sur le CD se recopiait dans le système, à l'insu de l'utilisateur. Une fois installé, il se comportait comme un logiciel espion, et envoyait à Sony l'identification du CD introduit dans le lecteur de l'ordinateur ; avec cet envoi , Sony était informé chaque fois qu'un CD donné était joué sur tel ou tel ordinateur, et recevait également l'adresse IP de cet ordinateur. De surcroît, ce logiciel assez mal conçu et réalisé créait dans le système des vulnérabilités supplémentaires qui facilitaient des attaques ultérieures par d'autres logiciels malfaisants. Clairement, le *Big Brother* du roman de George Orwell commençait à prendre réalité.

Mais le plus piquant (ou le plus scandaleux) de cette histoire, c'est que pour réaliser leur logiciel secret et malfaisant destiné à espionner leurs clients et à protéger de façon abusive leurs droits, *First 4 Internet* et son mandant Sony avaient purement et simplement piraté des parties de certains logiciels libres sous licence GPL dans des conditions contraires aux termes de cette licence, c'est-à-dire qu'ils n'avaient pas hésité à enfreindre les droits d'autrui.

---

[1] Mark E. Russinovich. Windows internals : *Windows 2000, Windows XP & Windows Server 2003*. Microsoft Press, Redmond, État de Washington, 2005.