Le système de DRM de Sony en question. Rootkit ou pas ?

Tout commence par un simple constat de notre casseur de DRM (Digital Right Management) Mark Russinovich, qui a malmené le système de protection contre la copie des derniers CD de Sony… Alors qu'un CD de Sony se lit correctement sur une platine, lorsque l'on essaie de les jouer sur un PC, un programme (Sony's CD Digital Media) se lance, obligeant l'utilisateur à lire le média sur un lecteur « bundle » ou « retail » de Sony qui restreint le nombre de copies possible. Dans les colonnes de « The Register », Mark Russinovich, explique qu'il considère le programme de Sony comme un « Root Kit » (RK). Et il justifie cette explication, du fait de la découverte d'un aspect particulièrement néfaste du programme de Sony. L'utilisation d'outils pour supprimer les protections de Sony peut entraîner le crash du lecteur CD, voire -pire- de faire de l'ordinateur une machine parfaitement inutile, si ce n'est pour décorer le salon. Dans ce dernier cas, la solution est de formater et de réinstaller le système. Dur, dur!. Alors, comme s'interroge non sans ironie Mark Russinovich, doit-on, considérer le programme de Sony comme un « Root Kit » ou bien comme une énième, vaine et risible tentative d'empêcher l'utilisateur de jouer des médias sur son ordinateur? Pour lui, la réponse est oui. Une opinion que ne partage pas les spécialistes de la sécurité de nos confrères de « Vulnerabilite.com » : « Le logiciel utilise des techniques de rootkit pour se dissimuler sur la machine mais il n'est en aucun cas malicieux et il ne s'agit donc pas d'un RK. » Alors « Root Kit » ou pas? Généralement, on utilise ce terme de Root kit (RK) pour désigner un code malicieux utilisé par les « Black Hackers » et visant à prendre le contrôle d'un système en toute discrétion. Mais pas seulement comme le précise nos confrères de Vulnerabilite.com : « La fonction principale du RK est de simplifier, voire automatiser, la mise en place d'une ou plusieurs backdoors ». Il existe donc depuis belle lurette dans l'univers de l'informatique. Un « Root Kit » a plusieurs caractéristiques : -Il sert à installer une ou plusieurs portes dérobées (généralement très stealth) sur un système déjà piraté. -Il se comporte de façon à rester indétectable -Et enfin, dernier volet de son action, il intercepte des routines pour les remplacer par les siennes ou remplace les exécutables d'un système par les siens. Selon Vulnerabilite.com, « un rootkit peut par exemple remplacer des binaires (su, ls, ps etc.) pour altérer leur fonctionnement (ne pas lister les process d'un utilisateur particulier par exemple pour 'ls') ou pour y cacher une backdoor qui permettrait (dans le cas de 'su' notamment) d'obtenir des droits root à partir d'un compte sans privilèges particuliers et sans avoir à connaître le password root. » De quoi sérieusement mettre à mal un système d'exploitation. Quoi qu'il en soit, et au-delà d'un problème de sémantique secondaire, si ce que Mark Russinovich indique est vrai, les conséquences sont importantes pour un utilisateur lambda ! Description technique du Root kit, avec des détails techniques permettant de faire la différence entre des objets cachés appartenant au système DRM, et les codes malicieux potentiels.