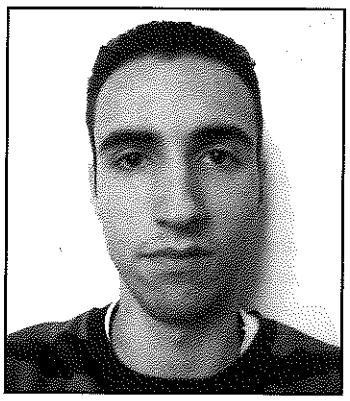
Linux et la sécurité



Pierre-Yves Rofes

Linux, le système sécurisé par excellence ? Non, bien sûr. Aucun système ne peut se targuer d'être invulnérable. Mais certains sont tout de même nettement plus robustes que d'autres face aux menaces numériques actuelles.

La sécurité est un argument qui revient régulièrement lorsqu'il s'agit d'exposer les points forts d'une distribution Linux. Qui ne s'est jamais vanté devant ses collègues utilisateurs de Windows de ne pas être ennuyé par les virus, spywares, chevaux de Troie et autre menaces numériques qui sévissent sur les différentes versions de ce système d'exploitation ? Il est vrai qu'à l'heure actuelle, GNU/Linux et plus généralement tous les systèmes d'exploitation dérivés d'Unix (BSD, MacOS, Solaris...) ne sont que très peu affectés par ce genre de problèmes. L'une des principales raisons à cela est l'un des piliers fondateurs d'Unix, le principe de moindre privilège : on affecte à un utilisateur ou à un programme uniquement les droits dont il a besoin, et rien de plus. Ce principe garantit qu'en cas de compromission du compte utilisateur ou du programme, le reste du système ne sera pas affecté. Ceci limite fortement les capacités de nuisance d'un code malveillant, celui-ci n'ayant en général pas suffisamment de privilèges pour compromettre durablement le système et pour se répandre à grande échelle.

Cependant, il faut garder à l'esprit que pour le moment, les utilisateurs de Linux sont encore très largement minoritaires si l'on considère les parts de marché des différents systèmes d'exploitation. Par conséquent, si l'on se place du point de vue d'une personne malveillante, diffuser un virus ou un cheval de Troie qui ne ciblerait que ces utilisateurs n'est pas vraiment rentable quand on sait qu'en développant le même code pour Windows, on toucherait sans problème un nombre beaucoup plus large d'utilisateurs.

Ces dernières années ont vu l'avènement des distributions résolument axées grand public, parmi lesquelles on peut citer Mandriva et Ubuntu. Et j'en profite pour saluer l'énorme travail réalisé par les développeurs de ces distributions pour les rendre accessibles au néophyte, notamment grâce à l'automatisation presque complète de certaines tâches souvent déconcertantes pour un débutant (partitionnement du disque, configuration du serveur X et de différents périphériques...).

Si l'on ne peut que se réjouir du fait que les systèmes libres commencent à devenir une réelle alternative crédible à Windows pour le marché du poste de travail, ils pourraient également devenir des cibles pour les auteurs de malwares en tout genre. En effet, même si le principe de moindre privilège expliqué précédemment reste important, il ne faut pas oublier que le principal vecteur d'infection d'une machine, ce n'est pas les vulnérabilités du système d'exploitation, mais bel et bien l'utilisateur final. Bien souvent, cela peut s'expliquer par un manque de formation et de connaissance. Aussi, si ces alternatives continuent à se développer, il serait tout à fait envisageable de voir apparaître dans un futur plus ou moins proche des *.deb*, *.rpm* ou même *.tgz* contenant du code malveillant.

Afin de rester à l'abri des risques, il est bon de rappeler quelques principes de base. Tout d'abord, un système doit être mis à jour régulièrement, afin de se protéger des vulnérabilités dernièrement découvertes. Pour ceux qui ne souhaitent pas mettre à jour tous leurs paquetages, il existe en général des solutions pour n'effectuer que les mises à jour de sécurité.

Utilisez toujours autant que possible les programmes paquetagés officiellement par sa distribution. L'utilisation de paquetages non-officiels ou le recours à la compilation manuelle depuis les sources ne doivent être considérées que comme des solutions de dernier recours quand il n'existe aucun équivalent paquetage. Dans ce cas, il peut être judicieux de s'adresser aux mainteneurs de paquets de votre distribution afin que le programme en question soit paqueté officiellement, ce qui lui garantira une plus grande pérennité et profitera au plus grand nombre.

Enfin, si l'utilisateur est le plus grand vecteur d'infection, il est également le meilleur anti-virus/spyware et autre que l'on puisse trouver, à condition de résister à la tentation d'installer tout et n'importe quoi sur sa machine...