Les logiciels malveillants sous Linux

- Objet : Les logiciels malveillants (malwares) sous Linux
- Suivi :
  à-compléter
  - Création par milou 14/10/2015
  - Tatouillé par paskal le 18/10/2015
- Commentaires sur le forum : c'est ici [1)]

Voir aussi Les malwares - Généralités

Introduction

Les systèmes d'exploitation GNU/Linux, Unix et « Unix-like » sont en général considérés comme peu ciblés par les virus informatiques. En effet, jusqu'ici, aucun virus opérant sous Linux n'a été répertorié comme étant très répandu, comme c'est parfois le cas avec Microsoft Windows.

Cependant, le nombre de programmes malicieux (incluant les virus, Trojans et autres types) sous Linux a augmenté ces dernières années,

"Il n’y a pas de virus sous Linux"

Cette affirmation est fausse même si, à vrai dire, les chances de se faire infecter par un virus sont bien plus faibles que sous Windows.
Aucun système n’est parfait et GNU/Linux, à l’image de Windows, possède des failles de sécurité qui peuvent être exploitées par des programmes malveillants.

Mais heureusement, les distributions GNU/Linux sont construites de telle manière qu’il est très compliqué pour un malware (virus, rootkit ou autre) de s’y installer et d’y commettre des dégâts significatifs.

Par exemple, la plupart des applications fonctionnent sans avoir les privilèges administrateurs requis par un virus voulant accéder aux parties critiques de l’OS.

De plus, la plupart des logiciels proviennent de sources bien entretenues et centralisées dans des logithèques et non pas de sites pris au hasard, ce qui rend d’autant plus difficile la propagation d’éventuels virus.

Les virus trouvent donc moins de crédit auprès de Linux, de même que les trojans.
Par ailleurs, les spywares sont rares sur les distributions Linux. On lira cependant avec intérêt l'article : Un logiciel espion dans Ubuntu ! Que faire ? de Richard Stallman.

Quoi qu'il en soit, nous vous recommandons la mise en place d'un pare-feu sur votre installation.

Linux et Windows face aux virus :

Les avantages de Linux par rapport à Windows

Pour maximiser leurs chances, les développeurs de malwares ont écrit leurs programmes pour infecter les postes de travail dont le système d'exploitation est le plus répandu, c'est-à-dire Microsoft Windows.

Si l'on regarde les statistiques de répartition des systèmes d'exploitation, Linux oscille plutôt entre 1,84% et 5% selon les études. Ce faible volume explique que les malwares ciblant des postes de travail sous Linux sont quasi-inexistants.

Un antivirus pour ce système d'exploitation n'est donc pas aussi important que sur Windows et il est tout à fait possible de s'en passer ordinairement.

Il est toutefois bon de rappeler que des malwares visant les postes de travail sous GNU/Linux existent.

Bien entendu, ces attaques tirent parti d'étourderies : méconnaissances en administration, mauvaises configurations, absences de mises à jour de la part des administrateurs. À ce sujet, quelques règles de bonne pratique à respecter :

- utiliser des logiciels récents ou mis à jour : la plupart des logiciels présentent des failles de sécurité ; les logiciels anciens (ou non mis à jour) constituent l'une des faiblesses principales sur une machine et, sur ce point, Linux se comporte comme un logiciel. Une maintenance efficace du système passe par la mise à jour régulière de l'intégralité des logiciels, noyau Linux compris ;
- sous Linux, on ne va pas, ou peu souvent, chercher les logiciels sur la toile. Nous utilisons un système de dépôts, où sont recensés tous les logiciels. Si les dépôts choisis sont sûrs, il y a peu de chance d'y rencontrer un virus. Ceci fait toute la différence car bon nombre de systèmes infectés par un virus le sont suite au téléchargement d'un fichier contaminé.

Face à la permissivité utilisée par défaut sous Windows, les variantes de l’architecture UNIX (Linux, BSD, Mac OS X) utilisent une gestion des droits extrêmement rigoureuse qui est un frein au développement de malwares sur ce type de plate-formes.

Les virus se trouvent le plus souvent isolés dans l’espace réservé à l’utilisateur ; les attaques les plus simples ne peuvent pas atteindre les parties vitales du système Linux.

De fait, les dégâts (si l’ordinateur est attaqué) sont donc limités à ces zones accessibles au seul utilisateur qui a démarré la session.

Ne vous y trompez cependant pas : un programme malveillant exécuté avec le compte root sous Linux pourrait occasionner des dégâts tout aussi importants que sous Windows !

Les principales menaces sous Linux

Les scripts malicieux

Ces programmes ne sont pas à proprement parler des virus, puisqu'ils n'ont pas pour objectif de porter atteinte à l'intégrité du système d'exploitation.
En revanche, ils s'attaqueront aux fichiers utilisateurs, c'est-à-dire la plupart des fichiers du dossier /home/[utilisateur].
Voir le détail sur ubuntu-fr.org : les « scripts malicieux ».

Les virus cachés dans les pièces jointes

Vous avez peut-être déjà constaté qu'un fichier téléchargé sous Linux n'est pas, par défaut, exécutable.
Pour des raisons évidentes de sécurité, Linux requiert que soit manuellement et volontairement donnée l'autorisation à un fichier de s'exécuter.

Attention ! Dans les archives compressées (du type .tar.gz, .tar.bz2, etc.) les fichiers conservent les droits qu'ils avaient au moment de l'archivage. Ainsi, vous pouvez très bien tomber sur un fichier exécutable après son désarchivage.

Les attaques par dépassement de tampon

Le dépassement de tampon ou “buffer overflow” est un type d'attaque lié à l'utilisation de la mémoire.

À la différence d'un virus cherchant à s'exécuter avec les privilèges de l'administrateur, un virus du type “buffer overflow” sera typiquement orienté vers la prise de contrôle d'un programme utilisateur habituellement sécurisé et possédant des accès ponctuels à des parties du système d'exploitation.

Un antivirus sous Linux ?

L'existence d'antivirus dédiés à Linux amène à s'intéresser aux possibilités d'existence et de propagation des virus sous Linux.

Malgré tout, l'utilité de ces antivirus est limitée car ils contrôlent, pour la quasi totalité d'entre eux, l'existence de virus pour Windows sur votre système Linux. Ce qui ne présente d'intérêt que dans certaines situations. En effet gardez à l'esprit qu'un virus pour Windows n'affectera quasiment jamais un système Linux.

Le second problème des antivirus sous Linux est que, si un nouveau virus est détecté sous Linux, il le sera bien moins rapidement que sous Windows.
Linux n'étant ni leur domaine de prédilection, ni leur cible principale, il est quasiment certain que le

virus sera devenu inefficace quand la mise à jour permettant de s'en débarrasser sortira.

Autant vous dire qu'il n'y a pas beaucoup de place pour un antivirus sur votre système Linux : le seul cas où il est nécessaire de se doter d'un antivirus sous Linux concerne les situations où vous auriez des fichiers à transmettre vers des systèmes sous Windows et que vous êtes concernés par leur sécurité.

Voir clamav

Les serveurs face aux menaces ...

... menaces souvent appelées rootkits.
Un rootkit n'est pas un virus à proprement parler, mais un logiciel injecté par un pirate dans un serveur ayant une faille de sécurité permettant d'exécuter du code non sollicité.

Un rootkit est capable de mettre en place un chemin permettant à un pirate d'effectuer des opérations sur votre serveur.

Pour être infecté par un rootkit il ne faut pas obligatoirement être un gros serveur mais il faut avoir attiré l'attention.
De plus, il faut qu'on puisse y accéder de l'extérieur, ce qui n'est pas le cas si vous utilisez un pare-feu et/ou n'avez aucun service réseau actif.

Bien entendu, si le but est de faire un serveur accessible de l'extérieur, il faudra ouvrir un port. Dans ce cas, il suffit simplement de n'ouvrir que le ou les ports qui vous intéressent et pas plus, et de suivre les mises à jour de sécurité avec attention.

Des anti-rootkits existent pour vérifier leur présence.

- rkhunter
- chkrootkit

Les principaux objectifs des infections visant les serveurs sont en général :

- effectuer du spam ;
- lancer des attaques DDoS ;
- infecter des utilisateurs Windows.

Pour les détails sur les principales menaces recensées sous Linux, voir :

- http://forum.malekal.com/malwares-virus-linux-t52397.html,
- Les liens suivants fournis par Severian sur le forum (Merci à lui) :
  - http://www.silicon.fr/xor-ddos-attaque-massive-botnet-linux-127751.html
  - http://www.undernews.fr/malwares-virus-antivirus/xor-ddos-un-nouveau-botnet-linux-qui-fait-des-ravages-150-gbps.html
  - http://www.undernews.fr/reseau-securite/seclists/mumblehard-malware-targets-linux-and-freebsd-servers.html
  - http://www.undernews.fr/malwares-virus-antivirus/turla-un-trojan-furtif-linux-ayant-fait-beaucoup-de-victimes.html

- Celui-là à prendre avec des pincettes comme tous les tests qu'il a dit Severian https://www.av-test.org/fr/nouvelles/news-single-view/linux-test-de-16-suites-de-protection-contre-les-programmes-malveillants-specifiques-a-windows-e/

Antivirus et serveurs GNU/Linux

Si un antivirus n'est pas franchement utile sur un poste client (ordinateur personnel), il peut trouver son utilité sur un serveur – par exemple un serveur mail connecté à des clients Windows : car si le serveur en question n'est pas lui-même en danger, l'antivirus peut éviter des propagations et ainsi protéger les clients Windows.

Attention toutefois aux faux-positifs que pourrait vous trouver votre antivirus. Regardez bien quel est le type d'infection présent, et n'hésitez pas à chercher des informations en tapant son nom dans votre moteur de recherche. Il y va de la stabilité de votre système.

Petit rappel

Les bons conseils de smolski

- Ne transigez pas avec les droits d'administration de votre système.
- Tout ce qui n'est pas nécessaire au simple utilisateur doit être réservé à l'utilisateur *root* !
- Ne vous baladez pas sur internet sous votre session *root* !
- Composez des mots de passe *root* robustes et n'hésitez pas à les renouveler périodiquement ! Un mot de passe robuste se compose d'au moins 20 caractères alpha-numériques !

Lien utile

Les cahiers de l'Administrateur Debian - La sécurité

Conclusion

Dans le cas d'une utilisation habituelle d'un ordinateur sous Linux (c'est-à-dire connecté avec des droits utilisateur et non administrateur, avec un mot de passe robuste pour chaque compte, et des logiciels et un système à jour), le développement de virus infectant des programmes exécutables est fortement limité par le fait que les exécutables appartiennent à l'administrateur et qu'ils peuvent être lus ou exécutés par l'utilisateur mais jamais écrits, donc jamais modifiés.

Par conséquent, il est très difficile, voire impossible, pour un virus, de se reproduire sous Linux en infectant des exécutables.
Ce type de virus très courant sous Windows ne peut que rester rarissime sous Linux.

Un dernier conseil : sécurisez votre Debian !

1)

N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !