Forum: Sécurité

Topic: Les logiciels malveillants sous Linux augmentent, et les entreprises ne sont pas prêtes

Subject: Re: Les logiciels malveillants sous Linux augmentent, et les entreprises ne sont pas prêtes

Publié par: tignothe
Contribution le : 13/02/2022 22:27:39

Bonsoir,

« je ne suis pas un spécialiste de Linux, juste un utilisateur par obligation professionnelle. »

— Ce simple propos résume toute la discussion ; un utilisateur qui a une méconnaissance totale du sujet sur lequel il souhaite intervenir.

Je n'ai jamais prétendu que Linux était exempt de tout risque d'infection, mais par contre les risques d'infection (malware, trucs malveillants et autres malfaisants) sont moins présents sur GNU/Linux de par l'approche de la sécurité qui est mise en place. :

– Chaque utilisateur sous GNU/Linux est complètement séparé des autres, avec un mot de passe spécifique et des droits d'accès très limité. Le simple fait d'accéder à des fichiers hors environnement propre demande tout de suite une élévation de privilège. Il n'est pas possible de modifier/déplacer/supprimer/créer un fichier sans en avoir expressément les droits y afférent et le mot de passe qui va avec. Ce qui limite (on le conçoit immédiatement) les risques d'installation de propagation de trucs non désirés. Tout se fait en plein accord avec celui qui se trouve sur la chaise derrière le clavier et à condition de le faire avec les bonnes commandes.

Pas question de trouver sur la toile un logiciel créé par "on n'sait qui" et de cliquer sur un "exe" qui donne un blanc seing sur le système. Les logiciels que l'on installe proviennent des dépôts dûment contrôlés et certifiés par la communauté.

Il est bien sûr possible d'installer des "trucs" hors dépôts, mais c'est aux risques et périls de celui qui est à la manœuvre (je pense principalement à des conflits de dépendances, notamment de forcer l'installation d'une "lib" non prévue sur la version du système sur lequel on se trouve, etc, etc.). Naturellement nous sommes loin de ce genre de considérations sous Windows, car l'approche sécuritaire y est complètement différente.

Petit test ; combien d'utilisateur travaille sous le compte "admin" sous Windows parce que c'est plus pratique ? on ne doit pas être loin des 99% … Il ne semble pas étonnant que la propagation des « des indésirables » s'en trouve facilité.

— Concernant la rapidité avec laquelle les différentes distributions sont patchés, désolé de te contredire c'est fait dès l'apparition d'un souci sur le noyau . N'oublions pas qu'il y a des personnes spécifiques pour gérer ce noyau donc le nombre de distributions existantes n'entre pas en ligne de compte, alors qu'un "ingé système" puisse croire en 2022 que chaque distribution fait sa p'tite salade dans son coin prouve bien la méconnaissance totale du sujet. Une distribution Linux, c'est un système bâtit autours d'un noyau, et non pas un assemblage fabriqué au gré d'un individu

quelconque.

Oui au début en 1991 une équipe de bénévoles gérait le cœur du système Linux, maintenant ce n'est plus le cas; Red Hat, Nowell, IBM, Intell mettent les doigts dans le cambouis… avec la maintenance « bienveillante » de Linus Torvalds en personne qui je le rappelle a été le premier développeur du noyau Linux. Je rappelle aussi que les sources du noyau sont visibles par tous ; c'est ce qui fait sa force.

— Pourquoi Linux serait meilleur ? Ce que je viens de dire plus haut se passe de commentaires et ce n'est nullement une question de nombre d'utilisateurs, mais bien une question de système (d'où les ≅ 95% de serveurs Linux) et aussi de la qualité de celui qui se trouve après le clavier qui ne fait pas n'importe quoi, car le « système » ne l'autorise pas !

Le propos n'est pas de savoir si un système est plus beau qu'un autre, donc le meilleur, mais bien de savoir dans quel environnement l'on s'engage et de ne surtout pas y venir avec des idées préconçues d'un autre époque. Les discussions sont intéressantes dans la mesure ou l'argumentation ne repose pas sur des légendes urbaines qui ne devraient plus avoir cours. Ces histoires de sécurité sont trop importantes de nos jours pour que l'on continue à ressortir les vieux dossiers.