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 09:30:49

Citation :
Tof81

Ces attaques semblent pour l'instant relativement peu sophistiquées, mais il est à parier qu'elles vont le devenir de plus en plus.

Questions ?

— Quelles sont ces attaques peu sophistiquées qui ciblent les serveurs sous Linux (je rappelle que 90 % des serveurs sont sous Linux). Je n'ai vu nul part la description de ces « fameuses attaques peu sophistiquées ».

— Qu'est-ce qui permet de soutenir que ces attaques « peu sophistiquées » vont gagner en efficacité dans un avenir plus ou moins proche ?

« De nombreuses organisations se laissent aller à des attaques parce que l'infrastructure Linux est mal configurée ou mal gérée » un peu plus loin dans le texte,« attaques par ransomware et cryptojacking conçues pour cibler les serveurs Linux dans des environnements qui ne sont peut-être pas aussi strictement surveillés que ceux fonctionnant sous Windows. »

Comme quoi un texte lu à la « va-vite » peut laisser croire que c'est le "software" qui est en cause et nullement le paramètre "humain" qui paraît le principal responsable de cet état de fait.

Il faut noter aussi que ce texte est tellement bien écrit que toutes les interprétations sont possibles, et cela laisse libre cours à une imagination galopante.

— Je ne suis pas certain Tof81 que tu aies eu la même analyse que moi, car le titre de ton propos me semble plus une "alerte" vers les utilisateurs Linux potentiels ou effectifs alors que ceux-ci n'ont souvent (toujours) rien à voir avec l'utilisation d'un serveur.

La meilleure preuve de ce que j'avance, c'est la réaction de « RGSOFT » qui s'interroge sur l'utilisation d'un antivirus sur une distribution Linux, et « reglisse » qui nous oriente vers un blog qui détient « les meilleurs antivirus » sous Linux.

Pour répondre à « RGSOFT», la décision d'utiliser une distribution Linux doit se faire en laissant derrière soi tous les vieux réflexes acquis par une longue utilisation de Windows.

Il n'y a pas besoin d'antivirus sous Linux, car ça ne protège en rien le système sur lequel on évolue. (je parle bien sûr de Linux bureau et non de Linux serveur) — Les logiciels sous Linux se trouvent dans les dépôts de la distribution que l'on utilise et sont fiables parce qu'ils ont été validés par la communauté. Naturellement si tu ne tiens pas compte de cela et que tu cherches "une perle rare" sur la toile qui viendra "bousiller" ton système, aucune protection ne pourra te protéger. Pour résumer, la gestion des droits sur les systèmes basés sur GNU/Linux est différente de ce que l'on trouve sur Windows. Sous Linux tout est fermé, et on autorise au coup par coup et pas n'importe comment.

Pour ce qui est des "meilleurs antivirus" sous Linux, ils ne servent qu'à trouver des "malveillants" qui n'opèrent que sous Windows. La base de donnée de ces antivirus ne contenant que des "malfaisant" Windows.

Alors Tof81 je pense qu'une petite précision aurait été nécessaire avant de commencer la lecture de cette alerte qui somme toute n'en est pas une ; elle ne sert qu'à refroidir les candidats à la liberté de GNU/Linux en leur agitant des peurs supposées sous le nez. Mais il est possible que tu aies une analyse différente de la mienne, auquel cas je suis tout ouïes…