Forum: Sécurité

Topic: Sur la protection de nos machines..!

Subject: Sur la protection de nos machines..!

Publié par: tignothe

Contribution le : 03/09/2018 14:17:41

Bonjour,

Je viens de lire un article qui ne peut laisser personne indifférent.

Tout dabord le titre; « 70% des exécutables malveillants au 1S(emestre)2018 étaient inconnus des services de réputation comme VirusTotal. (*VirusTotal sélectionné par PC World comme l'un des 100 meilleurs produits de 2007) VirusTotal est un agrégateur d'information .

Ce qui est quand même inquiétant si l'on base sa « quiétude journalière » sur les capacités de protection des différentes solutions antivirus qui ne se gênent pas pour vanter leurs mérites.

À quoi peut servir un « antivirus » sachant que 70 % des exécutables soumis à sa sagacité passera entre les mailles du filet à tous les coups?

Naturellement je me positionne dans le monde Windows où en général un exécutable n'a nullement besoin de demander une permission quelconque pour commencer à faire ce pour quoi il a été conçu. Ce qui est moins vrai dans le monde Linux ou Ios où les capacités de nuisance sont moindre par le simple fait que les « droits et permissions » sur un fichier sont données en connaissance de cause.

Ensuite, cet article porte à notre connaissance l'existence de « logiciels malveillants Fileless » qui s'attaquent exclusivement à la mémoire vive..!(pour l'instant je n'ai pas plus d'informations..?)

Puis les attaques par « Powershell » en très nette augmentation. (à relier avec les autorisations éventuelles donées aux exécutables).

En bref, la conclusion de l'article donné par SentinelOne est à prendre au pied de la lettre; « Au début du second semestre de 2018, les entreprises et les particuliers devraient surveiller un certain nombre de tendances et de menaces ».

Il serait peut être bon de revoir les stratégies de gestion des utilisateurs sous Windows, notamment le fait d'ouvrir les sessions en « administrateur » ...C'est quand même plus simple pour un exécutable de faire ce qu'il veut quand il veut!