



**Forum: Sécurité**

**Topic: HWMonitor : attention aux pièges proposés.**

**Subject: Re: HWMonitor : attention aux pièges proposés.**

Publié par: Tof81

Contribution le : 22/09/2018 15:19:08

Citation :

Lotesdelere a écrit:

Parce que Schtroumpf-Grognon a cliqué sur les liens pour tester, par curiosité, comme il l'a écrit.

Relis.

Et il a également posté des liens vers les analyses de VirusTotal que tu n'as pris la peine de lire non plus, sinon tu aurais vu ce qui a été analysé.

Car non, VirusTotal ne teste pas la machine mais uniquement des fichiers individuels et des URLs.

J'ai très bien lu et tu n'as pas compris mes propos ...

Sylvie a parlé d'un site en ligne : cela signifie en général que le soft/l'application est lancé(e) directement depuis leur serveur web et non par un exécutable à télécharger !!!

Et je sais très bien que VirusTotal ne teste pas la machine ...

D'autre part et pour info j'ai téléchargé driveragent-setup.exe sur <http://driveragent.com> = O/68 chez Virustotal

Ce fichier n'est pas empaqueté. Universal Extrauer en extrait DriverAgent.exe qui est l'exécutable = 2/67 (suspiciens) sur VirusTotal.

D'ou ma question de départ : où avait été téléchargé les .exe

Pour biosagentplus.exe téléchargé sur <https://www.biosagentplus.com> c'est un fichier empaqueté

UPX : il suffit de le dépaquer avec Universal Extractor et on obtient alors

biosagentplus\_décompressé.exe qui lui n'a que 3/67 à VirusTotal, et 2 chez

<https://metadefender.opswat.com>, probablement des faux positifs ...