## *Forum: Trucs en vrac*

### Topic: Quand un raccourci Windows peut flinguer votre sécurité

### Subject: Re: Quand un raccourci Windows peut flinguer votre sécurité

Publié par: rezoo

Contribution le : 27/12/2016 10:40:33

Citation :

Wullfk a écrit:
Citation :

rezoo a écrit:
C'est quoi cet article sans les sources de l'annonce de Jean-Pierre Lesueur, ?
moi j'appelle cela de la pub et non un article. Du coup, je remet un "prudence" sur cette annonce ...

Heu, j'ai pas tout compris, c'est moi qui est visé par cette remarque, ou l'article en question ?

C'est l'article qui n'a pas de sources. Pour trouver une vraie parade vaut mieux comprendre le problème et dans ce cas précis même avec google je ne retrouve pas les sources de Damien Bancal pour l'article.

J'ai cité une source possible et si c'est bien la source, il n'y a pas d'inquiétude à avoir...

Citation :
"Unfortunately for Hackers but fortunately for your safety since the introduction of Windows 7 you cannot use this technique anymore to run application file directly from Alternate Data Stream."

Je profite de cette réponse pour te viser :

La prudence avec un outil qui touche à la base des registres reste pour moi plus importante que sa modification hasardeuse pour corriger des bugs non identifiés correctement ou améliorer un système d'exploitation (voir ici un ensemble de système d'exploitations puisque l'on ne sais pas si on parle de la génération de windows 98 ou de windows 10).

En passant le programme Marmiton permet de filtrer les scripts malicieux mais il se base sur une liste blanche que l'utilisateur doit construire donc encore une fois c'est pas un outil pour un pc de tous les jours et du travail mais pour un pc de test qui permet de comprendre le fonctionnement d'une éventuelle menace.

Dans la présentation officiel de marmiton :
http://telecharger.malekal.com/download/marmiton/
on retrouve des liens pour mieux comprendre les problèmes et des conseils pour les éviter. Mais je vous l'accorde, c'est un vrai labyrinthe d'articles plus ou moins récent et pas toujours revue pour rester d'actualité.
http://www.malekal.com/ransomwares/
Citation :

Dans le cas des pièces jointes malicieuses, il suffit de bien faire attention aux emails que vous ouvrez et surtout aux fichiers qui y sont joints. Prenez bien le temps de lire.
Citation :
Il faut donc impérativement maintenir vos logiciels à jour afin de ne pas voir ces portes d'entrée sur ton système.
Citation :
La désactivation peut-il empêcher certaines applications de fonctionner ?  Cela peut arriver que des applications aient besoin d'utiliser des scripts VBS, dans ce cas, cela peut empêcher celle-ci de fonctionner correctement.
http://www.malekal.com/proteger-scripts-malicieux/
http://forum.malekal.com/securiser-so ... -version-courte-t381.html
http://www.malekal.com/securiser-le-navigateur-web-firefox-2/

Wullfk ton tuto Marmiton est bien mais, pour moi, inutile car c'est un logiciel pour utilisateur averti, de plus, rien ne le distingue de celui de l'auteur (http://telecharger.malekal.com/download/marmiton/ et http://secuboxlabs.fr/outils/marmiton/).
Il manque la partie indispensable : comment créer la liste blanche opérationnelle pour un système d'exploitation donnée et une suite de logiciels spécifiques.  La liste blanche contient donc **toutes** les applications autorisées.

Et ensuite on pourrait aussi parler du "couloir de la sécurité" ou des niveaux de protection ...
https://blog.kaspersky.fr/bienfaits-liste-blanche/3800/
bref de belles sources de revenue en perspective pour les spécialistes de la sécurité informatique.