



Forum: Trucs en vrac

Topic: Après Locky, le ransomware Petya encore plus virulent ?

Subject: Re: Après Locky, le ransomware Petya encore plus virulent ?

Publié par: rezoo

Contribution le : 22/11/2016 21:28:43

Citation :

Wullfk a écrit:

La première chose à faire c'est dans un premier temps (si l'infection est toute récente) c'est de débranché tout lecteur réseau (HDD externe, clé USB) puis d'ouvrir une demande d'aide sur un forum assistance comme par exemple Zebulon.fr il faut s'inscrire pour pouvoir poster un message dans la rubrique "*Analyses et éradication malwares*"

Traiter directement un tel virus en ouvrant une session sur l'ordinateur infectée est synonyme de perte supplémentaire de données. Après si la règle élémentaires d'une sauvegarde bien au chaud a été respecté et que l'on veut juste supprimer la menace ... pourquoi pas...

Pour le cryptage des données (ransomware...) j'aurais plutôt conseiller d'arrêter l'ordinateur, de le débrancher du réseau (au cas où quelqu'un le rallume et permet au virus de continuer sa propagation sur les appareils proches qui sont connectés).

Après, si on a les compétences et les outils, démonter le disque dur, faire une copie 'exacte' du support et essayer de récupérer les données non infectées et vérifier l'état des dégâts puis d'éradiquer l'intrus (vive les sauvegardes des systèmes).

Pour l'identification et l'éradication des menaces, une aide supplémentaire est souvent la source du succès. N'hésitez pas à passer par des forums spécialisés.

<http://forum.malekal.com>

<http://forum.zebulon.fr>

Et bien sur le meilleur conseil est des sauvegardes, des sauvegardes, et la plus grande prudence à l'égard des pièces jointes envoyées par mail.

On peut aussi se renseigner avant comme sur

<http://korben.info/locky-quil-y-a-a-savoir-malware-moment.html>

J'ai dit des SAUVEGARDES

mais on pourrait aussi parler de stratégie, de redondance, de backup « off site ». Bref un vaste sujet, plus intéressant et plus fiable que les multiples astuces, rustines et logiciels de protection qui ... devinez ;o)