Forum: Propositions de logiciels

Topic: Ace Locker

Subject: Re: Ace Locker

Publié par: Constance

Contribution le : 01/05/2016 12:49:46

Citation :
philou-traductions a écrit:

Peut-être pas écrire sur ce qui est déjà crypté: un dossier peut contenir des fichiers cryptés et non cryptés.
Je ne suis pas sûr de comprendre ce que tu veux dire, mais prenons un exemple simple : tu me transmets un fichier chiffré, sans la clef de déchiffrement, par exemple via une clef USB ou un disque dur externe.

Je n'ai pas besoin de savoir ouvrir et interpréter le contenu de ton fichier pour le chiffrer moi-même avec le système que je veux.
Dès lors, si je te rends ta clef USB tu ne pourras plus lire le document qui était dessus tant que je ne te donnerai pas la solution pour défaire mon chiffrement, avant que tu ne sois en mesure d'utiliser le tien.

Ben le ransomware c'est pareil, sauf qu'on n'a pas besoin de s'échanger un support, tout se fait directement sur les disques durs auxquels tu as accès en écriture tant que le malware est actif.

Si tu n'as pas de sauvegarde ou de moyen de récupérer la réponse qu'attend le malware et que tu es supposé obtenir en l'échange d'un paiement, tu peux dire adieu à ton document, qu'il ait été déjà chiffré avant l'activation du ransomware ou non.

Après je suis d'accord que la plupart des ransomwares se contentent de cibler certains fichiers en fonction de leur extension, donc si jamais ton fichier est dissimulé dans un conteneur (par exemple TrueCrypt), dont l'extension elle-même n'est pas ciblée par le malware, alors il ne devrait pas se faire chiffrer... tant que tu ne "monteras" pas le conteneur avec possibilité d'accès en écriture.