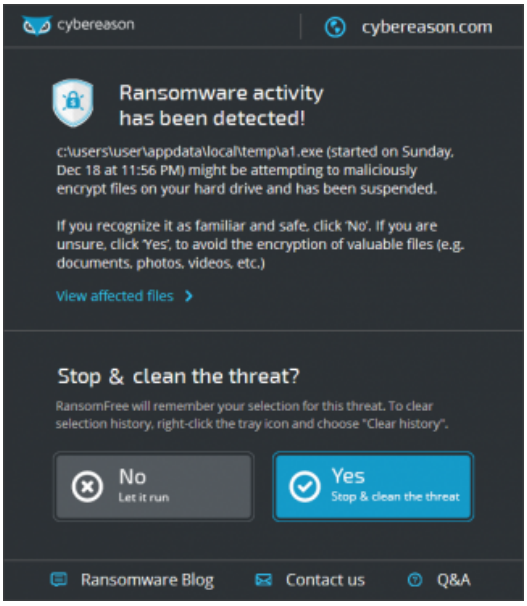
RansomFree, l'application qui leurre les ransomwares

Avec une estimation à plus d'un milliard de dollars récoltés en 2016, les ransomwares sont considérés comme la menace star de l'année. Ces malwares qui chiffrent les fichiers du PC/serveur (ou smartphone) infecté et exigent de payer une rançon (généralement en bitcoin) pour les récupérer sont la plaie des solutions antivirales. La vitesse d'évolution de leurs variantes les rend en effet difficile à détecter en amont. Ce qui n'empêche pas les éditeurs de proposer des solutions de protection alternatives.

C'est notamment le cas de Cybereason qui propose RansomFree, un outil de protection à la démarche assez originale et destiné à l'environnement Windows (7, 8 et 10, ainsi que Windows Server 2010 R2 et 2008 R2) pour l'heure. Plutôt que de s'acharner à vouloir arrêter l'exécution du rançongiciel, RansomFree entend leurrer les agents malveillants en les laissant exécuter leur tâche… dans le vide.

Le honeypot des ransomwares

Concrètement, l'application de protection crée un «honeypot», un piège dans lequel devrait inévitablement tomber le ransomware. Pour cela, le logiciel de Cybereason crée des faux dossiers dont le nom commence par « ! » ou « ~ ». Deux caractères qui, de par leur positionnement bas dans la table ASCII, devraient pousser les ransomwares à visiter en premier lieu ces répertoires leurres, rapporte Bleeping Computer qui a testé l'application.



Dès que RansomFree détecte une modification des fichiers contenus dans ces faux dossiers, il stoppe automatiquement le processus de chiffrement, ou toute autre action. L'anti-ransomware alerte alors l'utilisateur et lui demande s'il veut laisser le processus se poursuivre ou bien l'arrêter et nettoyer le système du probable rançongiciel.

Une quarantaine de ransomwares stoppés

Simple d'utilisation, RansomFree se veut d'autant plus ingénieux qu'il permet d'arrêter la plupart des agents de chiffrement, quelles que soient leur famille, leur signature et leurs dernières évolutions. Aux dires de son éditeur, la solution est efficace contre une quarantaine de ransomwares dont Locky, Cryptowall, TeslaCrypt, Jigsaw ou Cerber, indique Uri Sternfeld, chercheur du Cybereason Labs. RansomFree est gratuite qui plus est.

RansomFree n'est pas la première solution visant à se protéger des rançongiciels. On peut en trouver chez Bitdefender, Kaspersky ou Malwarebytes (en version bêta). D'autres éditeurs s'attachent à retrouver les clés de déchiffrement. Mais la meilleure défense reste la vigilance et la prévoyance : éviter de cliquer sur des liens potentiellement infectieux (phishing, fichier bureautique avec une macro, etc.) et faire des sauvegardes régulières de vos données pour les restaurer en cas d'attaque.

Lire également

Comment le ransomware est devenu le gagne-pain des cybercriminels
Le ransomware Locky s'invite sur Facebook
Ransomwares : les entreprises françaises touchées, se distinguent