Par Romain Castel
|Publié le 6 janvier 2014

Comment se protéger de Cryptolocker et autres virus qui cryptent vos fichiers pour vous rançonner

Les «rançongiciels» sont des virus qui rendent l'ordinateur qui en est victime inutilisable, et ce jusqu'à ce que paiement soit effectué..

Enfin, si il n'y a rien d'efficace sur Internet et qu'aucun de vos proches n'a pu vous aider, le meilleur moyen pour se débarrasser du malware est de réinstaller le système d'exploitation. Mais cela entraîne forcément la perte d'une partie des données du disque dur.
Même une fois sorti d'affaire et les données récupérées, existe-t-il un risque pour nos données personnelles ? Peuvent-elles par exemple être revendues ? Comment faire pour ne plus être ainsi soumis à une telle prise d'otage des données informatiques ?

Le risque, pour les données personnelles, dépend du ransomware. Si il a été conçu pour demander une rançon et également pour exfiltrer des données, alors oui, il y a un risque pour qu'elles soient revendues et réutilisées. Dans ce genre de cas, il est toujours conseillé de changer tout les mots de passe qui pourraient être stockés sur le disque dur, dans les navigateurs Web par exemple.

Afin de diminuer les risques d'être soumis à ce genre de rançonnage, il est nécessaire d'appliquer les recommandations faites plus haut : Mettre à jour le système d'exploitation et les différents éléments software (navigateur, java, flash...), être prudent avec les mails qui demandent de télécharger une pièce jointe ou un fichier. Il faut être extrêmement prudent avec les logiciels illégalement téléchargés, le crack permettant de faire marcher le logiciel contenant souvent du code malveillant. Un bon moyen pour se prémunir des ransomware est également de faire des sauvegardes régulières, ainsi la perte de données est minime et l'agresseur n'aura pas de moyen de pression.

Il est important de garder a l'esprit qu'il ne faut pas faire confiance au ransomware, que le seul moyen d'être tranquille est d'éradiquer le malware, pas de payer la rançon. Plus généralement il est utile de rappeler qu'il ne faut pas accorder une confiance aveugle a ce qui provient d'Internet car il est difficile d'en connaitre l'origine

- Le deuxième vecteur d'infection est la navigation Internet. En effet, lorsqu'un utilisateur utilise un navigateur Web qui n'est pas à jour, il s'expose au risque qu'un site web qu'il va visiter exploite une faille de son navigateur et injecte le malware, et ce absolument sans action de l'utilisateur.

Afin de prévenir les infections virales, quelle qu'en soit l'origine, il est important de respecter quelques principes

- Il faut avoir la plus grande vigilance face aux mails qui demandent d'effectuer des actions ou de télécharger un logiciel même si le mail provient d'un ami. Il faut se demander si l'expéditeur a une raison et/ou si il est légitime pour vous de demander de réaliser ce genre d'action. En cas de doute, il ne faut pas hésiter a se renseigner sur Internet, sachant qu'il est en général assez facile de trouver des informations concernant les attaques importantes de fishing.

- Le deuxième point de vigilance pour éviter les infections virales est d'effectuer toutes les mises à jours des principaux outils qui communiquent avec Internet (les navigateurs web, le java, le flash, etc...)

Il est également possible d'installer des logiciels de type antivirus ou anti-spyware qui vont ajouter un niveau de surveillance supplémentaire sur les fichiers téléchargés ou sur le comportement des programmes qui s'exécutent sur le système.
Si toutefois on a été infecté, comment faut-il réagir ? Est-il nécessaire de payer la rançon pour récupérer ses données ou existe-t-il d'autres moyens ?

En cas de rançonnage, il ne faut en aucun cas payer car il n'existe aucune garantie que le malware cessera sont activité. Par exemple, de nombreux ransomware qui se font passer pour une entité gouvernementale ne rendent jamais la main à l'utilisateur. Même dans le cas ou l'utilisateur a l'impression d'avoir réglé le problème en payant la rançon, il y a de forte chance pour que le malware soit toujours présent sur le système et qu'il soit programmé pour se relancer quelques mois plus tard ou pour espionner les utilisateurs du système.

La meilleure façon de réagir dans ce genre de cas est de prendre le temps de se renseigner, en cherchant sur Internet, car il existe très souvent des explications permettant de se débarrasser de ce type de malware. Il peut également être intéressant de se renseigner auprès des personnes qui vous entourent. Il est en effet rare qu'un malware de ce type ne touche pas quelqu'un parmi vos connaissances. Cette personne aura peut être trouvé une solution efficace pour éradiquer le problème. Il faut par contre se méfier des outils automatisés qui proposent des solutions toutes faites car ce sont souvent des malwares eux mêmes.

En ce qui concerne la récupération des données, si elles ont été chiffrées les chances de les récupérer sont à peu prés nulles. A moins qu'un expert en sécurité informatique n'ait publié un outil qui permette de déchiffrer les données a partir de l'analyse qu'il aura faite du virus. Si le système était simplement verrouillé, alors les données ne seront pas altérées et à la suppression du problème l'utilisateur les retrouvera.

Enfin, si il n'y a rien d'efficace sur Internet et qu'aucun de vos proches n'a pu vous aider, le meilleur moyen pour se débarrasser du malware est de réinstaller le système d'exploitation. Mais cela entraîne forcément la perte d'une partie des données du disque dur.
Même une fois sorti d'affaire et les données récupérées, existe-t-il un risque pour nos données personnelles ? Peuvent-elles par exemple être revendues ? Comment faire pour ne plus être ainsi soumis à une telle prise d'otage des données informatiques ?

Le risque, pour les données personnelles, dépend du ransomware. Si il a été conçu pour demander une rançon et également pour exfiltrer des données, alors oui, il y a un risque pour qu'elles soient revendues et réutilisées. Dans ce genre de cas, il est toujours conseillé de changer tout les mots de passe qui pourraient être stockés sur le disque dur, dans les navigateurs Web par exemple.

Afin de diminuer les risques d'être soumis à ce genre de rançonnage, il est nécessaire d'appliquer les recommandations faites plus haut : Mettre à jour le système d'exploitation et les différents éléments software (navigateur, java, flash...), être prudent avec les mails qui demandent de télécharger une pièce jointe ou un fichier. Il faut être extrêmement prudent avec les logiciels illégalement téléchargés, le crack permettant de faire marcher le logiciel contenant souvent du code malveillant. Un bon moyen pour se prémunir des ransomware est également de faire des sauvegardes régulières, ainsi la perte de données est minime et l'agresseur n'aura pas de moyen de pression.

Il est important de garder a l'esprit qu'il ne faut pas faire confiance au ransomware, que le seul moyen d'être tranquille est d'éradiquer le malware, pas de payer la rançon. Plus généralement il est utile de rappeler qu'il ne faut pas accorder une confiance aveugle a ce qui provient d'Internet car il est difficile d'en connaitre l'origine.