La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

Ransomware

Qu'est-ce qu'un Ransomware

Un Ransomware est un type particulier de logiciel malveillant qui est en train de se répandre aujourd'hui rapidement sur internet. Il menace de détruire les documents et les fichiers de la victime. Un logiciel malveillant est un programme utilisé pour réaliser des actions malicieuses. Un Ransomware est seulement un logiciel malveillant parmi d'autres, cependant, il est devenu très courant car il est très rentable pour les cybercriminels. Lorsqu'un Ransomware infecte votre ordinateur, il va chiffrer une partie de vos fichiers ou votre disque entier. Vous êtes ensuite bloqué et soit vous ne pouvez plus accéder à votre système soit vous ne pouvez plus ouvrir certains fichiers importants, comme vos photos ou vos documents. Le logiciel malveillant vous informe à ce moment-là que la seule façon de déchiffrer vos fichiers et récupérer l'accès à votre système est de payer une rançon au cybercriminel. C'est d'ailleurs de là que vient le nom Ransomware. Souvent cette rançon doit être payée avec de la monnaie virtuelle comme le bitcoin. Les Ransomware se propagent comme beaucoup d'autres logiciels malveillants. La méthode la plus courante est l'envoi d'un email corrompu au sein duquel se situe une pièce jointe ou un lien malveillant que les cybercriminels vous poussent à ouvrir.

Editeur invité

Lenny Zeltser travaille sur la protection des opérations Informatiques pour les clients au sein de NCR Corp. Il est également formateur en lutte contre les logiciels malveillants à l'institut SANS. Lenny est actif sur Twitter avec le compte **@lennyzeltser** et il écrit également pour le Blog **zeltser.com**.

Devez-vous pays la rançon ?

C'est une très bonne question à laquelle il est difficile de répondre. La difficulté réside dans le fait que plus les victimes payent les rançons, plus les cybercriminels seront motivés pour infecter d'autres victimes. D'un autre côté, vous n'avez peut-être pas d'autres choix pour récupérer vos données. Mais faites attention, même si vous payez la rançon, rien ne garantit que vous pourrez récupérer vos fichiers. Vous traitez avec des criminels, ils peuvent ne pas déchiffrer les fichiers. Même s'ils vous fournissent un moyen de déchiffrement en échange du payement, ce déchiffrement peut mal fonctionner ou alors votre ordinateur peut se retrouver infecté avec un autre logiciel malveillant.

Faites une sauvegarde de vos données

La sauvegarde des données est peut-être la meilleure façon de récupérer d'une attaque de Ransomware sans avoir à payer

Ransomware

la rançon. De cette façon, même si vous êtes infecté par un Ransomware vous pouvez retrouver vos données une fois que vous aurez nettoyé votre ordinateur. Par contre gardez en tête que si vos sauvegardes sont accessibles depuis le système infecté, le Ransomware peut chiffrer, voire effacer vos données sauvegardées. C'est pourquoi il est important de sauvegarder vos données sur un cloud de confiance ou alors sur des disques externes qui ne restent pas connectés en permanence à votre système. De plus, beaucoup de personnes commettent l'erreur de penser que les sauvegardes vont fonctionner directement sans jamais avoir à les tester. Faites régulièrement des tests de vos sauvegardes afin de vérifier qu'elles fonctionnent correctement et que vous pourrez récupérer vos données si jamais votre ordinateur est infecté par un Ransomware. Les sauvegardes seront également importantes si jamais ne vous effacez accidentellement des fichiers ou si votre système crash.

Un Ransomware est un malware qui, une fois votre ordinateur infecté, chiffre tous les fichiers sur celui-ci et vous empêche d'y accéder.

Aller plus loin dans la protection

Vous pouvez vous protéger d'une infection par Ransomware de la même façon que vous le feriez pour tout autre type de virus. Commencez par vérifier que votre Anti-virus est bien à jour et qu'il provient d'un distributeur officiel. Ces outils parfois appelés « Anti-malware » sont développés pour détecter et stopper les logiciels malveillants. Par contre, les Anti-virus ne peuvent pas bloquer et supprimer tous les programmes malicieux. Les cybercriminels sont en permanence en train d'innover et développent des logiciels malveillants de plus en plus sophistiqués qui peuvent échapper à la détection. En retour, les vendeurs d'Anti-virus développent constamment de nouveaux outils de détection de logiciels malveillants. Sur beaucoup d'aspects c'est devenu une course à l'armement avec chaque camp essayant de surpasser l'autre. Malheureusement, les pirates ont habituellement un coup d'avance. C'est pourquoi vous devez vous assurer d'avoir vos données sauvegardées et que vous pouvez employer les points suivants pour vous protéger :

- Les cybercriminels, afin d'infecter votre ordinateur utilisent souvent des vulnérabilités présentes dans les logiciels. Plus votre logiciel est à jour, moins il y aura de vulnérabilités dans votre système. Cela rendra l'infection beaucoup plus difficile pour les pirates. C'est pourquoi vous devez vous assurer que votre système d'exploitation, votre application et vos terminaux font les mises à jours de façon automatique et le plus régulièrement possible.

Ransomware

- Sur les ordinateurs, il faut utiliser des comptes d'utilisateurs avec des privilèges limités plutôt que le compte « administrateur » ou « root ». C'est une mesure additionnelle empêchant plusieurs types de logiciels malveillants de s'installer par eux-mêmes.
- Les cybercriminels dupent les utilisateurs afin qu'ils installent les logiciels malveillants pour eux. Par exemple, ils peuvent vous envoyer un email qui ressemble à un email légitime avec une pièce jointe ou un lien. Cet email peut sembler arriver de votre banque ou d'un ami. Par contre si vous ouvrez la pièce jointe ou cliquez sur le lien, vous activez le code malicieux qui installe le logiciel malveillant sur votre ordinateur. Si un message provoque un sentiment d'urgence, n'est pas clair ou s'il semble trop beau pour être vrai, cela peut-être une attaque. Faites attention et faites preuve de bon sens car c'est souvent votre meilleure défense.

Vous vous protègerez d'un Ransomware en étant vigilant lorsque vous ouvrez des pièces jointes ou lorsque vous cliquez sur des liens. Assurez-vous d'avoir votre Anti-virus à jour et soyez sûr d'avoir tous vos fichiers régulièrement sauvegardés et testés.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients. Pour en savoir plus, veuillez vous référer aux liens suivants : http://www.answer.ch et http://answersecurity.com/

Sources

Hammeconnage (Phishing) : https://securingthehuman.sans.org//ouch/2015#december2015

Qu'est-ce qu'un Malware : https://securingthehuman.sans.org/ouch/2016#march2016

Chiffrement : https://securingthehuman.sans.org/ouch/2016#june2016

Sauvegardes : https://securingthehuman.sans.org/ouch/2015#august2015

Article Microsoft : https://www.microsoft.com/security/portal/mmpc/shared/ransomware.aspx

Cours SANS FOR610 – Ingénierie Inverse de logiciels Malveillants : https://sans.org/for610

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley
Traduit par : Marilyn Combet