Parc d'Activités Schweitzer
26 rue du Bois Fossé
85300 CHALLANS
Tél. 02 51 49 31 31

espace technologie

FICHE CONSEIL

Se protéger des CryptoLockers et Ramsomwares

QU'EST-CE QU'UN CRYPTOLOCKER ?

Le CryptoLocker est un logiciel malveillant de type « ransomware ». Il se propage la plupart du temps via un courrier électronique contenant une pièce jointe comme un fichier .exe (ou zippé), un document PDF, Word, Excel (la liste est longue…) ou un lien permettant le téléchargement de ce même fichier. A l'ouverture de ce fichier par l'utilisateur, CryptoLocker s'installe sur le poste. Il peut dans certains cas ne pas être détecté par l'antivirus. Pour rappel, un antivirus fonctionne sur la notion de liste noire, et protège uniquement contre ce qu'il connait (les signatures) ainsi que les variantes pour lesquelles des sommes de comportements anormaux permettent une détection.
Cryptolocker travaille en tache de fond de façon imperceptible et à l'issu d'un certain temps (~5 à 15 min), certains types de documents sur les disques internes ou les partages réseau sont chiffrés. Ils deviennent illisibles par l'utilisateur. Un message des pirates demande alors le paiement d'une rançon en ligne dans un délai court (généralement 72 heures au-delà desquelles les documents seront définitivement perdus), en échange de la fourniture de la clef de déchiffrement des données. Attention, d'autres formes de propagation de ce ransomware existent : caché dans des versions de logiciels/jeux piratés téléchargés sur Internet ou suite à une infection par des malwares de type « cheval de Troie » contractée sur des sites de mauvaise réputation ou infectés.

Chaque jour les pirates améliorent les attaques. Nous constatons par exemple l'utilisation de fausses adresses emails utilisant le nom de domaine de votre société ou de partenaires connus.

« L'Agence France Presse a été la cible de deux tentatives d'attaque au «ransomware» Locky. Les particuliers, entreprises et institutions sont de plus en plus confrontés à cette nouvelle forme de menace - *source http://www.lefigaro.fr*».

COMMENT CA MARCHE ?

Une fois installé sur la machine de la victime, le CryptoLocker va utiliser son algorithme de génération de noms de domaine pour identifier le ou les serveurs de commande et de contrôle (C&C) avec lesquels il va pouvoir communiquer. Lorsqu'il a identifié son serveur C&C (cette opération peut durer environ 5 min), le CryptoLocker lui demande la génération d'un couple de clés RSA 2048 bits. La clé privée reste sur le serveur tandis que la clé publique est envoyée au ransomware pour qu'il crée sa nouvelle clef de chiffrement. Il utilisera celle-ci pour chiffrer les différents fichiers. Quand il aura fini, Cryptolocker communiquera au serveur C&C l'achèvement du chiffrement : le message de demande de rançon apparait alors à l'écran.

> C'est durant la 1ere phase de recherche du serveur C&C que l'on peut intervenir pour bloquer Cryptolocker en coupant toute communication Internet, soit environ 5 à 15 min pour les versions actuelles, après il sera trop tard ! Cryptolocker met en œuvre des techniques de chiffrement robustes, contre lesquelles aucun moyen simple de déchiffrement n'est actuellement connu.

COMMENT SE PROTEGER

Les bonnes pratiques de protection :

A) La mesure la plus efficace est l'information et la sensibilisation des utilisateurs aux risques associés aux messages électroniques, fichiers attachés et/ou téléchargés et liens internet. On ne le répétera jamais assez, la principale mesure préventive reste du côté de l'utilisateur ! Ce type d'infection peut être facilement évité, si les utilisateurs suivent ces 4 consignes de prudence élémentaire très efficaces :

- **Ne jamais ouvrir un courrier électronique suspect** (sujet, langue, syntaxe, sans rapport avec votre activité) ou de provenance douteuse (expéditeur inconnu) => le signaler à l'administrateur sécurité
- **Ne jamais cliquer sur un lien web dans un courrier électronique non sollicité** ou de provenance douteuse,
- **Supprimer immédiatement chaque courrier électronique suspect** ou de provenance douteuse.
- **Ne jamais double-cliquer sur des documents en pièce attachée de courrier d'expéditeurs inconnus ou suspects**, de type exe, zip ou avec un nom trop long pour voir l'extension. Ne jamais télécharger et installer des exécutables sans avis de l'administrateur, zip (logiciels, utilitaires, jeux,…), notamment à partir de sites web douteux.

B) Au niveau sécurité générale (administrateur) :

- Installer sur chaque machine un agent antivirus et préférablement une **suite de sécurité de poste** et le maintenir à jour : vérifier qu'il reçoit bien les dernières mises à jour de signatures plusieurs fois par jour.

- Avoir une solution de protection de messagerie (en passerelle ou sur le serveur) : pour contrôler le trafic de messagerie entrant : **anti-spam**, anti-phishing, anti-virus, **filtrage du contenu** : blocage des pièces attachées de type exécutables et doubles extensions, Zip avec mot de passe, ou fichier chiffré.

- Avoir une solution de protection de la navigation Internet **: filtrage WEB** : bloquer les catégories de sites non professionnels, suspects, illégaux ou dangereux, pour éviter les risques d'infections et d'accès en fonction de la réputation du site.

- Analyser les téléchargements avec un anti-virus en passerelle : bloquer les téléchargements de fichiers exécutables, zippés avec un mot de passe ou chiffrés ; analyser et filtrer les flux Https et FTP ; bloquer ou limiter les autres communications : media sociaux, notamment les transferts de fichiers.

- Maintenir les systèmes d'exploitation et les logiciels à jour, en appliquant les correctifs de sécurité et les patches les plus récents.

- Activez les mécanismes de contrôle d'applications afin de vous assurer que seuls les logiciels validés par votre entreprise et dont vous assurez l'application des correctifs soient installés et exécutés.

- Activez ou mettre en place des systèmes de contrôle des périphériques amovibles (clefs USB, disques externes, ...) afin de réduire le risque d'infection par ce vecteur.

Même avec les bonnes pratiques de sécurité, une infection peut tout de même survenir. Il vous sera alors nécessaire de recouvrer les données qui auront été chiffrées, sans payer de rançon qui finance les pirates et les aide à améliorer Cryptolocker pour le rendre encore plus rentable. A cet effet :

- Effectuer des sauvegardes régulières de vos données et les stocker sur des **médias non connecté en permanence au réseau** (afin qu'elles ne risquent pas d'infection) : en cas d'infection de type ransomware vous retrouvez vos données en clair sur vos disques ou stockage mis à l'abri.

=> Ne pas laisser son disque dur externe constamment branché à son ordinateur. - Faire preuve de prudence lors de l'utilisation et d'échange de clefs USB : installer un module contrôle des périphériques pour interdire l'exécution sur les périphériques de type clef USB ou disque amovible

- An niveau du serveur il convient d'utiliser **une solution logicielle et matérielle permettant d'isoler les sauvegardes du reste du réseau**. Pour cela il convient de prendre contact avec nos services d'ingénierie réseau, qui saura analyser votre infrastructure et vous proposer les solutions adaptées.

COMMENT REAGIR EN CAS D'INFECTION

1°) Déconnecter immédiatement les appareils infectés de tout réseau filaire ou WiFi : cela empêchera Cryptolocker de communiquer avec son serveur C&C et évitera le chiffrement. Nous vous conseillons de débrancher immédiatement électriquement votre poste de travail.

2°) Appeler immédiatement nos services d'assistance

3°) Changer ses mots de passe après avoir nettoyé le réseau, pour se protéger d'une réinfection.

EXISTE-T-IL UNE PROTECTION EFFICACE ?

Il n'existe pas (à notre connaissance) d'antivirus permettant d'éviter les infections. Cependant Sophos vient de mettre en place une solution.

« Sophos System Protector », appuyé par le module « Malicious Traffic Detection » (MTD) permet de bloquer les connexions sortantes de Cryptolocker (et d'autres malwares) vers les serveurs de Commande et Contrôle des pirates, empêchant ainsi la récupération de la clef de chiffrement. Le blocage des communications empêche le chiffrement des documents d'avoir lieu et la désinfection sera réalisée en conséquence, sans nécessiter de recouvrement des données à partir d'une sauvegarde, le chiffrement des données n'ayant pas encore été réalisé par CryptoLocker.

Le budget de cette option est d'environ 27€ht/an/utilisateur du réseau.

Si vous êtes déjà équipe de Sophos Endpoint, - (Hors coût d'installation)