SOPHOS
Security made simple.

# Conseils pour se protéger contre CryptoLocker

## Sophos Endpoint Protection


Sophos SARL
River Ouest
80 Quai Voltaire
95870 Bezons

Tel. : 01 34 34 80 00
Fax : 01 34 34 80 01
info@sophos.fr
**http://www.sophos.fr**

# Sommaire

# 1. Qu'est-ce que CryptoLocker ?

**CryptoLocker** est un logiciel malveillant de type « ransomware » qui se propage pour les versions actuelles la plupart du temps par un courrier électronique contenant une pièce jointe fichier .exe (ou zippé) caché sous un document PDF, 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, et 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 et deviennent donc illisibles par l'utilisateur. Un message des pirates demande alors le paiement d'une rançon en ligne dans un court délai (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**.

# 2. Mécanismes de CryptoLocker : le lien au serveur de Command & Control

**Une fois installé sur la machine de la victime, 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), **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 qu'il utilisera pour chiffrer les différents fichiers. Quand il aura fini, Cryptolocker communique 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.

# 3. Prévention : les correctifs de sécurité

**Appliquer tous les derniers correctifs de sécurité du système d'exploitation et des applications installées** pour empêcher Cryptolocker ou tout autre malware d'utiliser des failles de sécurité présentes pour s'installer sur le PC.

**Particulièrement, mettre à jour le navigateur et ses plugins** : les malwares utilisent les failles de sécurité de Flashplayer, Java, Shockwave player, Acrobat Reader, Vlc, Realplayer, etc. Par exemple, pour vérifier si tous vos plugins Firefox sont à jour:
http://www.mozilla.org/fr/plugincheck/

# 4. Les bonnes pratiques de protection

## 4.1. Les utilisateurs

**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, cab, 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.

## 4.2. Les administrateurs

Au niveau de la sécurité générale configuré par l'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.

- Maintenir les systèmes d'exploitation et les logiciels à jour, en appliquant les **correctifs de sécurité et les patches les plus récents**. **=> Sophos Endpoint : module Patch Assesment**

- 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. **=> Sophos Endpoint : modules Application Control**

- Activez les **mécanismes de contrôle des périphériques amovibles** (clefs USB, disques externes, …) afin de réduire le risque d'infection par ce vecteur. **=> Sophos Endpoint : module Contrôle des périphériques.**

- **Mettre en place des stratégies de restriction logicielle** : possible pour les clients (depuis Windows 7) et pour les serveurs (depuis Windows 2008 R2) (SRP/AppLocker sous Windows) pour empêcher l'exécution de code à partir d'une liste noire de répertoires :
  <profil>\AppData\Local\Temp ;
  <profil>\AppData\Local\Temp* ;
  <profil>\AppData\Local\Temp** ;

- **Limiter au maximum les ouvertures de sessions interactives avec un compte à privilège** (ex : administrateur de domaine, utilisateur avec pouvoir): limite la propagation du chiffrement à la totalité des disques partagés présents sur le poste de travail infecté.

- **Désactiver si possible le RDP** (Remote Desktop Protocol est un protocole Windows qui permet d'accéder à distance à une machine en utilisant Terminal Service) car des versions de Cryptolocker l'utilisent pour infecter d'autres machines.
  Voici quelques liens utiles : Windows XP RDP disable, Windows 7 RDP disable, Windows 8 RDP disable

Plus globalement :

- 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. **=> Sophos UTM : Mail Protection**

- Avoir une solution de **protection de la navigation Internet** : **filtrage d'URL** : bloquer les **catégories de sites** non professionnels, suspects, illégaux ou dangereux, pour éviter les risques infections et accès en fonction de la réputation du site. **=> Sophos UTM : Web Protection**
- **Analyser les téléchargements** avec un **anti-virus en passerelle**. Bloquer les téléchargements de fichiers exécutable, 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. **=> Sophos UTM : Web Protection**

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 car 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'abris.
  => **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.

# 5. Comment Sophos Endpoint vous en protège ?

**Utiliser les protections de Sophos Endpoint Protection :**

1. **Sophos Endpoint Protection** activé, mises à jour fréquentes des signatures (plusieurs fois par jour). Activer HIPS, anti-PUA, Live Protection (Live Antivirus et liveURL), et configurer le blocage si détection.

2. **Patch Assesment** : vérifier régulièrement la présence des derniers correctifs et mettre à jour les machines en fonction du niveau de criticité indiqué par Sophos.

3. **Web control** : bloquer les 14 catégories non professionnelles et dangereuses.

4. **Contrôle des périphériques** : interdire les clefs USB et disques amovibles non professionnels afin de réduire le risque d'infection par ce vecteur

# 6. Que faire si infecté ?

**Comment réagir si vous soupçonnez une 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.

   (**Voir** 2.)

2. **Ensuite**, **nettoyer les machines infectées** (ou soupçonnées) avec **Sophos Endpoint Protection à jour, ou Sophos Virus Removal Tools**.
   http://www.sophos.com/en-us/products/free-tools/virus-removal-tool.aspx?cmp=70130000001xGqlAAE

   **Télécharger Sophos VRT à partir d'une autre machine saine** et le copier sur une clef USB. Sophos VRT va éliminer Cryptolocker pour éviter le chiffrement de nouveaux fichiers et l'infection de nouvelles machines.
   Cependant, si des fichiers ont été chiffrés, ils le resteront (**d'où l'importance des sauvegardes**)

3. **Changer ses mots de passe** après avoir nettoyé le réseau

# 7. Renforcement de la protection avec Sophos System Protector et Malicious Traffic Detector

**Sophos System Protector**, appuyé par le module **Malicious Traffic Detection (MTD)** et qui est déjà disponible dans Sophos Cloud, et le sera prochainement dans les versions gérées par Sophos Enterprise Console 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.

# 8. Liens utiles

**Support Sophos :** articles à jour en français
http://www.sophos.com/fr-fr/support/knowledgebase/120797.aspx
http://www.sophos.com/fr-fr/support/knowledgebase/119006.aspx

**Explication détaillée :**
CERT : http://cert.ssi.gouv.fr/site/CERTFR-2014-ACT-007/