MALWARE CRYPTOLOCKER RANSOMWARE

PRÉCONISATIONS TECHNIQUES ET ORGANISATIONNELLES

04 OCTOBRE 2016

SOMMAIRE

Définition d'un malware

Un **malware** est un code malveillant qui, une fois exécuté sur un poste ou un serveur va avoir une activité néfaste pour l'organisation infectée :

- Vol de données
- Vol d'identifiants et de mots de passe (messagerie, intranet, banque, e-commerce….)
- Altération ou destruction de fichiers ou bases de données
- Spamming avec usurpation d'identité
- Propagation de malware
- Chiffrement des données locales et des lecteurs réseaux (cryptolocker)
- Chiffrement et blocage du poste ou du serveur avec demande de rançon (ransomware)
- Utilisation des ressources de l'organisation pour perpétrer des attaques vers d'autres cibles

Vecteurs d’infection d’un malware

Il existe plusieurs vecteurs d’infection qui sont :

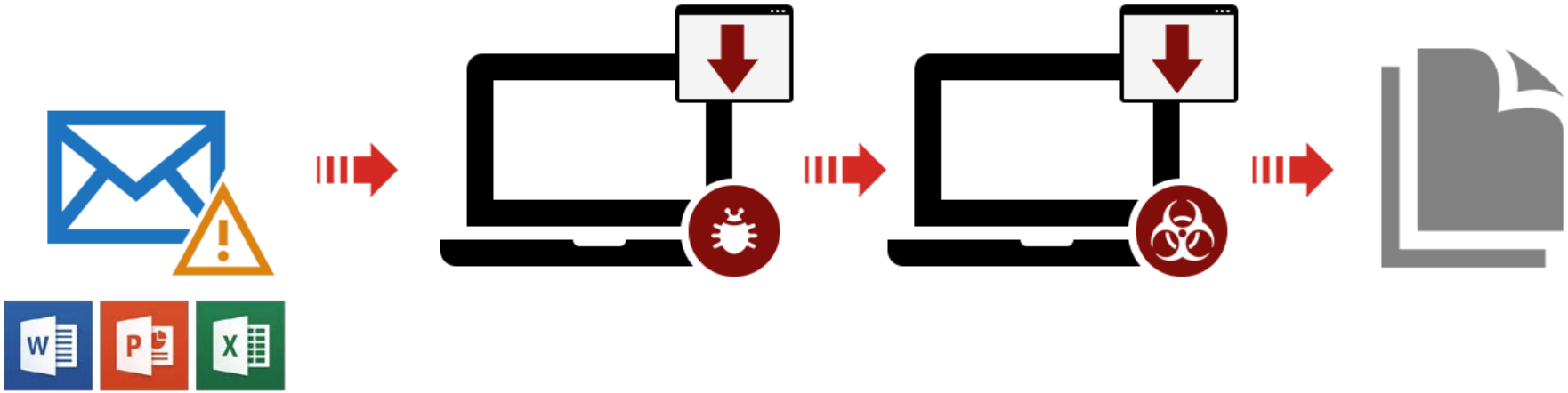
- Le mail frauduleux avec une pièce-jointe piégée (excel, word, zip…)
- Le mail frauduleux avec lien vers une page piégée
- Le téléchargement d’applications piégées
- Les supports de stockage (clé USB, disque sans fil)
- Le manque de contrôle des équipements se connectant au réseau de l’Organisation

SOMMAIRE

GROUPE acesi

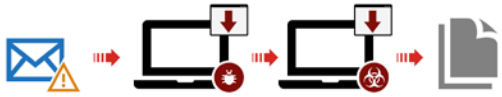
Mode de fonctionnement d'un cryptolocker

Via un mail et une pièce-jointe piégée



Mode de fonctionnement d'un cryptolocker

Via un mail et une pièce-jointe piégée

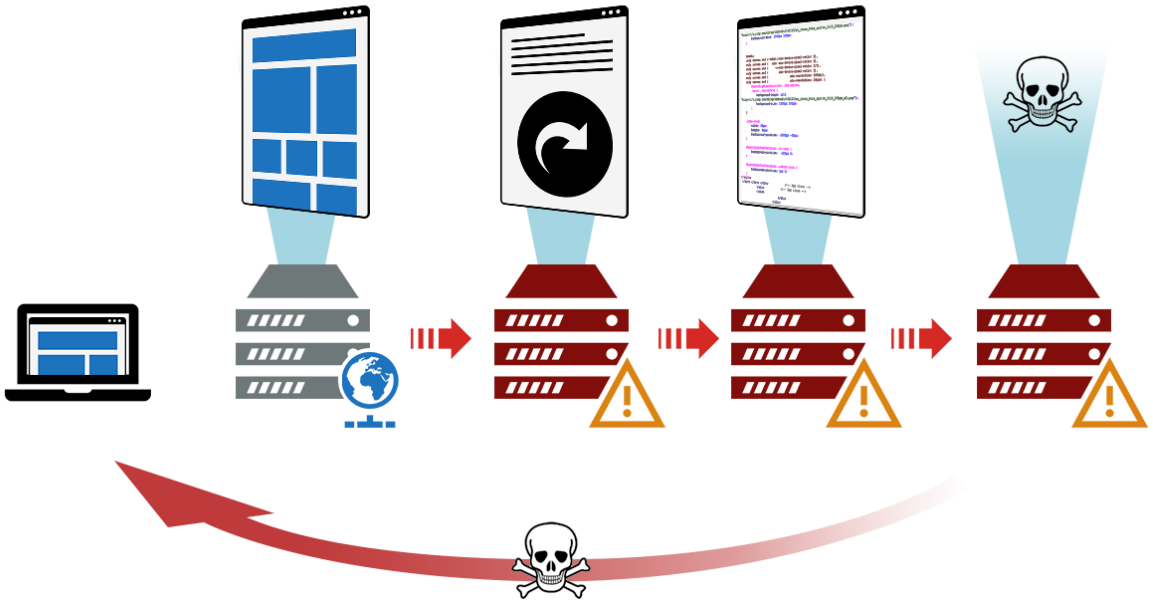


Un mail de spam, plus ou moins bien rédigé arrive dans la boite d'un utilisateur :

- L'utilisateur ouvre la pièce-jointe (souvent un word ou un zip)
- Le fichier word ou zip demande l'autorisation d'exécuter **une macro**
- L'utilisateur exécute la macro
- Cette macro va télécharger sur les sites des pirates, les briques pour construire son outil malveillant.
- Le malware commence son travail

Mode de fonctionnement d'un cryptolocker

Via des pages web piégées



Mode de fonctionnement d'un cryptolocker

Via des pages web piégées

Un mail de spam, plus ou moins bien rédigé arrive dans la boite d'un utilisateur :

- L'utilisateur clique sur le lien
- Le navigateur va ouvrir la page avec les droits de l'utilisateur
- La page malveillante va rechercher des vulnérabilités sur le navigateur, ses plugins et la machine
- La page malveillante va exploiter les vulnérabilités découvertes pour charger son malware sur le poste de la victime
- Le malware commence son travail

Propagation d’un cryptolocker

En utilisant les ressources de la victime

Après avoir infecté sa victime, le cryptolocker va :

- Récupérer les contacts de la victime
- Forger un nouvel email en usurpant l’identité, la signature et le réseau de la victime pour cibler les contact **=>** le mail ainsi forgé est propre, avec peu de critères de qualification *spam* et ressemble en tous points à un mail légitime favorisant la confiance des cibles.

SOMMAIRE

Parades techniques

Comment limiter techniquement les risques d'infection, le 100% n'existe pas !

Une passerelle SMTP antispam

Mise en place de filtrage web HTTP et HTTPS (EAL4+)

Une solution d'inspection des exécutables avec sandboxing

Une stratégie de contrôle d'accès au réseau 802.1x

Une solution antivirale endpoint de nouvelle génération

Une solution d'inspection des flux réseaux au niveau firewall

Une solution d'analyse comportementale du poste

Mise en œuvre d'un plan de sauvegarde et de restauration efficace

SOMMAIRE

Parades organisationnelles

Augmenter la fréquence de mise à jour du moteur antiviral (toutes les 15 minutes)

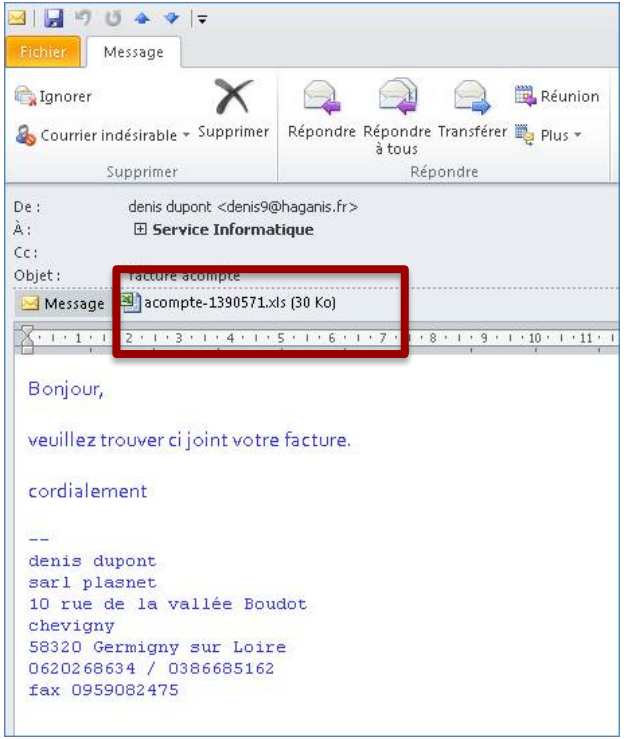
Sensibilisation et formation des utilisateurs

Sensibilisation et formation des administrateurs

Mise en œuvre de contrôles (audits internes, campagnes d'ingénierie sociales)

Conduite de plans de test du PRA/PCA

Exemple de mail contaminant




```
-$~=~|
+.*~*
.+-+$~.*~*_
        !!! INFORMATION IMPORTANTE !!!!

Tous vos fichiers ont été chiffrés avec les algorithmes RSA-2048 et AES-128.
Plus d'informations peuvent être trouvées ici:
    http://fr.wikipedia.org/wiki/Chiffrement_RSA
    http://fr.wikipedia.org/wiki/Advanced_Encryption_Standard

Déchiffrer vos fichiers est seulement possible en utilisant la clé privée et le programme
de déchiffrement se trouvant sur notre serveur secret.
Pour recevoir votre clé privée suivez l'un de ces liens:
    1. http://jhomitevd2abj3fk.tor2web.org/7B8F205946281571
    2. http://jhomitevd2abj3fk.onion.to/7B8F205946281571

Si aucune de ces adresses ne fonctionne, suivez ces instructions:
    1. Téléchargez et installez le navigateur Tor: https://www.torproject.org/download/download-easy.html
    2. Après son installation, démarrez-le et attendez son initialisation.
    3. Tapez dans la barre d'adresse: jhomitevd2abj3fk.onion/7B8F205946281571
    4. Suivez les instructions du site.

!!! Votre identifiant personnel: 7B8F205946281571 !!!
.+~_*+.+.=._~|$
```

SOMMAIRE

Conduite à tenir en cas d'infection à cryptolocker

En cas d'infection, le temps de réaction doit être le plus court possible afin de limiter au maximum les actions des malwares.
Il convient :

- D'identifier la ou les machines infectées
- De les déconnecter du réseau
- De communiquer à l'ensemble des collaborateurs sur l'incident de sécurité
- De demander à l'ensemble des collaborateurs d'exécuter un scan antivirus sur leur poste
- De contacter son prestataire afin d'auditer l'infrastructure et de définir l'impact
- De réinstaller intégralement les données, les postes ou serveurs infectés depuis la dernière sauvegarde saine.