Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 27 juin 2017
N° CERTFR-2017-INF-001

Affaire suivie par :
CERT-FR

NOTE D'INFORMATION DU CERT-FR

Objet : Protection contre les rançongiciels

Gestion du document

Référence	CERTFR-2017-INF-001
Titre	Protection contre les rançongiciels
Date de la première version	27 juin 2017
Date de la dernière version	–
Source(s)	–
Pièce(s) jointe(s)	Aucune

TAB. 1 – *Gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

Secrétariat général de la défense et de la sécurité nationale – ANSSI – COSSI – CERT-FR
51, bd de La Tour-Maubourg **Tél.**: 01 71 75 84 50 **Web**: http://cert.ssi.gouv.fr
75700 Paris 07 SP **Fax**: 01 71 75 84 70 **Mél** : cert-fr.cossi@ssi.gouv.fr

1 - Les rançongiciels

Les rançongiciels (ransomware en anglais) constituent une catégorie de programmes malveillants visant à obtenir le paiement d'une rançon. Pour ce faire, le programme malveillant essaie le plus souvent d'empêcher l'utilisateur d'accéder à ses fichiers, par exemple en les chiffrant, et lui affiche des instructions afin que celui-ci paie une rançon. Lorsqu'un ordinateur est infecté, les fichiers de cet ordinateur peuvent être bloqués, mais les conséquences peuvent aussi s'étendre au reste du système d'information. Ainsi, un partage de fichiers monté sur une seule machine infectée se retrouvera probablement concerné et risque ainsi d'impacter un plus grand nombre d'utilisateurs. De même, si l'infection initiale arrive souvent (mais pas nécessairement) par un courrier électronique piégé, le programme peut aussi chercher à se propager de manière autonome sur le reste du système d'information et au travers de ses interconnexions en exploitant des vulnérabilités à distance. Si certains de ces programmes comportent des défauts de fabrication permettant de retrouver partiellement ou totalement les données concernées, d'autres utilisent des méthodes proches de l'état de l'art et peuvent condamner l'accès aux fichiers si la clé de déchiffrement n'est pas obtenue. Il s'agit donc effectivement d'une menace à prendre très au sérieux et dont il vaut mieux chercher à se prémunir avant qu'il ne soit trop tard.

2 - Prévention

Assurer un bon niveau de sécurité global du système d'information

Pour infecter de manière automatisée une machine, un rançongiciel doit utiliser une vulnérabilité (ex: macro malveillante dans un document piégé, vulnérabilité logicielle d'un service réseau, mot de passe par défaut, etc.). Ainsi, afin de réduire les possibilités offertes à un rançongiciel de s'introduire, il convient d'assurer un bon niveau de sécurité global du système d'information. Si l'objectif de ce document n'est pas de constituer un guide de sécurisation d'un système d'information, quelques bonnes pratiques sont par exemple référencées dans le guide d'hygiène de l'ANSSI. Parmi les mesures s'appliquant particulièrement dans le cadre de ce document, on peut citer:

- appliquer les correctifs de sécurité fournis par les éditeurs;
- restreindre les programmes autorisés à être exécutés: application de stratégies de restriction logicielle ou de Applocker pour les systèmes Windows, options de montage en lecture seule des répertoires temporaires et de l'utilisateur pour les systèmes UNIX;
- durcir la configuration des logiciels bureautiques ou manipulant des données provenant d'Internet: restreindre l'autorisation des macros dans les suites bureautiques, désactiver le moteur Javascript des lecteurs PDF, activer les bacs à sable (sandbox) des logiciels le permettant, installer des extensions dédiées aux navigateurs Internet pour restreindre par défaut l'interprétation de code Javascript, etc.;
- configurer le pare-feu des postes de travail pour empêcher les flux de poste à poste ;
- lorsque des anti-virus sont employés sur les postes ou sur les passerelles de messagerie, veiller à la mise à jour fréquente des signatures et du moteur du logiciel;
- minimiser les droits sur les partages réseau: s'assurer que le droit en écriture n'est accordé qu'aux utilisateurs en ayant réellement le besoin et contrôler régulièrement les droits d'accès;
- effectuer des sauvegardes et des tests de restauration. Procéder à la mise hors ligne des sauvegardes des éléments les plus sensibles. Ces points sont développés par la suite;
- effectuer des audits et des tests d'intrusion réguliers et mettre en place un plan d'action pour corriger les défauts mis en évidence.

Sensibiliser les utilisateurs

Si le rançongiciel n'affecte pas de manière automatisée une machine, le vecteur d'infection sera l'utilisateur, que ce soit à son insu en ouvrant une pièce jointe piégée ou par inadvertance en désactivant une protection (technique d'ingénierie sociale incitant l'utilisateur à effectuer une action). La sensibilisation des utilisateurs est ainsi primordiale:

- ne pas ouvrir les pièces jointes des messages électroniques suspects(fautes d'orthographes, pièces jointes au nom trop succinct ou trop générique, etc.). Il faut toutefois noter que la caractéristique d'un courriel de type «hameçonnage ciblé» (spear phishing) est de personnaliser le contenu par rapport à l'environnement de l'utilisateur afin de duper sa vigilance ;

– ne pas suivre les liens des messages électroniques suspectset vérifier la cohérence entre l'adresse affichée dans le contenu et le lien effectif. Il faut toutefois noter que les attaques de type XSS (cross-site scripting) ou par point d'eau (watering hole) rendent inefficace cette pratique;
– ne pas réactiver des fonctionnalités désactivées dans la configuration des logiciels, même si le fichier ouvert y incite par un message particulier.

Effectuer des sauvegardes

La charge malveillante des rançongiciels étant de chiffrer des fichiers, la principale mesure permettant d'éviter les pires conséquences consiste à réaliser des sauvegardes, en priorité des serveurs de fichiers et des applications métier critiques. Il convient de garder à l'esprit que ces sauvegardes peuvent aussi, intentionnellement ou non, être victimes d'un rançongiciel. Il convient donc de les protéger de manière adéquate. Le moyen, souvent le plus sûr, mais aussi le plus simple, consiste à stocker une copie de ces sauvegardes sur un support déconnecté. Dans de nombreux cas, de simples disques durs amovibles peuvent suffire. Sur un périmètre large, cette méthode peut être privilégiée pour les données les plus sensibles. Des tests de restauration des sauvegardes doivent être régulièrement effectués afin de s'assurer que la procédure soit connue et que les sauvegardes soient complètes et intègres. Par ailleurs, pour des besoins particuliers, notamment en environnement industriel, s'assurer de la disponibilité d'équipements de secours dont les configurations sont sauvegardées hors ligne est primordial. De même, la possibilité de remplacer immédiatement un poste de commande doit être établie (image disque, équipements de spare à froid, poste ou chaine dupliquée hors ligne, etc.).

3 - En cas d'infection

Débrancher la machine du réseau informatique

Afin d'arrêter la propagation de l'infection hors de la machine victime, il convient de l'isoler du réseau en débranchant le câble réseau. Il est également nécessaire de vérifier si une éventuelle connexion sans fil (Wi-Fi) est présente et, le cas échéant, de la désactiver, de préférence avec l'interrupteur matériel.

Ne pas éteindre la machine concernée

Il est parfois possible de retrouver en mémoire des éléments permettant de recouvrer les fichiers victimes. Cependant, l'extinction d'une machine ou l'ancienneté d'une infection peuvent réduire les chances de fonctionnement d'une éventuelle méthode de recouvrement. Si la machine le permet, il est recommandé d'activer la mise en veille prolongée, afin d'arrêter l'activité du programme malveillant tout en préservant la mémoire pour une analyse ultérieure. Parallèlement, au cas où le processus de chiffrement n'aurait pas été terminé, les fichiers peuvent être copiés sur un support amovible vierge. Ceux-ci pourront éventuellement être traités plus tard à des fins de récupération en gardant à l'esprit que leur intégrité et leur innocuité ne peuvent être assurées.

Bloquer les nouvelles infections sur la base des éléments connus

Lorsque le programme malveillant qui a réalisé l'infection est identifié, il est possible de rechercher sur Internet ou dans les journaux du système d'information des éventuelles caractéristiques de celui-ci (URL utilisées, nom de fichier, sujet du courrier électronique, etc.). Ces éléments peuvent être utilisés pour éviter d'autres infections. Des actions peuvent notamment être entreprises sur les passerelles de messagerie, les passerelles de navigation sur Internet ou les serveurs de boîte aux lettres.

Restaurer le système depuis des sources saines

La machine ayant été infectée par un programme malveillant, l'intégrité du système peut d'autant plus être mise en doute. Plutôt que d'espérer qu'un éventuel utilitaire de désinfection ramène le système dans un état sain, il est préférable de réinstaller le système depuis un support connu et de restaurer les données depuis les sauvegardes ayant préalablement été effectuées. L'efficacité ou l'innocuité de méthodes de nettoyage alternatives sont difficiles à qualifier. Le vecteur initial de propagation doit par ailleurs être corrigé après réinstallation des systèmes, afin d'éviter une nouvelle infection: application des correctifs de sécurité, changement des mots de passe, modification du pare-feu local, etc.

En l'absence de sauvegarde, rechercher la disponibilité de méthodes de recouvrement des données

Comme cela a été mentionné, des défauts de conception des rançongiciels sont parfois découverts et peuvent permettre un recouvrement total ou partiel des données. Si les données victimes n'ont pas été préalablement sauvegardées et que leur niveau d'importance le justifie, un dernier recours peut être de rechercher d'éventuels utilitaires de recouvrement, proposés notamment par les éditeurs d'antivirus. Cependant, il faut faire preuve de vigilance et qualifier la provenance de ces utilitaires, car ceux-ci pourraient se révéler malveillants et provoquer une surinfection.

Ne pas payer la rançon

Outre le fait que payer la rançon entretient le système frauduleux, le paiement ne garantit nullement l'obtention d'une quelconque clé de déchiffrement ni la sécurité des moyens de paiement utilisés.

Gestion détaillée du document

27 juin 2017 version initiale.