Objet: Campagne de messages électroniques non sollicités de type Locky Locker

S.G.D.S.N

Agence nationale
de la sécurité des
systèmes d'information

Paris, le 03 août 2018

N° CERTFR-2018-ALE-008

Affaire suivie par: CERT-FR

le 03 août 2018

Bulletin d'alerte du CERT-FR

Gestion du document

Référence	CERTFR-2018-ALE-008
Titre	Campagne de messages électroniques non sollicités de type Locky Locker
Date de la première version	03 août 2018
Date de la dernière version	10 octobre 2018
Source(s)	

Pièce(s) jointe(s)	Aucune(s)

Tableau 1: Gestion du document

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

Risque(s)

Installation d'un logiciel malveillant de type Locky.

Systèmes affectés

Tous les systèmes d'exploitations Windows peuvent être victimes de ce logiciel malveillant.

Résumé

Depuis la fin juillet 2018, le CERT-FR constate une nouvelle campagne de courriels distribuant le rançongiciel Locky touchant actuellement la France. Les messages sont accompagnés d'un lien hypertexte encourageant à télécharger la facture d'une commande. Le taux de blocage par les passerelles anti-pourriel est relativement faible.

Un rançongiciel est un programme malveillant qui chiffre les données du poste compromis. Il va également cibler les partages de fichiers accessibles depuis le compte utilisateur dont la session est compromise. Celui-ci est exécuté, dans le cas présent, par une action de l'utilisateur. La victime est ensuite invitée à verser de l'argent afin que l'attaquant déchiffre les fichiers ciblés.

Dans le cadre de cette campagne, et d'après les échantillons que le CERT-FR a observés, la diffusion de Locky Locker s'effectue par l'intermédiaire d'un pourriel dans lequel se trouve un lien pour télécharger une facture. La facture téléchargée est une archive zip dans une autre archive zip contenant un exécutable.

Dans les échantillions que le CERT-FR a pu observé, l'objet du message est "Nous avons reçu votre paiement.".

Le corps du message se présente sous la forme suivante:

****

Madame, Monsieur,

Nous vous notifions que votre commande du XX/XX/2018 d'un montant de XXX€ a bien été enregistrée.
Le contenu de votre commande est détaillé dans la facture téléchargeable en cliquant ici

Tout changement sur l'état de votre commande (préparation, expédition, etc.) vous sera automatiquement et immédiatement notifié par email.

L'expédition du produit aura lieu 24 heures au plus après le passage à l'état "validé" de votre demande.
Toute commande qui nous parvient incomplète demande des délais de traitement supplémentaires dont nous ne saurions être tenus responsables.
****

Noms de domaines liés au téléchargement de Locky Locker:

hxxp://centredentairenantes[.]fr_BAD/wp-system.php
hxxps://savigneuxcom.securesitefr[.]com_BAD/client.php?fac=001838274191030

Solution

Mesures préventives

Le CERT-FR recommande de sensibiliser les utilisateurs aux risques associés aux messages électroniques pour éviter l'ouverture de pièces jointes. Il convient en effet de ne pas cliquer sans vérification préalable sur les liens de messages et les pièces jointes. Les utilisateurs ne doivent pas ouvrir des messages électroniques de provenance inconnue, d'apparence inhabituelle ou frauduleuse. Plus généralement, il convient de mettre à jour les postes utilisateurs, notamment le système d'exploitation et les applications exposées sur Internet (lecteur PDF, lecteur messagerie, navigateurs et greffons) dans le cas où le code malveillant (ou une variante) exploiterait une vulnérabilité logicielle.

Le CERT-FR recommande également de mettre à jour les logiciels antivirus du parc informatique (postes utilisateurs, passerelle de messagerie, etc.). Le code malveillant étant polymorphe, les éditeurs antivirus ont besoin de publier des signatures en constante évolution. Par ailleurs, il convient d'envoyer dès que possible un exemplaire du code malveillant à votre éditeur de logiciel antivirus si la variante n'est pas détectée par ce dernier.

Enfin, le CERT-FR recommande d'effectuer des sauvegardes saines et régulières des systèmes et des données (postes de travail, serveurs) puis de vérifier qu'elles se sont correctement déroulées. Les sauvegardes antérieures ne doivent pas être écrasées (cas où une version chiffrée aurait été sauvegardée). Les sauvegardes doivent être réalisées en priorité sur les serveurs hébergeant des données critiques pour le fonctionnement de l'entité. Celles-ci doivent être stockées sur des supports de données isolés du réseau en production.

Mesures réactives

Si le code malveillant est découvert sur vos systèmes, le CERT-FR recommande de déconnecter immédiatement du réseau les machines identifiées comme compromises. L'objectif est de bloquer la poursuite du chiffrement et la destruction des documents partagés. Le CERT-FR recommande aussi d'alerter le responsable sécurité ou le service informatique au plus tôt. Le temps de revenir à une situation normale, le CERT-FR recommande également de positionner les permissions des dossiers partagés en LECTURE SEULE afin d'empêcher la destruction des fichiers sur les partages. Les personnels pourront continuer de travailler localement et mettre à jour ultérieurement le partage. Aussi, le CERT-FR recommande de prendre le temps de sauvegarder les fichiers importants sur des supports de données isolés. Ces fichiers peuvent être altérés ou encore être infectés. Il convient donc de les traiter comme tels. De plus, les sauvegardes antérieures doivent être préservées d'écrasement par des sauvegardes plus récentes.

Le CERT-FR recommande également de bloquer sur le serveur mandataire l'accès aux domaines ou URLs identifiés dans le message malveillant. L'objectif est de prévenir toute nouvelle compromission sur le même site. En complément, le CERT-FR recommande de rechercher et supprimer les messages malveillants similaires dans les boîtes de messagerie des utilisateurs. Par ailleurs, le CERT-FR recommande la réinstallation complète du poste et la restauration d'une sauvegarde réputée saine des données de l'utilisateur. De plus, dans le cadre de l'utilisation de profils itinérants, il convient de supprimer la copie serveur du profil afin de prévenir la propagation des codes malveillants par ce biais.

Enfin, les fichiers chiffrés peuvent être conservés par la victime au cas où dans le futur, un moyen de recouvrement des données originales serait découvert.

Gestion détaillée du document

le 03 août 2018
Version initiale

le 09 août 2018
Correction d'inexactitudes dans l'objet du courriel de hameçonnage et dans le protocole de l'url contenant savigneuxcom.securesitefr[.]com

le 10 octobre 2018
Clôture de l'alerte.