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 14 mai 2017
N° CERTFR-2017-ALE-011

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Campagne de messages électroniques non sollicités de type Jaff

Gestion du document

Référence	CERTFR-2017-ALE-011
Titre	Campagne de messages électroniques non sollicités de type Jaff
Date de la première version	14 mai 2017
Date de la dernière version	14 mai 2017
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.

1 - Risque(s)

Installation et propagation d'un logiciel malveillant de type rançongiciel, voire, à terme, d'autres logiciels malveillants.

2 - Vecteurs d'infection

Le vecteur d'infection initial est un courriel avec une pièce jointe malveillante de type PDF.

3 - Systèmes affectés

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

4 - Résumé

Depuis le 11 mai 2017, le CERT-FR constate une nouvelle campagne de courriels malveillants contenant des pièces jointes au format PDF. Ce PDF contient un document embarqué au format DOCM contenant lui-même une macro malveillante lançant le téléchargement puis l'exécution du rançongiciel Jaff. Dans le cadre de cette campagne, et d'après les échantillons que le CERT-FR a observés, les URLs de téléchargement du rançongiciel Jaff se terminent avec les motifs suivants :

– /f87346b

– /77g643

Ces motifs peuvent donc être utilisés comme méthode de détection et/ou de blocage, dans la mesure des capacités techniques disponibles. Par ailleurs, plusieurs éditeurs ont déjà publié des indicateurs de compromission qui peuvent être utilisés afin de détecter Jaff.

Le CERT-FR attire l'attention sur le fait que cette campagne de distribution du rançongiciel Jaff n'est pas liée à celle du rançongiciel Wannacry dont le vecteur d'infection initial n'est toujours pas confirmé.

5 - Contournement provisoire

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 de configurer sur les postes de travail les restrictions logicielles pour empêcher l'exécution de code à partir d'une liste noire de répertoires :

- Si la solution utilisée est AppLocker, les règles de blocage suivantes doivent être définies :
  - OSDRIVE\Users*\AppData\
  - OSDRIVE\Windows\Temp\
- Si les restrictions logicielles (SRP) sont utilisées, les règles de blocage suivantes doivent être définies :
  - UserProfile\AppData
  - SystemRoot\Temp

Il est important de vérifier que le service "Application Identity" (AppIDSvc) est paramétré en démarrage automatique sur l'ensemble des postes pour que les restrictions logicielles soient opérantes (ce mode de démarrage peut être paramétré à travers une politique de groupe sur le domaine Windows). Si des dysfonctionnements sont rencontrés suite au déploiement de ces règles de blocage, il est nécessaire d'identifier les applications légitimes situées dans ces répertoires, et de définir des règles en liste blanche afin d'autoriser leur exécution.

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.

Cette alerte sera maintenue tant que le volume de message électronique constaté sera considéré significatif par le CERT-FR.

6 - Documentation

Indicateurs de compromission identifiés par l'éditeur Talos :

- `https://alln-extcloud-storage.cisco.com/ciscoblogs/jaff-domains-unique.txt`

Gestion détaillée du document

14 mai 2017 version initiale ;