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 10 mars 2016
N° CERTFR-2015-ALE-015-003

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Campagne de messages électroniques non sollicités de type TeslaCrypt

Gestion du document

Référence	CERTFR-2015-ALE-015
Titre	Campagne de messages électroniques non sollicités de type TeslaCrypt
Date de la première version	21 décembre 2015
Date de la dernière version	10 mars 2016
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 d'un logiciel malveillant de type TeslaCrypt.

2 - Systèmes affectés

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

3 - Résumé

Depuis le début du mois de décembre 2015, et plus massivement depuis la mi-décembre 2015, le CERT-FR constate à l'échelle nationale une vague de pourriels dont le taux de blocage par les passerelles anti-pourriel est relativement faible. Ces pourriels ont pour objectif la diffusion du rançongiciel TeslaCrypt.

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 TeslaCrypt s'effectue par l'intermédiaire d'un pourriel dans lequel se trouve une pièce jointe au format zip. Cette archive contient un fichier offusqué au format js (javascript) dont l'objectif est la récupération puis l'exécution du malware. L'exécution de ce dernier entraine le chiffrement des données et les fichiers sont renommés avec l'extension ".vvv".

Il est intéressant de noter que le binaire est jusqu'à présent composé de deux chiffres et de l'extension ".exe". Cette caractéristique peut permettre le blocage ou la mise en place d'alertes via les serveurs mandataires.

À l'aide les échantillons remontés, le CERT-FR a constaté que les URLs de téléchargement du binaire TeslaCrypt sont les suivantes (toutes les URLs suivantes ont été démilitarisées par l'adjonction du suffixe ._BAD_ aux noms de domaines et adresses IP) :

- http://5.39.222.193_BAD_/73.exe
- http://46.151.52.196_BAD_/80.exe
- http://46.151.52.196_BAD_/86.exe
- http://46.151.52.197_BAD_/73.exe
- http://46.151.52.197_BAD_/80.exe
- http://46.151.52.197_BAD_/85.exe
- http://46.151.52.197_BAD_/86.exe
- http://46.151.52.231_BAD_/87.exe
- http://74.117.183.84_BAD_/73.exe
- http://777advisors.com_BAD_/85.exe
- http://aawraa.com_BAD_/wp-includes/theme-compat/73.exe
- http://avtimespg.com_BAD_/73.exe
- http://abortoptions.com_BAD_/wp-includes/images/smilies/85.exe
- http://aboutacquisitions.com_BAD_/wp-includes/theme-compat/85.exe
- http://acabadosintegrales.com_BAD_/wp-includes/js/mediaelement/73.exe
- http://achesoncorner.com_BAD_/wp-includes/fonts/73.exe
- http://acsbrokerage.com_BAD_/css/fonts/__pages_sources/85.exe
- http://actuvillage.com_BAD_/images/thumbs/73.exe
- http://areyouwevenlisten.com_BAD_/73.exe
- http://artskorat.com_BAD_/html/images/80.exe
- http://auctorit.com_BAD_/beta/js/73.exe
- http://aycenergy.com_BAD_/wp/wp-includes/fonts/80.exe
- http://autocraftmedia.com_BAD_/mappalachian/tmp/73.exe
- http://babykucomel.com_BAD_/wp-admin/js/73.exe
- http://balwindersingh.in_BAD_/bsdemo/js/73.exe
- http://baneyconstruction.com_BAD_/kldf/cachec50da2243ebb9d634cfad3427cafcc61/73.exe
- http://bareknucklebabes.com_BAD_/wp-admin/maint/73.exe
- http://bauelementeberater.info_BAD_/73.exe
- http://beandbecomeadvising.com_BAD_/wp-admin/maint/73.exe
- http://beatifulgdf9dr.com_BAD_/73.exe
- http://bellychef.com_BAD_/wp-includes/theme-compat/73.exe
- http://bereanbibledenver.com_BAD_/wp-admin/js/73.exe
- http://bestsurfinglessons.com_BAD_/wp-includes/theme-compat/73.exe
- http://betterhealth4us.com_BAD_/wp-includes/fonts/73.exe
- http://bfcaterers.com_BAD_/wp-includes/certificates/73.exe
- http://fernytowd.com_BAD_/73.exe
- http://fernytowd.com_BAD_/80.exe
- http://firstwetakemanhat.com_BAD_/80.exe
- http://firstwetakemanhat.com_BAD_/91.exe
- http://gammus.com_BAD_/69.exe
- http://gammus.com_BAD_/73.exe
- http://goonricerwiththat.com_BAD_/69.exe
- http://goonricerwiththat.com_BAD_/80.exe
- http://hopemillsglassco.com_BAD_/wp-includes/fonts/85.exe
- http://iamthewinnerhere.com_BAD_/73.exe
- http://iamthewinnerhere.com_BAD_/80.exe
- http://iamthewinnerhere.com_BAD_/97.exe
- http://ifyougowegotoo.com_BAD_/90.exe
- http://ifyougowegotoo.com_BAD_/94.exe

- http://igonnafuckyougood.com_BAD_/73.exe
- http://igonnafuckyougood.com_BAD_/80.exe
- http://miracleworld1.com_BAD_/80.exe
- http://miracleworld1.com_BAD_/91.exe
- http://prestakitchen.com_BAD_/wp-includes/pomo/85.exe
- http://soft2webextrain.com_BAD_/87.exe
- http://softextrain64.com_BAD_/80.exe
- http://softextrain64.com_BAD_/86.exe
- http://soughreneg.com_BAD_/93.exe
- http://soughreneg.com_BAD_/94.exe
- http://washawaydesctrucion.com_BAD_/90.exe
- http://whatdidyaysay.com_BAD_/73.exe
- http://whatdidyaysay.com_BAD_/80.exe
- http://whatdidyaysay.com_BAD_/97.exe

4 - Solution

Solutions 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.

Solutions 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. Sur ce point, il est intéressant de noter que le déchiffrement des fichiers impactés par la version de TeslaCrypt utilisée lors de cette campagne semble, dans certains, cas envisageable. En effet, un projet comme TeslaCrack peut s'avèrer efficace mais nécessite plusieurs étapes de mise en oeuvre (récupération de dépendances, compilations, ...) mais aussi obligatoirement une étape d'initialisation (factorisation) qui peut être très coûteuse en temps d'exécution.

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

5 - Documentation

– Projet TeslaCrack
https://github.com/Googulator/TeslaCrack

Gestion détaillée du document

21 décembre 2015 version initiale ;
31 décembre 2015 ajout de marqueurs supplémentaires ;
15 janvier 2016 mise à jour des mesures réactives ;
10 mars 2016 clôture de l'alerte ;