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 juillet 2015
N° CERTFR-2015-ALE-003-001

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Nouvelle campagne d'hameçonnage de type rançongiciel

Gestion du document

Référence	CERTFR-2015-ALE-003-001
Titre	Nouvelle campagne d'hameçonnage de type rançongiciel
Date de la première version	05 février 2015
Date de la dernière version	10 juillet 2015
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)

Atteinte à la disponibilité des fichiers après chiffrement.

2 - Systèmes affectés

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

3 - Résumé

Depuis le début du mois de février 2015, le CERT-FR constate une nouvelle vague importante de compromissions de type rançongiciel, qui utilise cette fois principalement le programme malveillant appelé CTB-Locker.

Un **rançongiciel** est un code malveillant qui chiffre les données du poste compromis. Il va également cibler les partages de fichiers accessibles en écriture à l'utilisateur dont la session est compromise. À travers une boîte de dialogue, la victime est ensuite invitée à verser de l'argent afin de récupérer la clé qui permettra de déchiffrer les documents ciblés (Bitcoin, Paypal, carte bleue). Il n'existe pas de moyens fiables pour récupérer la clé utilisée par le code malveillant.

Attention, le CERT-FR tient à souligner que le recouvrement des données après paiement n'est en aucun cas garanti. Au-delà du fait que cela encourage ce type d'attaque, le recours à un moyen de paiement par carte bleue expose la victime à des utilisations frauduleuses de celle-ci.

Méthode d'attaque:

Dans le cas présent, la propagation constatée repose sur une campagne d'hameçonnage. Les messages malveillants reçus prétendent être accompagnés d'un fax en pièce jointe, qui en réalité est un programme malveillant.

Ce code s'installe localement sur le poste par différents moyens :

- fichier avec l'extension SCR ;
- fichier avec l'extension SCR compressé dans un fichier au format zip (parfois il s'agit de compressions imbriquées) ;
- fichier avec l'extension CAB ;
- fichiers exécutables classiques (.EXE).

Le fichier avec l'extension SCR est un fichier exécutable : ce dernier télécharge ensuite le code malveillant réalisant le chiffrement des fichiers.

4 - Solution

Mesures préventives

Le CERT-FR recommande de sensibiliser les utilisateurs aux risques associés aux messages électroniques pour éviter l'ouverture de pièces jointes de type SCR, CAB ou EXE. 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 de messages électroniques de provenance inconnue, d'apparence inhabituelle ou frauduleuse.

Le CERT-FR recommande également de filtrer les fichiers portant l'extension SCR, EXE et CAB en pièce jointe des messages électroniques. Si l'échange de tels fichiers est indispensable dans certains contextes fonctionnels, il convient de bloquer ces fichiers globalement et de ne les autoriser que pour les boites de messageries qui le nécessitent absolument. Par ailleurs, si la passerelle de messagerie le permet, il est recommandé de réaliser ce filtrage également dans les fichiers des archives ZIP.

Plus généralement, il convient de mettre à jour les postes utilisateur, 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`

(cf les recommandations de l'ANSSI à ce sujet dans la partie "Documentation")

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 utilisateur, 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. Une liste d'URL connues du CERT-FR est fournie en annexe, toutefois il est bien précisé qu'elle n'est pas exhaustive.

En complément, le CERT-FR recommande de rechercher et supprimer les messages malveillants similaires dans les boîtes de messagerie des utilisateurs

Enfin, 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.

Néanmoins, le CERT-FR souhaite faire remarquer que des fichiers chiffrés peuvent être conservés par la victime au cas où dans le futur, un moyen de recouvrement des données originales serait découvert.

Annexes : marqueurs de CTB-Locker

Cette liste de marqueurs n'est pas exhaustive et susceptible d'être mise à jour ultérieurement.

Champs "Objet" de messages malveillants

```
[Fax server] +07909 546940
copy from +07540040842
Message H4H2LC68B7167E4F4
New incoming fax message, S8F8E423F9285C5
Incoming fax from +07843-982843
[Fax server]:+07725-855368
Fax ZC9257943991110
New fax message from +07862-678057
```

Liens utilisés pour le téléchargement du logiciel malveillant

```
hxxp://agatecom.fr/voeux/doom.tar.gz
hxxp://aspiroflash.fr/cai/abc.tar.gz
hxxp://baselineproduction.fr/Modules/doom.tar.gz
hxxp://bikeceuta.com/templates/nero.tar.gz
hxxp://breteau-photographe.com/tmp/pack.tar.gz
hxxp://cargol.cat/IESABP/nero.tar.gz
hxxp://cds-chartreuse.fr/locales/sancho.tar.gz
hxxp://cognacbrown.co.uk/ChromeSetup.exe
hxxp://collection-opus.fr/_gfx/cario.tar.gz
hxxp://compassfx.com/OLD/cario.tar.gz
hxxp://dariocasati.it/logs/dostanes_do_drzky.tar.gz
hxxp://dequinnzangersborne.nl/language/upupup.tar.gz
hxxp://dieideenwerkstatt.at/css/abc.tar.gz
hxxp://evalero.com/img/cario.tar.gz
hxxp://fbrugues.com/language/hiser.tar.gz
hxxp://firststepbahamas.com/PDF/abc.tar.gz
```

```
hxxp://fotocb.de/php/upupup.tar.gz
hxxp://funnydeando.com/pdthm0/moon1.exe
hxxp://hotel-mas-saint-joseph.com/css/pack.tar.gz
hxxp://Icedjungle.com/pdthm0/dan2.exe
hxxp://integritysites.net/files/nero.tar.gz
hxxp://jbmsystem.fr/jb/pack.tar.gz
hxxp://joefel.com/easyscripts/sancho.tar.gz
hxxp://krzysztofkarpinski.pl/log/hiser.tar.gz
hxxp://locamat-antilles.com/memo/sancho.tar.gz
hxxp://maisondessources.com/assets/pack.tar.gz
hxxp://m-a-metare.fr/media/sancho.tar.gz
hxxp://masterbranditalia.com/downloader/cario.tar.gz
hxxp://microneedle.com/menu_files/pack.tar.gz
hxxp://mmadolec.ipower.com/me/cario.tar.gz
hxxp://n23.fr/asstempo/doom.tar.gz
hxxp://necaps.org/pagestyles/mine.tar.gz
hxxp://ohayons.com/dostanes_do_drzky.tar.gz
hxxp://ourtrainingacademy.com/LeadingRE/sancho.tar.gz
hxxp://peche-sportive-martinique.com/wp-includes/pack.tar.gz
hxxp://pinballpassion.fr/images/mine.tar.gz
hxxp://pleiade.asso.fr/piwigotest/pack.tar.gz
hxxp://ppc.cba.pl/cache/nero.tar.gz
hxxp://prevencionprl.com/im/hiser.tar.gz
hxxp://pubbliemme.com/plugins/doom.tar.gz
hxxp://scolapedia.org/histoiredesarts/pack.tar.gz
hxxp://shop-oye.it/XXXinstallXXX/abc.tar.gz
hxxp://siestahealthtrack.com/media/pack.tar.gz
hxxp://smartoptionsinc.com/data-test/nero.tar.gz
hxxp://sp107.home.pl/logs/dostanes_do_drzky.tar.gz
hxxp://springtree.cba.pl/modules/cario.tar.gz
hxxp://stevenblood.com/ChromeSetup.exe
hxxp://stmarys-andover.org.uk/audio_files/upupup.tar.gz
hxxp://telasramacrisna.com.br/ramacrisna/mine.tar.gz
hxxp://telasramacrisna.com.br/site/lightbox/hiser.tar.gz
hxxp://thelastxmas.com/ChromeSetup.exe
hxxp://thehollow.co/ChromeSetup.exe
hxxp://thinkonthis.net/style/dostanes_do_drzky.tar.gz
hxxp://thomasottogalli.com/webtest/sancho.tar.gz
hxxp://voigt-its.de/fit/pack.tar.gz
hxxp://wcicinc.org/flv/dostanes_do_drzky.tar.gz
hxxp://wireandwoods.ru/pdthm0/042.exe
hxxp://www.baddadclub.com/ChromeSetup.exe
hxxp://www.cpeconsultores.com/tmp/pack.tar.gz
hxxp://www.geordie.land/ChromeSetup.exe
hxxp://www.goodtobeloved.com/ChromeSetup.exe
hxxp://www.lamas.si/picture_library/upupup.tar.gz
hxxp://www.sazlar.de/sazlar/mine.tar.gz
hxxp://www.thelatxma.com/ChromeSetup.exe
hxxp://wymiana-wsb.cba.pl/pp/abc.tar.gz
hxxp://zysztofkarpinski.pl/log/hiser.tar.gz
```

(remplacer hxxp par http)

5 - Documentation

- Note d'information du CERTA sur les bons réflexes en cas d'intrusion sur un système d'information http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html

- Recommandations de l'ANSSI pour la mise en oeuvre d'une politique de restrictions
  http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/recommandations-et-guides/securite-du-poste-de-travail-et-des-serveurs/recommandations-pour-la-mise-en-oeuvre-d-une-politique-de-restrictions.html
- Article du CERT Société Générale sur CTB Locker
  http://blog.cert.societegenerale.com/2015/02/ctb-locker-new-massive-crypto.html
- Article de Bleeping Computer sur CTB Locker
  http://www.bleepingcomputer.com/virus-removal/ctb-locker-ransomware-information
- Article de 2-viruses sur CTB Locker
  http://www.2-viruses.com/ctb-lockercritroni-ransomware-now-is-distributed-with-fake-google-chrome-update
- Article de McAfee sur CTB Locker
  https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT$_DOCUMENTATION/25000/PD25696/en_US/Locker.pdf$

Gestion détaillée du document

05 février 2015 version initiale ;
06 février 2015 mise à jour des recommandations.
10 juillet 2015 fermeture de l'alerte.