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 07 avril 2016
N° CERTFR-2016-ALE-001-001

Affaire suivie par :
CERT-FR

BULLETIN D'ALERTE DU CERT-FR

Objet : Campagne de messages électroniques non sollicités de type Locky

Gestion du document

Référence	CERTFR-2016-ALE-001
Titre	Campagne de messages électroniques non sollicités de type Locky
Date de la première version	19 février 2016
Date de la dernière version	7 avril 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 Locky.

2 - Systèmes affectés

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

3 - Résumé

Depuis la mi-février 2016, 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 Locky.

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 s'effectue par l'intermédiaire d'un pourriel dans lequel se trouve une pièce jointe au format doc. Ce document Microsoft Office contient un texte illisible ainsi qu'un message indiquant la nécessité d'activer les macros pour l'affichage correct du message. Macro 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 ".locky".

Il est intéressant de noter que le message eléctronique a pour sujet "ATTN: Invoice J-<8 chiffres>" et la pièce jointe pour nom "invoice_J-<8 mêmes chiffres>". 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 Locky sont les suivantes :

```
http://avp-mech.ru_BAD_/7/7.exe
http://bebikiask.bc00.info_BAD_/5/5.exe
http://bnfoviesrdtnslo.uk_BAD_
http://cscrrxyiyc.be_BAD_
http://dkoipg.pw_BAD_
http://drhxvktlaprrhl.be_BAD_
http://dulichando.org_BAD_
http://fnarsipfqe.pw_BAD_
http://gahal.cz_BAD_
http://193.124.181.169_BAD_/main.php
http://195.154.241.208_BAD_/main.php
http://91.195.12.185_BAD_/main.php
http://91.234.33.206_BAD_/main.php
https://103.23.154.184_BAD_:443
https://103.245.153.70_BAD_:343
https://129.15.240.105_BAD_:443
https://140.78.60.4_BAD_:443
https://144.76.73.3_BAD_:1743
https://148.202.223.222_BAD_:443
https://174.70.100.90_BAD_:443
https://176.53.0.103_BAD_:443
https://181.177.231.245_BAD_:443
https://181.53.255.145_BAD_:444
https://185.24.92.236_BAD_:1743
https://185.47.108.92_BAD_:443
https://188.126.116.26_BAD_:443
https://193.17.184.250_BAD_:443
https://194.126.100.220_BAD_:443
https://200.57.183.176_BAD_:443
https://209.239.86.10_BAD_:443
https://217.35.78.204_BAD_:443
https://41.38.18.230_BAD_:443
https://41.86.46.245_BAD_:443
https://46.183.66.210_BAD_:443
https://62.109.133.248_BAD_:444
https://85.143.166.200_BAD_:1743
http://iamnickrobinson.com_BAD_
http://iynus.net_BAD_
http://jaomjlyvwxgdt.fr_BAD_
http://jbdog.it_BAD_
http://killerjeff.free.fr_BAD_/2/2.exe
http://kpybuhnosdrm.in_BAD_
http://luvenxj.uk_BAD_
http://vmanipalecom.net_BAD_
http://vodcxeeg.tf_BAD_
http://ofhhoowfmnuihyd.ru_BAD_
http://onigirigohan.web.fc2.com_BAD_/1/1.exe
http://premium34.tmweb.ru_BAD_/4/4.exe
http://qheksr.de_BAD_
http://sdwempsovemtr.yt_BAD_
http://seaclocks.co.uk_BAD_
http://tirohbvok.in_BAD_
http://uponor.otistores.com_BAD_/3/3.exe
```

http://vkrdbsrqpi.de_BAD_
http://vldxhdofpmcos.uk_BAD_
http://wpogw.it_BAD_
http://www.iglobali.com_BAD_
http://www.jesusdenazaret.com.ve_BAD_
http://www.southlife.church_BAD_
http://www.villaggio.airwave.at_BAD_

Mise à jour Ajout de nouveaux marqueurs suite à une publication de McAfee (2016/02/22):
http://95.181.171.58_BAD_
http://185.14.30.97_BAD_
http://195.22.28.196_BAD_
http://195.22.28.198_BAD_
http://pvwinlrmwvccuo.eu_BAD_
http://cgavqeodnop.it_BAD_
http://kqlxtqptsmys.in_BAD_
http://wblejsfob.pw_BAD_

Mise à jour Depuis le 29 févier 2016, le CERT-FR constate à l'échelle nationale une vague de pourriel sous la forme d'un message électronique provenant de l'opérateur de téléphonie mobile Free Mobile du type suivant :

```
Subject: Facture mobile du 29-02-2016
From: "Free Mobile" <freemobile@free-mobile.fr>
Date: 29/02/2016 12:01
To: <xxx@yyy.zzz>

Cher(e) abonne(e),

Veuillez trouver en piece jointe votre facture mobile du 01-02-2016, d'un montant de 19.

Vous pouvez a tout moment desactiver la reception de votre facture par email dans votre

Sinceres salutations.

L'equipe Free

--
Free Mobile - SAS au capital de 365.138.779 Euros - RCS PARIS 499 247 138 -
Siege social : 16 rue de la Ville l'eveque 75008 Paris


Attachments:
Freemobile_0782884641_29-02-2016.pdf 1,7 KB
```

La pièce jointe est en fait une archive ZIP contenant un fichier javascript nommé EPSON000<nombre à 10 chiffres>.js. Ce script va ensuite télécharger la charge malveillante. Parmi les échantillons analysés, les URLS suivantes sont utilisées pour ce téléchargement :
http://baiya_BAD_.org/image/templates/7ygvtyvb7niim.exe
http://bindulin_BAD_.by/system/logs/7ygvtyvb7niim.exe
http://english-well_BAD_.ru/assets/js/7ygvtyvb7niim.exe
http://kokliko_BAD_.com.ua/admin/swfupload/7ygvtyvb7niim.exe
http://liquor1.slvtechnologies_BAD_.com/system/logs/7ygvtyvb7niim.exe
http://mansolution_BAD_.in.th/system/logs/7ygvtyvb7niim.exe
http://u1847.netangels_BAD_.ru/system/smsgate/7ygvtyvb7niim.exe
http://www.notebooktable_BAD_.ru/system/logs/7ygvtyvb7niim.exe

Mise à jour Nouveaux marqueurs (03/03/2016):
http://sm1_BAD_.by/vqmod/xml/76tr5rguinml.exe
http://dohoatrang.vn._BAD_/system/logs/23f3rf33.exe

Mise à jour Nouveaux marqueurs (15/03/2016):
Téléchargement de la charge :

```
http://tech-cart.com._BAD_/system/logs/lkj87h.exe
http://mutlulukhayali.com._BAD_/system/logs/lkj87h.exe
```

Mise à jour Nouveaux marqueurs (29/03/2016):

```
store.brugomug.co.uk._BAD_/765f46vb.exe
ggbongs.com._BAD_/765f46vb.exe
dragonex.com._BAD_/765f46vb.exe
homedesire.co.uk._BAD_/765f46vb.exe
scorpena.com._BAD_/765f46vb.exe
pockettypewriter.co.uk._BAD_/765f46vb.exe
enduro.si._BAD_/pdf/765f46vb.exe
185.130.7.22._BAD_/files/qFBC5Y.exe
```

Serveurs de Commande et Contrôle (CnC) Sur la base des différentes sources ouvertes sur Internet ainsi que d'éléments transmis par des partenaires du CERT-FR, voici une liste d'URLs suspectées d'abriter des services de commande et contrôle. La mise en liste noire de ces adresses est à considérer dans le cadre d'une protection contre le rançongiciel Locky.

```
http://193.124.181.169_BAD_/main.php
http://195.154.241.208_BAD_/main.php
http://91.195.12.185_BAD_/main.php
http://91.234.33.206_BAD_/main.php
http://109.234.38.35_BAD_/main.php
http://lneqqkvxxogomu.eu_BAD_/main.php
http://qpdar.pw_BAD_/main.php
http://ydbayd.de_BAD_/main.php
http://ssojravpf.be_BAD_/main.php
http://gioaqjklhoxf.eu_BAD_/main.php
http://txlmnqnunppnpuq.ru_BAD_/main.php
http://jbdog.IT_BAD_/main.php
http://kpybuhnosdrm.in_BAD_/main.php
http://luvenxj.uk_BAD_/main.php
http://dkoipg.pw_BAD_/main.php
http://31.184.197.119_BAD_/main.php
http://5.34.183.195_BAD_/main.php
http://51.254.19.227_BAD_/main.php
http://91.219.29.55_BAD_/main.php
http://46.4.239.76_BAD_/main.php
http://94.242.57.45_BAD_/main.php
http://80.86.91.232_BAD_/main.php
http://wblejsfob.pw_BAD_/main.php
http://kqlxtqptsmys.in_BAD_/main.php
http://cgavqeodnop.it_BAD_/main.php
http://vpvwinlrmwvccuo.eu_BAD_/main.php
http://dltvwp.it_BAD_/main.php
http://uxvvm.us_BAD_/main.php
http://195.154.241.208_BAD_/main.php
http://kqlxtqptsmys.in_BAD_/main.php
http://cgavqeodnop.it_BAD_/main.php
http://pvwinlrmwvccuo.eu_BAD_/main.php
http://dltvwp.it_BAD_/main.php
http://uxvvm.us_BAD_/main.php
http://wblejsfob.pw_BAD_/main.php
http://185.14.29.188_BAD_/main.php
http://91.219.29.55_BAD_/main.php
```

http://5.34.183.195_BAD_/main.php
http://188.138.88.184_BAD_/main.php
http://31.184.197.119_BAD_/main.php
http://51.254.19.227_BAD_/main.php
http://5.34.183.195_BAD_/main.php
http://185.14.29.188_BAD_/main.php
http://88.138.88.184_BAD_/main.php
http://31.184.197.119_BAD_/main.php
http://51.254.19.227_BAD_/main.php
http://5.34.183.195_BAD_/main.php
http://185.14.29.188_BAD_/main.php
http://31.184.197.119_BAD_/main.php
http://185.46.11.239_BAD_/main.php
http://185.22.67.27_BAD_/main.php
http://31.184.233.106_BAD_/main.php
http://pccibcjncnhjn.yt_BAD_/main.php
http://qtysmobytagnrv.it_BAD_/main.php
http://rddipikmrap.us_BAD_/main.php
http://suhpqiumpjsv.ru_BAD_/main.php
http://vkcims.pm_BAD_/main.php
http://5.34.183.136_BAD_/main.php
http://91.121.97.170_BAD_/main.php
http://188.138.88.184_BAD_/main.php
http://31.41.47.37_BAD_/main.php
http://kcdxkbsk.tf_BAD_/main.php
http://31.184.197.119_BAD_/main.php
http://51.254.19.227_BAD_/main.php
http://91.219.29.55_BAD_/main.php
http://5.34.183.195_BAD_/main.php
http://185.14.29.188_BAD_/main.php
http://kxsvgrpytxfar.tf_BAD_/main.php
http://nuhiqgn.yt_BAD_/main.php
http://qkcehlnkcuts.fr_BAD_/main.php
http://slkyatnnaq.eu_BAD_/main.php
http://tdhlnatbwyc.pm_BAD_/main.php
http://195.154.241.208_BAD_/main.php
http://46.4.239.76_BAD_/main.php
http://94.242.57.45_BAD_/main.php
http://kqlxtqptsmys.in_BAD_/main.php
http://cgavqeodnop.it_BAD_/main.php
http://pvwinlrmwvccuo.eu_BAD_/main.php
http://dltvwp.it_BAD_/main.php
http://uxvvm.us_BAD_/main.php
http://wblejsfob.pw_BAD_/main.php
http://91.121.97.170_BAD_/main.php
http://46.4.239.76_BAD_/main.php
http://31.184.233.106_BAD_/main.php
http://185.46.11.239_BAD_/main.php
http://69.195.129.70_BAD_/main.php
http://5.34.183.195_BAD_/main.php
http://31.184.197.119_BAD_/main.php
http://51.254.19.227_BAD_/main.php
http://91.219.29.55_BAD_/main.php
http://wblejsfob.pw_BAD_/main.php
http://dkoipg.pw_BAD_/main.php
http://85.25.149.246_BAD_/main.php
http://31.184.197.119_BAD_/main.php
http://51.254.19.227_BAD_/main.php

```
http://185.14.29.188_BAD_/main.php
http://192.71.213.69_BAD_/main.php
http://95.213.184.10_BAD_/main.php
http://192.121.16.196_BAD_/main.php
```

Mise à jour Nouveaux marqueurs (15/03/2016). Liste de CnC pouvant être contactés :

```
149.154.157.14
37.235.53.18
89.108.85.163
212.47.223.19
192.121.16.196
```

Mise à jour Nouveaux marqueurs (29/03/2016):

```
176.31.47.100._BAD_/submit.php
185.117.72.94._BAD_/submit.php
185.141.25.150._BAD_/submit.php
78.46.170.79._BAD_/submit.php
83.217.8.127._BAD_/submit.php
84.19.170.249._BAD_/submit.php
91.200.14.73._BAD_/submit.php
92.63.87.134._BAD_/submit.php
```

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. 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.

5 - Documentation

- https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26383/en_US/McAfee_Labs_Threat_Advisory_Ransomware_Locky.pdf

Gestion détaillée du document

19 février 2016 version initiale ;

02 mars 2016 ajout des informations relatives à la fausse facture FreeMobile ;

02 mars 2016 ajout des serveurs de Commande et Contrôle ;

07 avril 2016 Clôture de l'alerte.