Le ransomware Locky inonde la France, via de fausses factures Free Mobile

Le ransomware Locky, à l'origine d'une attaque récente contre un hôpital à Los Angeles, est toujours actif et il cible particulièrement la France. Selon une analyse de l'éditeur Kaspersky, le malware, dont la société a identifié plus de 60 variantes à ce jour, serait en effet particulièrement diffusé en France et en Allemagne. Le **CERT-FR**, le centre d'alerte et de réaction aux attaques informatiques de l'administration hexagonale, confirme d'ailleurs cette analyse dans une note datée du 2 mars (sa première version date du 19 février). L'organisme indique constater une « *vague de pourriels dont le taux de blocage par les passerelles anti-pourriel est relativement faible* », des spams ayant pour objectif de diffuser le rançongiciel Locky.

Ce ransomware doit son nom au suffixe qu'il donne aux fichiers qu'il crypte (transformé en .locky). Classiquement, les cybercriminels demandent aux victimes de s'acquitter d'une rançon pour retrouver l'accès à leurs données devenues inaccessibles (entre 0,5 et 1 Bitcoin dans le cas présent, selon les données publiées par Sophos, un Bitcoin valant aujourd'hui quelque 360 euros).

Diffusion de Locky : haro sur les macros Office

Locky **chiffre un grand nombre de fichiers**, en particulier tous ceux ayant des extensions renvoyant à des vidéos, des images, des codes source et des fichiers Office. Il cible même le fichier *wallet.dat*, autrement dit le portefeuille de Bitcoin si l'utilisateur en possède un. Faute de sauvegarde de ce dernier et s'il renferme plus d'un Bitcoin, les criminels sont quasiment sûrs d'amener leur victime à payer la rançon !

La méthode de diffusion du malware est assez classique et rappelle celle utilisée pour un autre malware célèbre, Dridex : l'infection se dissimule, la plupart du temps, dans **une pièce jointe à un e-mail**, prenant par exemple l'apparence d'une facture. Sauf que ce fichier (très souvent un .doc) semble codé de façon inappropriée. C'est là que réside le piège : un message conseille alors à l'utilisateur d'autoriser les macros pour revenir à un codage plus adapté. Cette action permet d'installer sur le disque dur de la victime un fichier qui, à son tour, va aller télécharger le malware à proprement parler. Cette mécanisme à double détente, assez courant, permet aux hackers de modifier et de peaufiner leur malware au fil du temps, sans avoir à bouleverser leur procédure d'installation.

« *Il est intéressant de noter que le message électronique 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* », écrit le


Cher(e) abonné(e),

Veuillez trouver en pièce jointe votre facture mobile du 01-02-2016, d'un montant de 19.99 .

Vous pouvez tout moment désactiver la réception de votre facture par email dans votre espace abonné : http://mobile.free.fr

Sincères salutations.

L'équipe Free

--

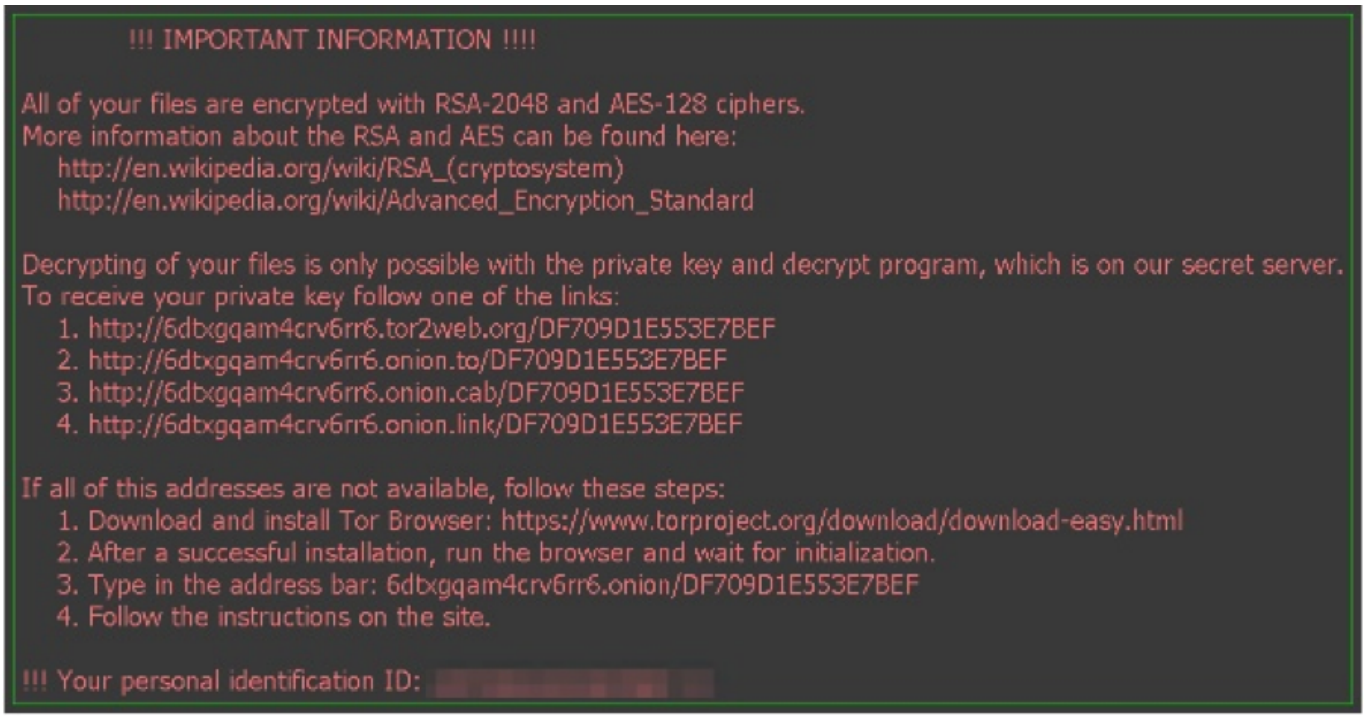
Free Mobile - SAS au capital de 365.138.779 Euros - RCS PARIS 499 247 138 - Siège social : 16 rue de la Ville l'Evêque 75008 Paris

CERT-FR. Ce dernier précise toutefois que la méthode de diffusion du malware peut varier : depuis le 29 février, l'organisme observe une **nouvelle vague de pourriels** prenant la forme de fausses **factures Free Mobile**, envoyées par e-mail (voir ci-dessus). Ces dernières renferment cette fois un fichier Javascript dont l'objectif est de télécharger Locky.

Kaspersky Lab assure également avoir identifié d'autres méthodes de propagation, notamment via des pages web légitimes sur lesquelles le malware Locky est implanté. Lors d'une simple visite d'une de ces pages, Locky cherche à se diffuser sur le poste de l'utilisateur en exploitant d'éventuelles vulnérabilités logicielles présentes sur sa configuration. L'éditeur d'antivirus ajoute que, dans ses versions les plus récentes, le malware peut se présenter également « *sous la forme d'une notification de fax ou de scanner* ».

Attention à la propagation sur le réseau de l'entreprise

Une fois l'ordinateur infecté, un écran s'affiche, informant l'utilisateur du forfait et l'invitant à se connecter à des pages décrivant de la marche à suivre pour payer sa rançon et récupérer ses données (ci-dessous). Comme le rappelle Sophos, les effets d'un ransomware comme Locky peuvent être dévastateurs en entreprises, car le malware **ne se contente pas de chiffrer le disque C:** de sa victime. Il bloque aussi les fichiers des disques auxquels le poste a accès, y compris les disques amovibles, les serveurs de fichiers du réseau ou les machines de tiers (y compris sous Linux ou OS X). Dévastateur si la victime est connectée en tant qu'administrateur du domaine. Dans sa note, le CERT-FR recommande d'ailleurs, en cas d'infection, de « *déconnecter immédiatement du réseau les machines identifiées comme compromises* » et de « *positionner les permissions des dossiers partagés en lecture seule afin d'empêcher la destruction des fichiers sur les partages* ».



Locky a fait récemment la démonstration de sa dangerosité en bloquant les systèmes d'un hôpital de Los Angeles, le Hollywood Presbyterian Medical Center. Selon le *New York Post*, ce dernier a été

contraint de verser 17 000 $ aux pirates – après négociation, les criminels réclamaient au départ plus de 3,5 M$ – pour obtenir les clefs de déchiffrement et retrouver l'accès à ses données.

Un ransomware qui rebondit grâce au Cloud

« *2016 est probablement l'année du ransomware. Au cours du seul mois de février, nous avons déjà dénombré autant de tentatives d'attaques contre nos clients que lors des cinq mois précédents cumulés* », commente Marco Preuss, à la tête de l'équipe de recherche et de développement de Kaspersky Lab en Europe. L'éditeur a dénombré au cours du mois dernier **plus de 40 000 tentatives d'infection** par un ransomware chez ses clients.

Récemment, un autre rançongiciel écrit en PHP s'en est pris non plus aux postes de travail mais directement aux serveurs Web, preuve de la volonté des cybercriminels d'exploiter le filon partout où c'est possible. Par ailleurs, Netskope, éditeur spécialisée dans la sécurisation des applications Cloud, a récemment expliqué avoir détecté des phénomènes de diffusion de ransomware via le Cloud, au travers de la fonction de synchronisation de fichiers que ces services offrent à leurs utilisateurs.

A lire aussi :

Ransomware : un tiers des Français prêts à payer et seulement 188 €

Le ransomware prospère grâce à l'apathie des autorités

Ransomware : un retour sur investissement très lucratif

Crédit photo : Carlos Amarillo / Shutterstock