# Patcher, un ransomware bien mal codé pour macOS

Mais bel et bien dangereux 13


**Un nouveau ransomware frappe actuellement les utilisateurs peu scrupuleux de Mac. « Patcher » ressemble ainsi à un crack pour Premiere Pro ou Office, mais cache en réalité un malware qui va chiffrer le contenu du disque. Malheureusement, il n'est même pas équipé d'un mécanisme de déverrouillage.**

Patcher ressemble donc à un bon vieux crack, c'est-à-dire un petit programme se proposant d'activer des logiciels sans en avoir la licence authentique. Dans le cas présent, il vise particulièrement la suite Office de Microsoft et le logiciel de montage Premier Pro d'Adobe. La promesse est bien ancienne : utiliser ces logiciels sans avoir à payer. Bien mal en prendra à l'utilisateur.

## Le crack pour logiciel, une vieille recette

Le ransomware se présente initialement sous la forme d'un fichier Zip contenant deux « patchs », un pour chaque logiciel. En lancer un ouvrira une fenêtre sans fond – qui devrait déjà être une alerte en soi – et présente simplement un petit texte explicatif, accompagné d'un bouton Start. Cliquer sur ce dernier ne modifie en rien l'installation du logiciel, mais lance par contre un processus de chiffrement pour toutes les données personnelles présentes dans le disque.

Patcher crée une clé de 25 caractères de long qu'il va utiliser pour l'ensemble des fichiers (la même pour tous). Il place dans chaque dossier personnel (Documents, Images…) un fichier README expliquant en anglais la situation. Elle est simple : si l'utilisateur veut revoir ses données, il doit payer 0,25 bitcoin à l'adresse indiquée (près de 270 euros aujourd'hui).


## Le ransomware ne communique avec personne

Cependant, comme l'explique ESET, la situation est nettement plus compliquée, car personne ne peut déchiffrer les données, pas même l'auteur du ransomware. Pourquoi ? Parce que Patcher ne contient pas la moindre ligne de code lui permettant de communiquer avec un serveur C&C (command-and-control). Dès lors, le ou les pirates ne sont même pas avertis que le malware a rempli sa sinistre mission, et ne peuvent donc pas envoyer la précieuse clé.

ESET estime que le malware n'est globalement pas une merveille, l'éditeur parlant de mauvais code. Le fait qu'aucun lien avec un serveur C&C ne soit présent en dit long selon l'entreprise sur la compétence de ceux qui ont créé Patcher, ou en tout cas cette version. Cela étant, le malware reste dangereux, et ce d'autant plus qu'il est impossible de récupérer la clé. Sa taille – 25 caractères – la rend en effet trop résistante aux attaques par force brute.

La méfiance reste donc de mise, comme globalement tout ce qui « paraît trop beau pour être vrai ». Ce type de menace est finalement très courant, et même si les systèmes d'exploitation disposent de protections plus avancées, il suffit d'amener l'utilisateur à cliquer au bon endroit et à accorder les droits quand ils sont demandés.

Publiée le 23/02/2017 à 15:00

**Vincent Hermann**
Rédacteur/journaliste spécialisé dans le logiciel et en particulier les systèmes d'exploitation. Ne se déplace jamais sans son épée.





**En continu**

Kit Philips Hue avec 2 ampoules, détecteur de mouvement et bandeau LED : 139 €
Valable jusqu'au 01/03/2017

Patcher, un ransomware bien mal codé pour macOS
5 min 14

Synology : le DSM 6.1 disponible en version finale pour les NAS dès la série x11
5 min 23

L'UFC-Que Choisir étrille les plateformes de prêt participatif aux entreprises
5 min 4

Orange : des bénéfices en hausse, le FTTH et la 4G gagnent encore du terrain
5 min 21

Alimentation Be Quiet! System Power 8 de 500 W (80Plus) : 45,90 €
Valable jusqu'au 01/03/2017

Terrorisme : Éric Ciotti propose d'inscrire le délit de consultation dans la Constitution
5 min 75

Piratage : selon l'ALPA, le nombre d'internautes « indélicats » a baissé en 2016
5 min 63

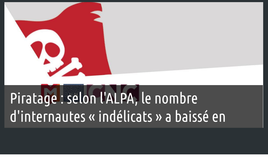
Twitter ajoute les onglets et fenêtres multiples dans son application Windows 10
5 min 8

Aux 20 ans de l'Arcep, la régulation des plateformes comme horizon
Abonné 5 min 6

Disque dur externe Hitachi USB 3.0 de 1 To (2,5") : 49,99 euros
Valable jusqu'au 01/03/2017

**Analyses de la rédaction**


Orange : des bénéfices en hausse, le FTTH et la 4G gagnent encore du terrain


Piratage : selon l'ALPA, le nombre d'internautes « indélicats » a baissé en


Aux 20 ans de l'Arcep plateformes comme

Chargement des commentaires…