Vous et Votre Mac

Vous et Votre Mac

N° 131 • mars 2017 100 % Mac en pratique

AIRPODS

Notre test des écouteurs audio 100 % sans fil d'Apple.

Chromebook et smartphone Android : est-ce un choix raisonnable quand on a déjà un Mac ?

Les utilisateurs Mac face à la menace Malwares

Comment se protéger, se défendre et traiter un Mac touché

Zoom sur les fonctions clés de macOS Sierra

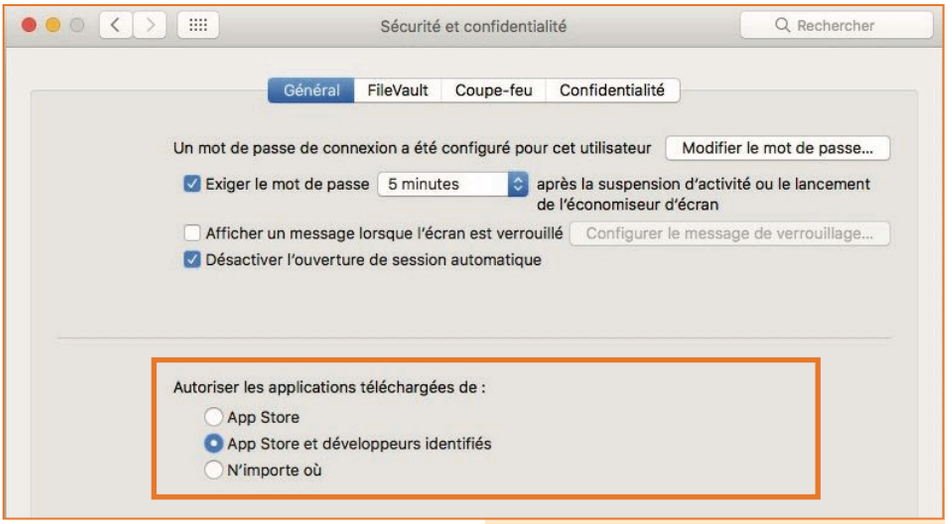
FRANCE métropolitaine : 5,90 € • SUISSE : 9,90 FS
DOM - BEL - MUX - PORT CONT : 6,90 € • CANADA 10,99 $
L 11206 - 131 S - F : 5,90 € - RD

Face à la menace Malwares
ces logiciels malveillants venus du Net

Non, nos Mac ne sont plus épargnés ! Si les virus n'attaquent pas nos machines, des menaces plus modernes, souples, et peut-être plus dangereuses encore, rodent sur le réseau des réseaux. Conseils et outils pour se protéger des malwares.

Sur Mac, pendant longtemps, on a cru pouvoir se passer d'un antivirus. C'était même un de nos meilleurs arguments face aux systèmes concurrents – et une posture longtemps entretenue par Apple. Cette époque est révolue. Au fil du temps, le Mac est devenu un PC (au sens d'ordinateur personnel) presque comme un autre. Même si nous sommes encore très loin dela prolifération des logiciels malveillants qui sévissent sous Windows, de nombreuses menaces nous touchent désormais. Que celui qui n'a jamais été confronté à un logiciel malveillant, me jette la première pierre ! **DENIS DUBOIS (TWITTER : @DEDUBO)**

Les malwares ou logiciels malveillants sont des logiciels développés dans le but de nuire. Que ces programmes aient pour objectif de collecter des informations vous concernant, d'héberger des informations illégales sur votre disque dur, de prendre en otage vos données, d'utiliser votre ordinateur à votre insu pour envoyer du spam à vos contacts, ou encore d'en prendre le contrôle à distance, **ils n'ontjamais été aussi nombreux sur Mac**. L'éditeur Objective-See en dresse le bilan 2016 ***(https://objective-see.com/blog/blog_0x16.html)***.



QUELS SONT LES SYMPTÔMES D'UN MAC INFECTÉ PAR UN MALWARE ?

Les symptômes d'une infection sont **aussi nombreux que variés**. En voici quelques exemples, sans prétendre à l'exhaustivité !

Si vous trouvez que votre Mac tourne **au ralenti** sans aucune raison, si votre disque dur trahit **une activité intense** aussi soudaine qu'inexpliquée (en dehors de Time Machine), il est possible que vous soyez infecté par un malware en activité ou un rançongiciel (ransomware) qui chiffre vos documents en arrière-plan. Il en sera de même, **si votre réseau Wi-Fi est extrêmement actif** par rapport à votre (modeste) activité.

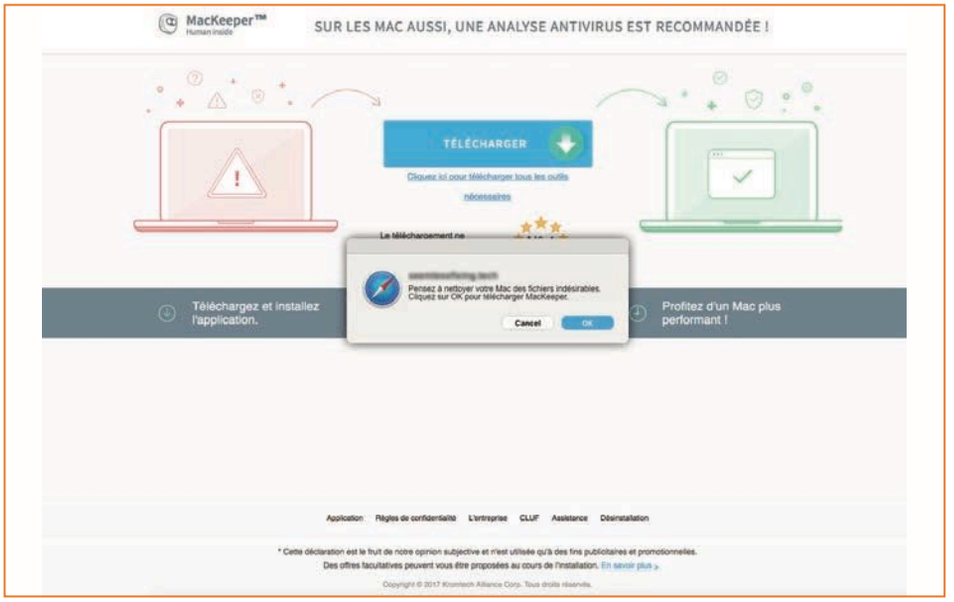
Que des applications refusent de se lancer ou que vous ne puissiez plus accéder à vos documents sans que des messages d'erreur s'affichent peut-être être un signe d'infection. Si vous recevez **en notification du pare-feu** qu'un programme inconnu essaie d'accéder à Internet sans votre consentement, vous êtes sans doute victime là aussi d'un malware.

Si vous êtes harcelé par **des fenêtres publicitaires** qui s'ouvrent spontanément dans votre navigateur ou si vous êtes régulièrement **redirigé vers des sites inconnus qui cherchent à vous vendre des services ou des produits**, vous avez probablement installé un **adware** (logiciel publicitaire) par inadvertance. Si votre antivirus se désactive soudainement, une technique fréquemment utilisée par les malwares, il y a anguille sous roche !

Bref, tout comportement anormal ou inhabituel doit vous alerter.

Il faut évoquer le cas particulier du **logiciel MacKeeper** qui n'est pas un logiciel malveillant à proprement parler (encore que…). Il redirige vers une page qui affiche une fausse alerte d'infections et propose alors ses pseudo-services de nettoyage, de protection antivirus et d'optimisation des performances de votre Mac.

Des pratiques commerciales douteuses et malhonnêtes qui ont pour objectif de vous inciter à acheter cette application totalement inutile. Une fois en place,



Le mécanisme **GateKeeper** de macOS permet de limiter les risques en contrôlant de façon stricte l'installation des applications. Seules celles provenant du Mac App Store ou signées d'un développeur agréé sont autorisées. Si vous aviez déjà opté pour la désactivation de GateKeeper (option **De n'importe où**), vous conservez ce choix après avoir mis à jour vers Sierra.

Si vous aviez choisi une des deux premières options, vous constaterez **que macOS 10.12 Sierra a purement et simplement supprimé la troisième**.

Si vous voulez installer tout de même une application qui ne vient pas du MAS et qui n'est pas signée, vous pouvez le faire: cliquez droit sur son icône tout en appuyant sur la touche [ctrl] et demandez alors **Ouvrir** dans le menu contextuel. L'autorisation ayant été donnée, l'application ne sera plus jamais bloquée.

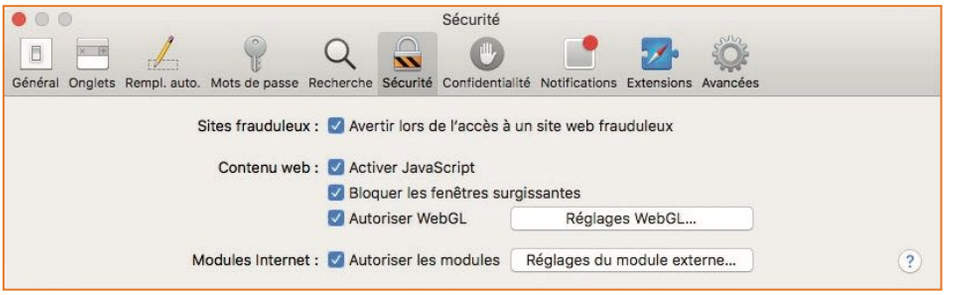
Si jamais le troisième choix est absent et que vous vouliez le rétablir pour ne jamais être « dérangé », c'est possible. Vous prenez vos responsabilités. Ouvrez le Terminal, tapez la commande: **sudo spctl --master-disable**, entrez votre mode passe administrateur. L'option **De n'importe où** réapparaîtra dans le panneau Sécurité et confidentialité des Préférences Système et sera activée par défaut.

Si vous vous ravisiez, il suffit de cocher l'une des deux premières options du panneau, et la troisième disparaîtra instantanément de nouveau.

l'application s'avère difficile à désinstaller proprement (***http://bit.ly/2iVwca0***).

CE QUE FAIT APPLE POUR NOUS PROTÉGER

Pour s'installer sur un ordinateur, certains logiciels malveillants exploitent les vulnérabilités des systèmes d'exploitation ou des applications. Apple prend le problème très au sérieux et n'a de cesse d'améliorer la sécurité de macOS en intégrant, au fil des versions, des techniques de sécurisation de plus en plus poussées. **GateKeeper** propose une protection contre des logiciels malveillants en limitant l'exécution d'applications téléchargées depuis le Mac App Store ou d'applications signées par des développeurs identifiés, donc de confiance. Il est configurable dans le panneau des **Préférences Système > Sécurité et confidentialité > Onglet Général**, sous l'intitulé **Autoriser les applications téléchargées de**. Il est toujours possible d'exécuter une application non signée d'un développeur tiers non identifié ; on désactive ponctuellement GateKeeper lors du premier lancement de l'application en appuyant sur la touche [ctrl] tout en cliquant sur son icône et en demandant Ouvrir dans le menu contextuel.



On peut aussi désactiver de façon permanente GateKeeper (lire encadré page précédente), mais nous ne vous le conseillons évidemment pas pour un usage « normal » du Mac.

Autre technologie déployée par Apple, **le sandboxing (ou bac à sable)** consiste à isoler les applications dans un environnement contrôlé qui les empêche de modifier des composants critiques du système ou d'autres applications. En cas de comportement malveillant, la source du problème est immédiatement bloquée. Ainsi les modules sensibles que sont Java, Adobe Flash, Silverlight… qui s'exécutent dans Safari, sont en théorie protégés contre des accès malveillants.

Le **module anti-hameçonnage de Safari** détecte les sites suspects, des imitations plus ou moins réussies de sites « officiels » qui tentent de récupérer vos informations sensibles. Avec El Capitan, Apple a introduit **SIP (ou System Integrity Protection)** qui bloque tout accès à certains dossiers stratégiques du système, même si l'on se fait passer pour l'utilisateur root, celui qui dans un système Unix « normal » a tous les droits, même celui de « flinguer » le système (lire un autre article d'Henri Dominique Rapin, dans ce même numéro de VVMac).

Il faudrait aussi évoquer **le pare-feu** (à paramétrer dans les Préférences Système) et d'autres technologies Apple qui concourent à cette sécurité interne. Cependant, cela reste insuffisant. Nous vous conseillons de mettre en place, de votre côté, un certain nombre d'outils complémentaires pour sécuriser votre environnement et de vous alerter en cas de tentative d'infection.

DES OUTILS TIERS À INSTALLER

Commencez par **un antivirus**, gratuit ou payant. C'est aujourd'hui, une première mesure indispensable car les (bons) antivirus ne se contentent pas de traquer les virus – qui n'existent pratiquement pas sur Mac – **mais ils détectent et éradiquent de nombreux types de malwares**. Si vous ne souhaitez pas payer un

Les différentes menaces

ADWARE
Type de malware qui affiche des annonces publicitaires non désirées sur l'écran d'un ordinateur et qui transmet à son éditeur des renseignements permettant d'adapter ces annonces au profil de l'utilisateur.

CHEVAL DE TROIE OU TROYEN
Logiciel apparemment inoffensif au sein duquel a été dissimulé un programme malveillant qui peut, par exemple, permettre la collecte frauduleuse, la falsification ou la destruction de données.

KEYLOGGERS
Programmes chargés d'enregistrer à l'insu de l'utilisateur, les séquences de touches frappées au clavier, dans un journal. Le journal sera utilisé pour obtenir les mots de passe, les numéros de carte bancaire, les codes d'accès de l'utilisateur… Les keyloggers logiciels peuvent être détectés et supprimés par les antispywares et les antivirus.

HIJACKERS
Programmes qui modifient, à votre insu et sans votre accord, les pages par défaut (démarrage, recherche…) de votre navigateur internet pour les rediriger vers un site généralement pornographique ou malveillant. Les hijackers peuvent être détectés et supprimés par les antispywares et certains antivirus.

RANSOMWARE (RANÇONGICIEL)
Logiciel qui prend en otage vos données personnelles en chiffrant à votre insu le contenu de votre disque dur, puis il demande une rançon (généralement en Bitcoin) en échange de la clé de déchiffrement. Il se propage à travers des e-mails piégés ou via des failles de sécurité du système.

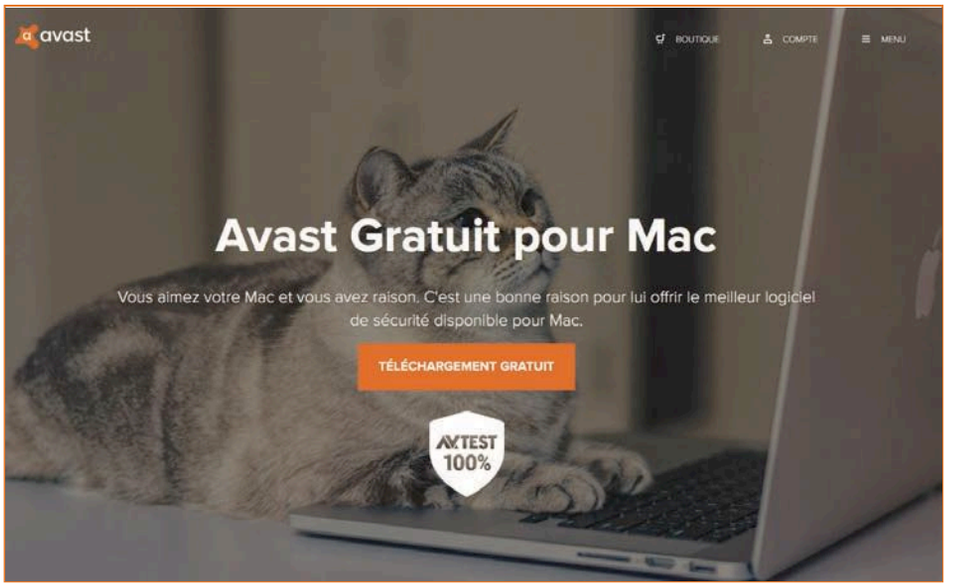
ROGUE
Un faux logiciel de sécurité (inutile ou malveillant) proposé à l'occasion d'une alerte de sécurité fictive (messages simulant une infection) destinée à convaincre l'utilisateur de l'acheter pour assainir son ordinateur. Il s'agit d'une pratique de marketing douteuse.

ROOTKIT
Programme malveillant qui se dissimule au plus près du système afin de ne pas être détecté par les antivirus. Une fois en place, il installe divers outils permettant au pirate de prendre le contrôle de la machine à distance afin d'espionner et de voler les données de l'utilisateur légitime.

SPYWARE (ESPIOGICIEL)
Logiciel espion destiné à collecter et à transmettre à des tiers, à l'insu de l'utilisateur, des données le concernant ou des informations relatives au système qu'il utilise.

VER
Logiciel malveillant indépendant qui se transmet d'ordinateur à ordinateur par Internet ou tout autre réseau et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs.

VIRUS
Logiciel malveillant, généralement de petite taille, qui s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un évènement donné.



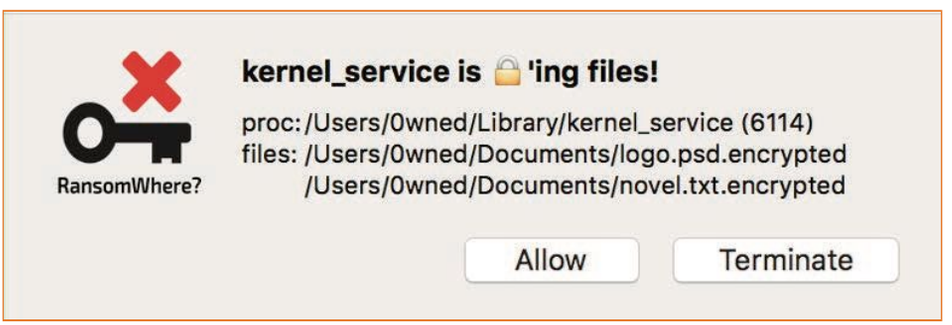
abonnement auprès d'un éditeur (ce qui reste malgré tout la meilleure solution), je vous recommande d'excellent **Avast Mac Security 2016** (Gratuit • ***https://www.avast.com/fr-fr/free-mac-security***), leader sur le marché des antivirus gratuits – et il ne plombera pas vos performances.

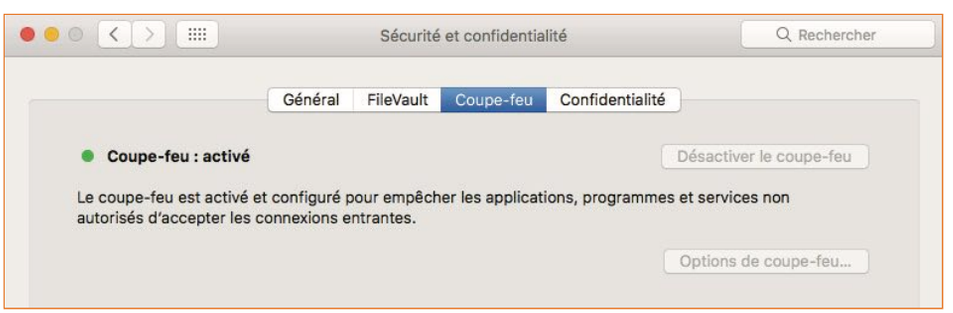
En l'absence d'antivirus, soumettez les fichiers suspects (ou une URL) à un examen complet via le site VirusTotal (***https://www.virustotal.com***) qui va le passer au crible de dizaines d'antivirus en ligne. Ce site appartient à Google.

Ensuite, je vous incite à renforcer votre sécurité avec des modules complémentaires spécialisés.

Malwarebytes Anti-Malware for Mac (ex-AdwareMedic) est très efficace pour détecter et éradiquer **les programmes publicitaires** (adwares) qui envahissent votre Mac et surgissent à la moindre occasion. Il est aussi efficace **contre des programmes malveillants** et des chevaux de Troie. Une alternative : **Bitdefender Adware Removal Tool for Mac** (gratuit - ***http://bit.ly/2joUqFO***).

RansomWhere? (Gratuit - ***https://objective-see.com***) se chargera de détecter les rançongiciels de type **Locky** ou **KeRanger** (lire le glossaire en page de gauche), en bloquant les processus qui chiffrent le contenu de vos fichiers, à votre insu, afin de vous demander une rançon (généralement en Bitcoin) en échange de la clé de déchiffrement (sans aucune garantie !) censée libérer vos précieux documents. En cas de doute, le programme vous demande d'autoriser (Allow) ou de « tuer » (Terminate) le processus en cours.





Complétez votre trousse à outils par **un bloqueur de pub comme uBlock ou uBlock Origin** (lire WMac numéro 118) qui vous permettra d'être protégé contre les malwares qui se cachent dans les bannières publicitaires ou les fenêtres surgissantes (pop-up) et autres animations agaçantes.

LES BONNES PRATIQUES POUR LIMITER LES RISQUES D'INFECTION

Pour se prémunir d'une infection, il est nécessaire de respecter quelques règles élémentaires.

On ne le dira jamais assez : **n'ouvrez pas une pièce jointe à un e-mail sans en connaître l'expéditeur**, et ne cliquez jamais directement sur le lien contenu dans un e-mail – il peut pointer vers des documents malveillants.

Ne téléchargez pas de logiciel de provenance inconnue. Particulièrement ceux issus des sites pirates genre warez, ou des torrents.

Gardez le système **à jour en téléchargeant les mises à jour d'Apple et de vos applications** (activez la mise à jour automatique). De nombreuses vulnérabilités sont régulièrement corrigées par ce biais.

Gardez à jour notamment **vos navigateurs web** ainsi que **les extensions et plugins** installés qui font souvent l'objet de bien des vulnérabilités (Java, Flash, etc.).

Faites **des sauvegardes régulières**, sur un support hors ligne (disque dur externe, disque en réseau local) afin de vous prémunir d'une attaque par chiffrement des données – en plein essor actuellement. Connectez-vous à votre Mac avec **un compte utilisateur Standard** plutôt qu'Administrateur. Les droits d'accès seront limités et toutes modifications du système seront portées à votre connaissance (le mot de passe administrateur sera systématiquement requis). De quoi éveiller les soupçons !

N'activez, dans les Paramètres Système de macOS, que **les services de partage** dont vous avez besoin.

Enfin, pensez à activer **le pare-feu de macOS** (désactivé par défaut) ou, plus sophistiqués, Little Snitch ou Hands Off. Mieux encore, activez le pare-feu de votre box internet via la page de configuration dédiée de votre FAI.

Les logiciels gratuits, téléchargés en dehors du Mac App Store, installent fréquemment des logiciels « compagnons » qui s'avèrent être parfois des adwares. À l'installation automatique, **préférez toujours l'installation manuelle** si elle vous est proposée, et **décochez systématiquement les programmes « associés »** que l'on tente de vous imposer.

Ces quelques recommandations permettront de réduire le risque de contamination de votre Mac mais dites-vous bien que le risque zéro n'existe pas.