Supprimer Adwares, Publicité indésirable, Scams, MacKeeper sous Mac OS X

Posez votre question »

Mai 2016 BR IT US FR

Commentcamarche....
1,168,400 likes
Like Page
Sign Up
2 friends like this

1. Préambule
2. Désinfection par l'utilisation d'utilitaires gratuits
3. Désinfection manuelle
4. **Les emplacements critiques à inspecter dans tous les cas**
5. Cas de nettoyage général
6. Nettoyage de Safari
7. Cas ou Safari ne se lance plus
8. Nettoyage de Firefox
9. Supprimer Genieo / InstallMac / AppYM
10. Supprimer Conduit - Community Tool Bar
11. Supprimer Bundlore - Flashmall
12. **Supprimer MacKeeper**
13. Supprimer Advanced Mac Cleaner
14. Nettoyer les caches
15. Verification
16. Conseils
17. Anti-virus pour Mac
18. Des protections pour Safari et autres navigateurs
19. A lire aussi: Adware mac

Préambule

Lorsque vous faites des recherches dans votre navigateur, Safari ou autre, et que vous constatez un afflux de liens publicitaires, souvent en écriture de couleur verte, que vous avec un nouveau moteur de recherche qui vous est inconnu, vos pages sont redirigées vers des sites non désirés, vous avez une multitudes de pop-up ou fenêtres publicitaires, c'est que vous avez probablement et inconsciemment accepté l'installation d'un ou plusieurs adwares issus d'un site malsain. (comme Softonic ou autres sites de téléchargement infectés).
Il ne s'agit pas de virus à proprement parler, mais d'adwares.
Il faut donc "nettoyer" le Mac.

Désinfection par l'utilisation d'utilitaires gratuits

Si le Mac tourne sous une version d'OS X supérieure à Mac OS X 10.6, il faut avant tout privilégier un nettoyage à l'aide d'un utilitaire dédié à cela. Ça sera bien plus rapide, efficace et très simple.

La désinfection manuelle ne sera nécessaire que dans le cas ou le Mac tourne sous une version antérieure à Mac OS X 10.7 ou en cas d'échec de ces utilitaires ou devant certains cas récalcitrants comme par exemple MacKeeper.

Le plus souvent, le recours à l'un de ces outils suffira.

Pour supprimer ces Adwares sur Mac, à partir de Mac OS X 10.7 ou OS 10.8, il existe actuellement :

- **Malwarebytes Anti-Malware**

https://www.malwarebytes.org/antimalware/mac/

Dernière minute :
- La dernière version de MalwareBytes exige OS X 10.8
- Pour Mac OS X 10.7, essayez ce lien, si encore valide lorsque vous lirez cette page, qui permet le téléchargement d'une version ancienne d'AdwareMedic :
http://macdownload.informer.com/adwaremedic/download/

et aussi :

- **Adware Removal Tool** de Bitdefender:

http://www.bitdefender.fr/solutions/adware-removal-tool.html
"Adware Removal Tool" de BitDefender fonctionne à partir de Mac OS X 10.7

Note : Malwarebytes pour Mac est issu du logiciel **AdwareMedic** initialement édité par : The Safe Mac, logiciel qui, ensuite, a été acquis par MalwareBytes.

Une aide pour AdwareMedic a été publiée ici :
http://assiste.com/AdwareMedic.html

Note concernant MalwareBytes / Adwaremedic :
Le logiciel de désinfection MalwareBytes ne contient pas forcément une base de données complète lors du téléchargement du logiciel, cette base de données étant constamment mise à jour, lors de son lancement, MalwareBytes va se connecter sur le serveur de MalwareBytes, (ex.SafeMac), pour charger les dernières infos permettant la désinfection. En conséquence, le Mac devra être connecté au net lors de son lancement.

Dans tous les cas, Mac OS X 10.7 ou 10.8 est le minimum requis pour ces utilitaires

Désinfection manuelle

Lorsque j'ai écrit cette aide, il n'existait pas d'aide de la part d'Apple sur ce type d'infection. Depuis, Apple a également publié une aide pour remédier à ce type de pollution, elle peut être consultée ici :
https://support.apple.com/fr-fr/HT203987

Pour nettoyer manuellement le Mac il va falloir inspecter plusieurs endroits du disque dur, dont les différentes bibliothèques.

Pour info : Il y a au minimum 3 Bibliothèques dans le système Mac OS X :

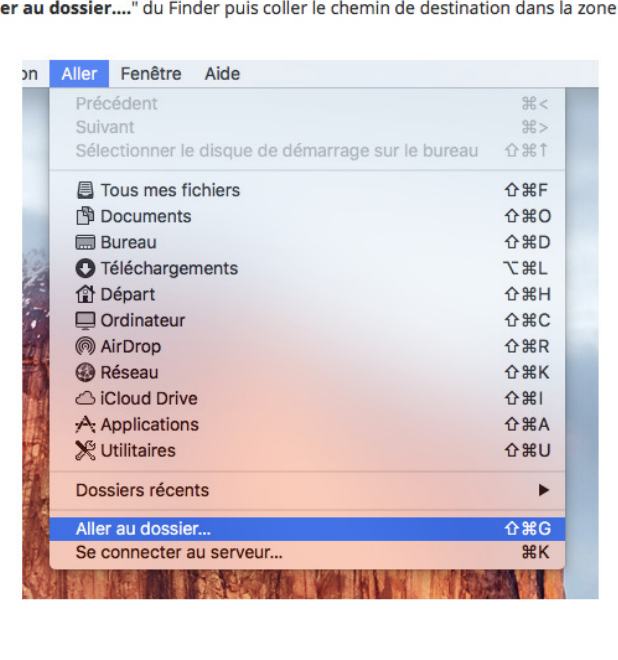
- la principale se trouve à la racine même du disque dur, son chemin est :
/Library

- la seconde se trouve dans le dossier Système, son chemin est :
/System/Library

- et enfin, une Bibliothèque pour chaque utilisateur, celle-ci se trouve à la racine du répertoire de chaque utilisateur, son chemin, pour l'utilisateur en service est :
~/Library

La Bibliothèque utilisateur est cachée dans les dernières versions d' OS X. En conséquence, et depuis Mac OS 10.7, votre bibliothèque personnelle n'étant plus visible par défaut, pour y accéder vous pouvez dérouler le menu "**Aller**" du Finder, cela tout en gardant la **touche alt enfoncée**.
Vous verrez alors apparaître la ligne Bibliothèque, si vous cliquez sur cette ligne vous allez dans votre Bibliothèque personnelle.

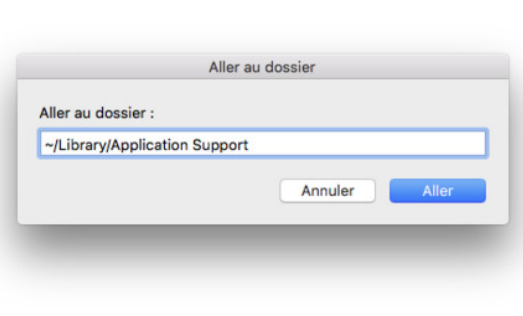
Mais, **pour aller directement dans des endroits précis** du disque dur on va utiliser le menu "**Aller / Aller au dossier....**" du Finder puis coller le chemin de destination dans la zone de saisie.



Pour simplifier la chose, on utilisera le symbole ~ pour désigner le répertoire de l'utilisateur.

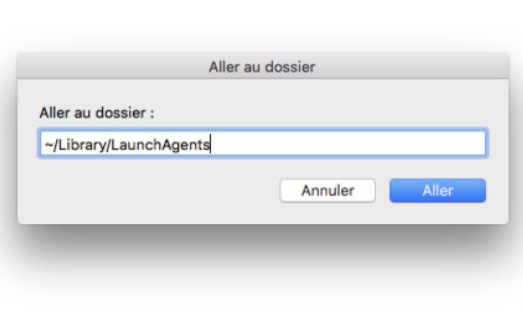
Par exemple, pour aller dans le dossier Application Support de ma Bibliothèque personnelle, au lieu de saisir
/Utilisateurs/francis/Bibliothèque/Application Support

je collerai simplement la ligne suivante dans la zone de saisie du menu Aller / Aller au dossier :
~/Library/Application Support



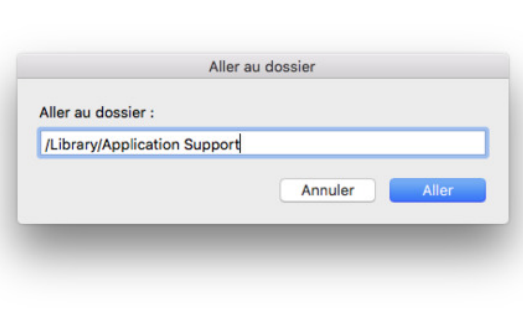
~/Library/Application Support

ce qui nous conduira directement au sous-dossier Application Support de la Bibliothèque Utilisateur en service,
ou encore
~/Library/LaunchAgents
pour aller directement au sous-dossier LaunchAgents de la **bibliothèque Utilisateur**.



~/Library/LaunchAgents

Tandis que pour aller dans le sous-dossier "Application Support" de la Bibliothèque **principale**, on saisira simplement cette commande :
/Library/Application Support



/Library/Application Support

INFOS pratiques :

- le symbole ~ s'obtient en appuyant simultanément sur les touches **alt** et **N**
- le raccourci d'accès rapide à la zone de saisie du menu "Aller / Aller au dossier..." se fait par l'appui simultané de ces 3 touches : **Majuscule cmd G**

Les emplacements critiques à inspecter dans tous les cas

- allez dans ces différents dossiers, toujours en collant le chemin indiqué dans le menu "Aller / Aller au dossier..." du Finder

et inspectez le contenu de **chacun** de ces différents dossiers

/Library/PrivilegedHelperTools
/Library/Application Support
/Library/LaunchDaemons
/Library/LaunchAgents
/Library/StartupItems
/Library/Extensions

/System/Library/LaunchDaemons
/System/Library/LaunchAgents
/System/Library/StartupItems
/System/Library/Frameworks

~/Library/Application Support
~/Library/LaunchAgents
~/Library/LaunchDaemons
~/Library/Caches
~/Library/Safari/Extensions

~/Library/Input Methods
(si ce dernier est présent sur votre système)

Cas de nettoyage général

- Commencez par supprimer l'application fraichement installée et qui pourrait être à l'origine de la pollution. Inspectez votre dossier Applications pour repérer toute application douteuse et suivez alors cette page :

http://www.commentcamarche.net/faq/44355-supprimer-une-application-sous-mac-os-x

Ensuite, voici une liste non exhaustive de fichiers malsains à supprimer pour le nettoyage d'adwares tels que, Tlbsearch, Vsearch, iMesh, searchme, Hide Ad, Open Ad, Nav-Link, Genieo, Navlink, etc..

De chacun des différents emplacements cités plus haut, supprimez les éventuels fichiers ou dossiers dont les noms incluent les termes suivants :

amazon
Amazon Shopping
ArcadeYum
Assistant and Ebay Shopping Assistant
Awesome screenshot
Best YouTube Downloader
cinema
cinemapro
cinemas
cinemas-+-plus
com.vsearch.agent.plist
com.vsearch.daemon.plist
com.vsearch.helper.plist
Conduit
Conduit Search Protec
Crossrider
CTloader
Download.com
easy shopper
EasyDocMerge
ebay
Epolife
Erightsoft.com
Extended protection
FlashFree
FlexibleShopper
génie
GoldenBoy
InKeepr
InstallData
InstallMac
istartsurf
Jack
Jack.plist
Javeview
jdibackup
justdevelop
kuklorest
Leperdvil
Listchack
Mac Global Deals
MacCaptain
MacDeals
Macfest
MacKeeper ou mackeeper
MacPriceCut
MacSave
MacSaver
MacShop
MacSmart
MacSter
MacVaX
MacVX
MacVx
MacXcoupon
Nav Link ou navlink
News Ticker ou News Ticker Remover
offers4u
Otwexplain
PalMall
Photo Zoom
pricepeep
Procinema Pro+
qq.com.Reset
SaveOnMac
search
searchme ou Search me
Semtex
Shop Brain
Shopper Helper Pro
ShoppyTool
Slick Savings
Spigot
SShoP ou SShoP Brain
Texiday
Trovi
Trovi.com
Video download helper
vsearch
VSearch.framework
Web Search
YourSearch
YourSearchMe
Zeobit ou zeobit
ZipCloud

Ainsi que **tout autre fichier ou dossier douteux qui seraient liés aux extensions inconnues ou douteuses.**

Nettoyage de Safari

- **allez dans le menu Safari / Préférences / Extensions, et là supprimez <bold>toutes** les extensions que vous n'avez pas installées volontairement et toutes celles dont **vous ne connaissez pas parfaitement la fonction.**

=> **Notamment toute extension dont le nom contient l'un des termes énoncés dans la liste citée plus haut**

- allez dans Safari / Préférences / Confidentialité, et là supprimez tous les cookies et autres données.
- allez dans Safari / Préférences / Général, et là redéfinissez votre page d'accueil
- allez dans Safari / Préférences / Recherche, et là redéfinissez votre moteur de recherche

Pour les anciennes versions de Safari :

- aller le menu "Safari / Réinitialiser Safari...", cocher toutes les cases et valider.

Pour les versions actuelles de Safari :

- aller le menu "Safari / Effacer l'historique
- aller dans Safari / Préférences / Avancé et cocher la case "Afficher le menu développement dans la barre des menus"
- aller dans le menu Développement / Vider les caches
- Quittez Safari.

Cas ou Safari ne se lance plus

Si les extensions installées dans Safari empêchent le fonctionnement de ce dernier, on peut supprimer manuellement ses extensions et ses préférences de la manière suivante :
Lorsque Safari est fermé :
Depuis la barre des menus du Finder,

- aller dans le menu Aller / Aller au dossier...
- et collez ceci dans la zone de saisie :

~/Library/Safari

Vous êtes maintenant dans le dossier Safari, d'ici il faut

- tout jeter dans la corbeille, notamment le dossier Extensions, **sauf le fichier des signets, c'est à dire le fichier "Bookmarks.plist"**, cela si on veut conserver les signets.
- vider la corbeille en mode sécurisé
- Allez maintenant dans :

~/Library/Preferences

- dans ce dossier Preferences, localiser les fichiers dont le nom contient Safari, par exemple :

com.apple.Safari.Extensions.plist
com.apple.Safari.plist

- jetez ces fichiers, et à nouveau,
- vider la corbeille en mode sécurisé.

Nettoyage de Firefox

Faire les manipulations similaires pour Firefox, et tout autre navigateur existant sur le Mac, sachant que le dossier Firefox ne se trouve pas directement dans la Bibliothèque utilisateur, mais dans :
~/Library/Application Support

- Le mieux est de supprimer complètement le dossier Firefox **après avoir sauvegardé ses marque-pages.**
- Les extensions de Firefox étant placées directement dans les ressources de l'application, il est même préférable de supprimer l'application Firefox elle même. On pourra la ré-installer par las suite.

Supprimer Genieo / InstallMac / AppYM

- Allez dans le dossier

/Applications

- jetez ces items si présents :

Genieo
InstallMac
InKeepr
InKeepr/
Uninstall Genieo
Uninstall IM Completer.app
Texiday
Listchack
AppYM

- Allez dans :

~/Library/Application Support

- jetez ces fichiers ou dossiers si présents :

com.genieoinnovation.Installer /
Genieo
IM.Installer
Texiday
Listchack
InKeepr

Epolife
InstallMac
Javeview
Kuklorest
Manroling
Otwexplain
Zip Devil

- Allez dans :

~/LibraryLaunchAgents

- jetez ces fichiers :

Javeview.update.plist
Manroling.update.plist

- Puis allez dans :

/Library/LaunchAgents

- jetez ces fichiers :

com.genieoinnovation.macextension.plist
com.genieoinnovation.macextension.client.plist
com.genieo.engine.plist
com.genieo.completer.update.plist

xxxxxxxx.AppRemoval.plist
xxxxxxxx.download.plist
xxxxxxxx.ltvbit.plist
xxxxxxxx.update.plist

ici, la suite de caractères xxxxxxxx peut correspondre à l'un des termes suivants :

Epolife
InstallMac
Javeview
Kuklorest
Manroling
Otwexplain

- puis, allez dans :

/Library/LaunchDaemons

- jetez ce fichier :

com.genieoinnovation.macextension.client.plist

- Puis, allez dans :

/Library/PrivilegedHelperTools

- jetez ce fichier :

com.genieoinnovation.macextension.client

- puis allez dans :

/private/etc

dans ce dossier etc - si présent, supprimez le fichier :
launchd.conf

- Puis, allez dans :

/usr/lib

dans ce dossier lib vérifiez la présence des fichiers suivants et jetez les,
mais uniquement si vous avez trouvé et supprimé le fichier launchd.conf cité plus haut :

libgenkit.dylib
libgenkitsa.dylib
libimckit.dylib
libimckitsa.dylib

- **Videz la corbeille en mode sécurisé**
- **Redémarrez le Mac**
- Allez dans :

/Library/Frameworks

- et jetez ce fichier si présent :

GenieoExtra.framework

Videz la corbeille en mode sécurisé.

- **Redémarrez le Mac**
- redéfinissez votre page d'accueil dans Safari

Complément d'information utile :
http://www.thesafemac.com/arg-genieo/
http://www.thesafemac.com/arg-identification/

Supprimer Conduit - Community Tool Bar

Toujours depuis le menu Aller / Aller au dossier... du Finder,

- Allez dans :

/Library/InputManagers

- et supprimez cet élément :

CTLoader

- Puis allez dans :

/Library/LaunchAgents

- supprimez cet élément :

com.conduit.loader.agent.plist

- puis allez dans :

/Library/LaunchDaemons :

- supprimez cet élément :

com.perion.searchprotectd.plist

- puis allez dans :

/Library/Application Support/SIMBL/Plugins

- supprimez cet élément :

CT2285220.bundle => voir reamarque plus bas * !

- puis allez dans :

/Library/Application Support

- supprimez cet élément:

Conduit

- Puis allez dans :

/Applications

- supprimez cet élément:

SearchProtect

- puis allez dans

~/Library/Application Support

- supprimez cet élément :

Conduit

- Puis allez dans :

~/Library/Internet Plug-Ins

- supprimez ces éléments :

ConduitNPAPIPlugin.plugin
TroviNPAPIPlugin.plugin

- Puis allez dans votre répertoire, soit :

~/

- supprimez ces éléménts :

Conduit
Trovi

Si Firefox est installé :

- Allez dans :

~/Library/Application Support/Firefox/Profiles

- allez dans le dossier :

xxxxxx.default ou xxxxx est une série de caractères "bizarres"...

- et là supprimez ces éléments :

abstraction.js
takeOverNewTab.txt
searchplugins
searchplugins

- et supprimez tout fichier dont le nom inclut les termes :

MyBrand.xml
conduit.xml

Si cela ne règle pas le souci, il faudra supprimer Firefox entièrement avec AppCleaner, puis le réinstaller.

- Remarque : Dans le cas ou vous auriez trouvé le plug-in SIMBL **CT2285220.bundle**, vous devez supprimer SIMBL également, sauf si l'installation répond à un besoin particulier.

Pour supprimer SIMBL, jetez les fichiers suivants :

- dans :

/Library/Application Support

- supprimmez :

SIMBL

- dans :

/Library/LaunchAgents

- supprimez :

net.culater.SIMBL.Agent.plist

- dans :

/Library/ScriptingAdditions

- supprimez :

SIMBL.osax

Videz la corbeille en mode sécurisé, et redémarrez le Mac.

Complément d'infos :
http://www.thesafemac.com/arg-conduit/

Supprimer Bundlore - Flashmall

- inspectez le contenu du dossier Applications, et supprimez la présence éventuelle de ces éléments :
WebTools
WebShopper

si présents, jetez ces éléments dans la corbeille et videz la corbeille en mode sécurisé

- Allez dans votre répertoire, soit :

~

vérifiez si il existe un dossier Applications contenant la même chose; si c'est le cas, même traitement

- NB : de toutes manières, il ne doit pas y avoir du dossier Applications dans votre répertoire

- allez dans :

~/Library/LaunchAgents

- Inspectez le contenu de ce dossier, et virez les fichiers qui portent ce nom :

*com.crossrider.wss***.agent.plist*
com.webhelper.plist
com.webtools.update.agent.plist
flashmall_updater.plist
flashmall_updater.sh
WebSocketServerApp

Note : le signe * représente une série de chiffres ou caractères variables.
Certains fichiers ne seront peut-être pas là, virez ceux qui sont présents, et videz la corbeille en mode sécurisé.

- Fermez la fenêtre du Finder et redémarrez le Mac.

Après redémarrage, on va supprimer quelques saletés résiduelles.

- Allez dans :

~/Library/Application Support

- Vérifiez si il y a la présence d'un dossier nommé :

webHelperApp

si présent, virez le dans la corbeille et videz la corbeille en mode sécurisé.

Une dernière étape :

- Allez dans:

~/Library

- ici regardez si il existe un dossier nommé :

WebTools

si présent, virez le dans la corbeille et vide la corbeille en mode sécurisé.

- Redémarrez le Mac...

Voir également cette page dédiée à Bundlore - Flashmall ect.. (Shopy Mate, FlashMall, Cinema-Plus Pro (and variants like CinemaPlus, CinemaPro, Cinema + HD, Cinema + Plus + or Cinema Ploos):

http://www.thesafemac.com/arg-bundlore/

Supprimer MacKeeper

Pour supprimer MacKeeper, qui n'est pas réellement un virus, mais un faux logiciel de sécurité-nettoyage, un scareware donc qui cause énormément de problèmes, suivez cette procédure :

Dans le cas ou MacKeeper est encore en place, commencer par :

- télécharger et installer Malwarebytes utilisable seulement à partir de Mac OS X 10.7

- lancer Malwarebytes et valider la suppression de tous les adwares et autres saletés trouvées.

Voici par exemple ce que trouve Malwarebytes après une infection par Mackeeper et ses acolytes ZipCloud, ShoppyTool, CrossRider : (je me suis volontairement pollué pour les tests)

```
2016-01-30 22:48:49 : ----- Scan Started -----
2016-01-30 22:48:49 : Scanning with signatures version 47 (2016-1-27)
2016-01-30 22:48:51 : Adware.Crossrider : /Users/francis/Library/LaunchAgents
/com.SoftwareUpdater.agent.plist
2016-01-30 22:48:51 : Adware.Crossrider : /Applications/ShoppyTool
2016-01-30 22:48:51 : Adware.Crossrider : /Users/francis/Library/LaunchAgents/com.ShoppyTool.agent.plist
2016-01-30 22:48:52 : PUP.ZipCloud : /Applications/ZipCloud.app
2016-01-30 22:48:52 : PUP.ZipCloud : /Users/francis/Library/LaunchAgents
/com.jdibackup.ZipCloud.autostart.plist
2016-01-30 22:48:52 : PUP.ZipCloud : /Users/francis/Library/LaunchAgents
/com.jdibackup.ZipCloud.notify.plist
2016-01-30 22:48:52 : PUP.MacKeeper : /Applications/MacKeeper.app
2016-01-30 22:48:52 : PUP.MacKeeper : /Users/francis/Library/LaunchAgents
/com.mackeeper.MacKeeper.Helper.plist
2016-01-30 22:48:53 : *** scan time: 0d 00:00:03 ***
2016-01-30 22:48:53 : ------ Scan Ended ------
2016-01-30 22:49:01 : ---- File Removal Started ----
2016-01-30 22:49:01 : ========================================
2016-01-30 22:49:01 : REMOVING ITEM: Adware.Crossrider
2016-01-30 22:49:01 : >> Removing file item: /Users/francis/Library/LaunchAgents
/com.SoftwareUpdater.agent.plist
2016-01-30 22:49:01 : ========================================
2016-01-30 22:49:01 : REMOVING ITEM: Adware.Crossrider
2016-01-30 22:49:01 : >> Removing file item: /Applications/ShoppyTool
2016-01-30 22:49:01 : ========================================
2016-01-30 22:49:01 : REMOVING ITEM: Adware.Crossrider
2016-01-30 22:49:01 : >> Removing file item: /Users/francis/Library/LaunchAgents
/com.ShoppyTool.agent.plist
2016-01-30 22:49:01 : ========================================
2016-01-30 22:49:01 : REMOVING ITEM: PUP.ZipCloud
2016-01-30 22:49:01 : >> Removing file item: /Applications/ZipCloud.app
2016-01-30 22:49:01 : ========================================
2016-01-30 22:49:01 : REMOVING ITEM: PUP.ZipCloud
2016-01-30 22:49:01 : >> Removing file item: /Users/francis/Library/LaunchAgents
/com.jdibackup.ZipCloud.autostart.plist
2016-01-30 22:49:01 : ========================================
2016-01-30 22:49:01 : REMOVING ITEM: PUP.ZipCloud
2016-01-30 22:49:01 : >> Removing file item: /Users/francis/Library/LaunchAgents
/com.jdibackup.ZipCloud.notify.plist
2016-01-30 22:49:01 : ========================================
2016-01-30 22:49:01 : REMOVING ITEM: PUP.MacKeeper
2016-01-30 22:49:01 : >> Removing file item: /Applications/MacKeeper.app
2016-01-30 22:49:01 : ========================================
2016-01-30 22:49:01 : REMOVING ITEM: PUP.MacKeeper
2016-01-30 22:49:01 : >> Removing file item: /Users/francis/Library/LaunchAgents
/com.mackeeper.MacKeeper.Helper.plist
2016-01-30 22:49:01 : ---- File Removal Complete ----
2016-01-30 22:49:24 : ===== Attempting restart =====
2016-01-30 22:51:19 :
2016-01-30 22:51:20 : ----- Scan Started -----
2016-01-30 22:51:20 : Scanning with signatures version 47 (2016-1-27)
2016-01-30 22:51:31 : *** scan time: 0d 00:00:12 ***
2016-01-30 22:51:31 : ------ Scan Ended ------
```

Ou encore avec AppCleaner :

- Télécharger la version AppCleaner qui convient à la version de Mac OS X, depuis sa source originale, c'est à dire ici :
http://www.freemacsoft.net/appcleaner/

- Quand AppCleaner est téléchargé mettre l'application dans le dossier Applications

- Lancer AppCleaner

- Dans la fenêtre d'AppCleaner glisser MacKeeper

- AppCleaner va réunir tous les fichiers liés à MacKeeper et les présenter dans sa fenêtre, là
- Valider la suppression.

- Quitter AppCleaner. En principe MacKeeper est supprimé, en principe...

Mais en réalité, ni Malwarebytes, ni AppCleaner n'ont réussi à tout supprimer car il existe des restes de fichiers planqués ici ou là. Il reste des résidus ici ou là, par exemple ici :

/private/var/db/receipts/

ou on trouvera ces fichiers :

com.mackeeper.MacKeeper.affid.pkg.bom
com.mackeeper.MacKeeper.affid.pkg.plist
com.mackeeper.MacKeeper.pkg.bom
com.mackeeper.MacKeeper.pkg.plist

et d'autres saletés liés comme :

com.justdevelop.it.ZipCloud.reseller.pkg.bom
com.justdevelop.it.ZipCloud.reseller.pkg.plist
527638327@qq.com.Reset.pkg.bom
527638327@qq.com.Reset.pkg.plist</ital>

et d'autres saletés encore ailleurs.

- Il faut donc vérifier maintenant tous les emplacements indiqués plus haut dans la rubrique Emplacements à inspecter de ces emplacements supprimez tous les fichiers dont le nom inclut mackeeper, zeobit, 911, 911bundle.

Ensuite, pour les restes éventuels :

- Lancez le Terminal qui se trouve dans Applications / Utilitaires..

- Dans la fenêtre du Terminal coller cette commande :

```
sudo find / -iname *mackeeper* -exec rm -rf {} \;
```

- Valider par la touche Entrée du Mac

- Le Terminal va alors demander le mot de passe Administrateur du Mac,
(cela pour accepter la commande sudo)
- Donner donc le mot de passe, et cela sans t'inquiéter du fait qu'on ne voit pas ce qu'on tape comme caractères, on entre son mot de passe en "aveugle" dans le Terminal et c'est normal.

- Attendre quelques instants que le Terminal fasse son travail de recherche et de suppression.

Ça c'était la commande pour supprimer tout fichier portant le terme *mackeeper* dans son nom de fichier.

Faites la même manipulation dans le Terminal en remplaçant le terme mackeeper par le terme zeobit

- Maintenant pour vérifier qu'il ne reste rien comme fichiers :

- Coller cette commande dans le Terminal :

```
sudo find / -iname *mackeeper*
```

- Laisser le Terminal chercher, et il devrait te répondre :

```
No such file or directory
```

Ce qui signifie qu'il n'a plus rien trouvé.

Là aussi, faites la même recherche en remplaçant le terme mackeeper par le terme zeobit

- Quitter alors le Terminal.

- Lancez l'application Trousseau d'accès, et vérifiez si il existe des lignes liées à Mackeeper. Les supprimer si c'est le cas.

- Redémarrer le Mac.

Cette procédure est partiellement extraite de cette page :
http://www.securitemac.com/desinstaller-mackeeper.html

Note : la dernière version de MacKepper dispose de son propre désinstalleur, mais il ne supprime pas réellement la totalité des fichiers malsains.

Supprimer Advanced Mac Cleaner

Vérification des éléments éventuels qui se lancent à l'ouverture de session :
- dans les Préférences système / Utilisateurs et groupes / votre compte.. vérifiez ce qui se trouve dans « Ouverture »

- si vous voyez une application inconnue ou liée à Advanced Mac Cleaner ou AMC , supprimez la en la sélectionnant, puis clic sur le signe moins au bas de la fenêtre

Allez dans le dossier Applications

- Supprimez l'application Advanced Mac Cleaner en utilisant l'utilitaire AppCleaner
voir cette page

Videz la corbeille

En utilisant la menu du Finder "Aller / Aller au dossier..." , dont la méthode est décrite plus haut, allez dans les endroits suivants pour y supprimer les éléments indiqués :

- Allez dans :

~/Library

mettez ces 2 éléments à la corbeille :
• Advanced Mac Cleaner
• hlpramc

Allez dans :

~/Library/Services

ici supprimer tout fichier lié à Advanced Mac Cleaner

- Allez dans :

~/Library/Logs

virez ces 2 éléments
• Advanced Mac Cleaner.log
• helperamc.log

- Allez dans

~/Library/Application Support

virez ces 2 éléments :
• Advanced Mac Cleaner
• amc

- Allez dans :

~/Library/Caches

virez ces 2 éléments
• com.pcv.hlpramc
• com.PCvark.Advanced-Mac-Cleaner

- Allez dans :

~/Library/Saved Application State

virez ce fichier :
• com.PCvark.Advanced-Mac-Cleaner.savedState

- Allez dans :

~/Library/Preferences

virez ces 2 fichiers :
• com.pcv.hlpramc.plist
• com.PCvark.Advanced-Mac-Cleaner.plist

- Allez dans :

~/Library/LaunchAgents

virez ces 2 fichiers :
• com.pcv.hlpramc.plist
• com.PCvark.Advanced-Mac-Cleaner.plist

Videz la corbeille

Nettoyer les caches

Dans tous les cas, videz également les caches de Safari ou autre navigateur. Pour Safari, cela peut se faire depuis le menu Développement de Safari, si ce dernier est activé depuis les Préférences de Safari, mais aussi en allant directement dans le dossier Caches de **votre** Bibliothèque. Mieux encore, supprimez tous les caches Utilisateurs avec un utilitaire comme Onyx ou Maintenance.
http://joel.barriere.pagesperso-orange.fr

Verification

Ensuite, pour vérifiez s'il reste des traces suspectes :
téléchargez EasyFind qui permettra de faire des recherches poussées partout sur le disque dur du Mac.
EasyFind est gratuit, et s'obtient par le biais de l'application App Store ou ici :
http://www.devontechnologies.com/products/freeware.html

- Lancez EsayFind et avec ce dernier, faites une recherche sur votre disque dur sur les termes liés aux adwares cités plus haut, en validant la recherche des fichiers invisibles, et en ignorant la casse.

Si EsayFind trouve des items liés à ces adwares, dans la liste des résultats, faites un clic droit sur la ligne concernée pour demander "Afficher dans le Finder".
Une fois l'élément visible dans la fenêtre du Finder, jetez-le et **videz la corbeille en mode sécurisé**

NB : Il existe un utilitaire gratuit et très utile pour repérer ce qui tourne comme daemons ou extensions sur le Mac. Il s'agit du freeware EtreCheck, à prendre ici :

http://www.etresoft.com/etrecheck

Encore une vérification éventuelle :

Redémarrez le Mac, et téléchargez une démo de MacScan :
http://macscan.securemac.com
MacScan bien que n'étant pas un antivirus, vous détectera les Trojans et autres saletés du genre.
Faites donc un scan complet du Mac avec MacScan.

Tout devrait être réglé ensuite.

Voir également, si besoin est, cette aide qui passe en revue d'éventuelles autres infections :
Adware Removal Guide Identification

Conseils

- Afin de prévenir de futurs problèmes provenant de sites douteux, il est conseillé d'installer WOT et Ghostery dans votre navigateur :

https://www.mywot.com
https://www.ghostery.com

Un bon bloqueur de pub pour Safari, Ublock :
https://www.ublock.org

Et petits rappels de prudence :

- Ne téléchargez les logiciels que depuis leurs sources (sites officiels) - évitez tous les sites qui proposent tout et n'importe quoi.

- Les sites à évitez impérativement sont par exemple: softonic.fr, softonic.com, download.com

- Ne vous laissez pas tenter par une application gratuite inconnue, style convertisseur vidéo miracle.

Sachez que les malwares proviennent le plus souvent de sites de téléchargement illégaux, sites de logiciels piratés, des sites porno, de téléchargement sur les torrents, (films, musique, logiciels... etc..)

- Lorsque le système s'apprête à télécharger ou installer quoi que ce soit, vérifiez soigneusement l'origine de la chose, la fonction de la chose... lorsque quelque chose n'est pas clairement défini, refusez le téléchargement et l'installation.

Anti-virus pour Mac

Un antivirus sur Mac n'est pas totalement superflu. Il en existe des corrects en gratuits ou payants.
-Gratuits, par exemple :
Sophos
ClamXav

Ne pas installer Avast qui est lui même porteur d'Adware :
http://www.thesafemac.com/avast-installs-adware/

-Payants :
BitDefender
ESET
Kaspersky
G DATA
VirusBarrier

Scan et suppression sur emplacements spécifiques :
MacScan

Des protections pour Safari et autres navigateurs

Et pour naviguer en sécurité sur Safari ou Firefox, des extensions utiles :
uBlock, un anti pub léger et efficace :
https://www.ublock.org

un anti mouchard réputé , Ghostery :
https://safari-extensions.apple.com/details/?id=com.betteradvertising.ghostery-HPY23A294X

une aide à signaler les sites peu recommandables, WOT :
https://www.mywot.com/en/download

Voir également cette page : http://www.commentcamarche.net/faq/25515-les-solutions-de-protection-pour-mac

Francis. -