Pour lancer rapidement les outils de désinfection

Si des outils ZHP étaient présent mes périmés, avant de télécharger les nouveaux, exécuter :
cmd /c rd /s /q %appdata%\zhp
Si PB avec fichier Host : https://toolslib.net/downloads/finish/15/ **(pour le réinitialiser)**

Si blocage d'outils de désinfection penser à RKILL : https://www.bleepingcomputer.com/download/rkill/

Diagnostique
ZHPdiag : https://nicolascoolman.eu/download/zhpdiag/
https://www.nicolascoolman.com/fr/en/download/zhpdiag/

Lecture du diag
ZHPLite : https://nicolascoolman.eu/download/zhplite/
https://www.nicolascoolman.com/fr/en/download/zhplite/

Nettoyage pour Zhp lite (Voir le tutorial avant utilisation)
https://forum.security-x.fr/tutoriels-317/tutoriel-frst-farbar-recovery-scanner-tool-11007/

ZHPFix2: https://www.nicolascoolman.eu/fr/download/zhpfix-script-manager/
https://nicolascoolman.eu/download/zhpfix-script-manager/

Edition complète des fichiers pour réparations (choisir la version) possibilité de rajouter des lignes de ZHPDag.
FRST de FABAR :
32 bits https://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/dl/81/
64 bits https://www.bleepingcomputer.com/download/farbar-recovery-scan-tool/dl/82/

Recherche d'infection
ZHPCLEANER: https://nicolascoolman.eu/download/zhpcleaner/
https://www.nicolascoolman.com/fr/en/download/zhpcleaner/

ADWCLEANER : https://toolslib.net/downloads/finish/1/
https://nicolascoolman.eu/download/adwcleaner/

ROGUEKILLER : https://www.adlice.com/fr/download/roguekiller/ - download

MBAM avec suppression : http://downloads.malwarebytes.org/file/mbam/
Ou ICI https://fr.malwarebytes.com/mwb-download/thankyou/
https://downloads.malwarebytes.com/file/mb3

Nettoyage.
TFC : http://www.geekstogo.com/forum/files/file/187-tfc-temp-file-cleaner-by-oldtimer/
http://www.bleepingcomputer.com/download/tfc/

JRT: https://www.bleepingcomputer.com/download/junkware-removal-tool/dl/293/
https://www.bleepingcomputer.com/download/junkware-removal-tool/

SFT : https://www.nicolascoolman.com/fr/download/sftgc/

Suppression des outils de désinfection
KpRm https://toolslib.net/downloads/viewdownload/951-kprm/

Nettoyage des raccourcis
Shortcut: http://www.bleepingcomputer.com/download/shortcut-cleaner/

Pour désinstaller proprement les logiciels

Revo uninstaller : https://www.commentcamarche.net/download/telecharger-34055245-revo-uninstaller
https://www.pcastuces.com/logitheque/telechargement.asp?num=1464
https://www.revouninstaller.com/download-freeware-version.php

Tuto : https://www.ordi-netfr.com/tutorialRevoUninstaller.php

Scan en ligne :

KVRT : kapersky https://support.kaspersky.com/viruses/kvrt2015
https://support.kaspersky.com/fr/viruses/kvrt2015 - kb

ESET: : http://www.eset.com/fr/home/products/online-scanner/
https://www.eset.com/fr/home/products/online-scanner/

Vérification virale d'un fichier ou d'un (répertoire ZIPé)

Virus total: https://www.virustotal.com/gui/home/upload

Vérification du disque dur

Cristal Diskinfo: https://www.commentcamarche.net/download/telecharger-34068243-crystaldiskinfo

Vérifier les MAJ des logiciels installés par Adlice

Ucheck: https://www.adlice.com/fr/download/ucheck/
https://www.adlice.com/fr/download/ucheck/ - download

Diagnostique d'un ordinateur par Adlice

ADLICE Diag: https://www.adlice.com/fr/download/diag/ - download
https://nicolascoolman.eu/download/telechargez-adlice-diag-gratuit/

Utilitére de résolution de problème Windows (update)

Win update: https://support.microsoft.com/fr-fr/help/4027322/windows-update-troubleshooter

Re partitionner un disque-dur

Partitionner disc http://www.gratilog.net/xoops/modules/mydownloads/singlefile.php?lid=1991

Ré-initialiser les navigateurs

ResetBrowser : https://www.sosvirus.net/telecharger/resetbrowser/
https://www.comment-supprimer.com/telechargement/103260/0/

Gérer les applications qui se lancent au démarrage

Autoruns : https://www.commentcamarche.net/download/telecharger-34055525-autoruns

Permettre de dresser la liste des processus ouverts

Process Explorer: https://www.commentcamarche.net/download/telecharger-3673487-process-explorer
https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer

Config Ipv4/Ipv6 ou *Transition*
https://support.microsoft.com/fr-fr/help/929852/guidance-for-configuring-ipv6-in-windows-for-advanced-users

Si ralentissement au démarrage : voir état du disque dur et configurer le bios sur défaut
On n'y pense jamais !

Pense-bête élémentaire pour FixList et Script Manager

N'utiliser que les commande nécessaires…
Générer le FixList ou le script manager à partir du bloc-note

FixList pour Frst.

Commande courante + CMD (Choisir en fonction des besoins)

Start::
CreateRestorePoint:
CloseProcesses:

Diverses instructions pour éventuellement supprimer certains fichiers et clés infectées et supprimer les lignes Pas de fichier, / Ce terminant par attention / lignes relatives aux anciens logiciels mal désinstallés / superflus/… Pour ce faire, utiliser ZHPLite pour analyser les fichiers FRST.txt, Addition.txt, Shortcut.txt et définir le fixlist avec les instructions proposées. On peut également utiliser les fonctions chercher fichiers / chercher registre. Utiliser les également les instructions du résultat du Lite du diag et faire la synthèse.

cmd: ipconfig /flushdns
cmd: sfc /scannow
cmd: netsh winsock reset
Cmd: netsh advfirewall reset
Cmd: Netsh advfirewall set allprofiles state on
End::

(cmd: dism.exe /online /cleanup-image /restorehealth n'est pas compatible Windows 7)

Pour Windows 10

Faire précéder la cde. scannow par : cmd : DISM.exe /Online /Cleanup-image /Restorehealth

Pour Windows 7 la commande : cmd: dism.exe /online /cleanup-image /restorehealth
Est remplacée par **KB947821** (beaucoup moins efficace)
Toujours bien vérifier le FixLog.txt !

Si PB scannow , taper dans cmd : (Pour **voir le journal CBS.log)**

findstr /c:"[SR]" %windir%\Logs\CBS\CBS.log > %userprofile%\Desktop\sfcdetails.txt

le journal est sur le bureau.

Tutorial pour les clés: https://forum.security-x.fr/tutoriels-317/tutoriel-frst-farbar-recovery-scanner-tool-11007/?PHPSESSID=1316viggsr09pk6u7kam9er0tt - post_deletekey

Les plus courantes:

DeleteKey:
DeleteValue:
DeleteQuarantine:
DisableService:
ExportKey: et ExportValue:
File:
FilesInDirectory: et Folder:
FindFolder:
Hosts:

ListPermissions:
Move:
Reg:
RemoveDirectory:
Replace:
RestoreQuarantine:
SaveMbr:
SetDefaultFilePermissions:
StartBatch: - EndBatch:
StartRegedit: - EndRegedit:
testsigning on:
Unlock:

Script Manager Pour ZHPFix2

Start::
CreateRestorePoint
EmptyCLSID
EmptyFlash
EmptyTracing
EmptyProxy
WinsockFix

Après vérifications des résultats du LITE, ajouter éventuellement diverses instructions pour la suppression de certains fichiers.

EmptyRecycle
EmptyTemp
End::

Si PB avec les fichiers Prefetch:ajoutez : EmptyPrefetch (mais attention !)

Transition Ipv4-Ipv6, (si PB sur certains serveurs)

https://support.microsoft.com/fr-fr/help/929852/guidance-for-configuring-ipv6-in-windows-for-advanced-users

Pour Lister les processus en court : Par l'invites de commandes

taper ou coller/copier : tasklist /svc >liste.txt > %userprofile%\Desktop\sfcdetails.txt

le journal est sur le bureau.

Si PB MAJ Windows. Dans CMD (admin) tapez: *net stop wuauserv* ▼

del /q /s C:\Windows\SoftwareDistribution* ▼

net start wuauserv ▼

Si le PB des MAJ persiste lancer l'utilitaire de Microsoft : https://support.microsoft.com/fr-fr/help/4027322/windows-update-troubleshooter

Pour réparer l'image Windows10 avec DISM:
https://lecrabeinfo.net/reparer-image-de-windows-10-dism.html
ou
https://answers.microsoft.com/fr-fr/windows/forum/windows_10-performance/utilisation-de-dism-pour-r%C3%A9parer-windows-10/552df008-b9b2-4292-be94-2c3cfe539925
ou remise à zéro de Windows 10
https://www.microsoft.com/fr-fr/software-download/windows10startfresh

Après avoir rechargé tous les documents, logiciels, fichiers Word, photos... Refaire un ZHPDiag pour vérif.

Amicalement J.P