# Trojan:Win32/Opachki : redirections Google

By Malekal_morte

Published: 2009-11-11 · Archived: 2026-04-05 17:09:02 UTC

Combofix supprime le malware Opachki.
Malwarebyte Anti-Malware doit aussi parvenir à supprimer l'infection.

> ComboFix 09-11-09.02 - Malekal_morte 11/11/2009 3:40.1.1 - NTFSx86
> Microsoft Windows XP Professional 5.1.2600.2.1252.33.1033.18.223.55 [GMT -8:00]
> Lancé depuis: c:\documents and settings\Malekal_morte\Desktop\ComboFix.exe
>
> AVERTISSEMENT - LA CONSOLE DE RÉCUPÉRATION N'EST PAS INSTALLÉE SUR CETTE MACHINE !!
> .
>
> ((((((((((((((((((((((((((((((((((((((( Autres suppressions ))))))))))))))))))))))))))))))))))))))))
> .
>
> c:\documents and settings\Malekal_morte\ntuser.dll
> c:\documents and settings\Malekal_morte\Start Menu\Programs\Startup\scandisk.dll
> c:\documents and settings\Malekal_morte\Start Menu\Programs\Startup\scandisk.lnk
> c:\program files\fklwur
> c:\program files\fklwur\amdcsysguard.exe
> c:\program files\sjidsv
> c:\program files\sjidsv\bvfpsysguard.exe
> c:\windows\system32\calc.dll
> c:\windows\system32\ieHElper.dll
>
> .
> ((((((((((((((((((((((((((((((((((((((( Pilotes/Services ))))))))))))))))))))))))))))))))))))))))
> .
>
> -------\Legacy_NDISRD
> -------\Service_NPF
>
> ((((((((((((((((((((((((((( Fichiers créés du 2009-10-11 au 2009-11-11 ))))))))))))))))))))))))))
> .
>
> 2009-11-11 11:10 . 2009-11-11 11:10 24064 ----a-w- C:\calc.dll
> 2009-10-31 15:19 . 2009-10-31 15:19 -------- d-----w- c:\program files\Common Files\Adobe
>
> .
> ((((((((((((((((((((((((((((((( Compte-rendu de Find3M ))))))))))))))))))))))))))))))))

.
2009-11-11 11:13 . 2009-03-20 09:44 -------- d-----w- c:\program files\System Safety Monitor
2009-10-31 15:19 . 2007-08-13 01:06 -------- d-----w- c:\program files\InCtrl5
.

((((((((((((((((((((((((((((((( Points de chargement Reg ))))))))))))))))))))))))))))))))
.
.
*Note* les éléments vides & les éléments initiaux légitimes ne sont pas listés
REGEDIT4

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]
"VMware Tools"="c:\program files\VMware\VMware Tools\VMwareTray.exe" [2007-02-05 49152]
"VMware User Process"="c:\program files\VMware\VMware Tools\VMwareUser.exe" [2007-02-05 114688]

c:\documents and settings\All Users\Start Menu\Programs\Startup\
Lancement rapide d'Adobe Reader.lnk - c:\program files\Adobe\Acrobat 7.0\Reader\reader_sl.exe [2004-12-14 29696]

[HKLM\~\services\sharedaccess\parameters\firewallpolicy\standardprofile\AuthorizedApplications\List]
"%windir%\\system32\\sessmgr.exe"=

R0 vmscsi;vmscsi;c:\windows\system32\drivers\vmscsi.sys [12/08/2007 17:19 10880]
R2 VMTools;VMware Tools Service;c:\program files\VMware\VMware Tools\VMwareService.exe [04/02/2007 19:43 159744]
R2 vnccom;vnccom;c:\windows\system32\drivers\vnccom.SYS [10/06/2008 09:05 6016]
R3 vmmouse;VMware Pointing Device;c:\windows\system32\drivers\vmmouse.sys [12/08/2007 17:19 4608]
R3 vmx_svga;vmx_svga;c:\windows\system32\drivers\vmx_svga.sys [12/08/2007 17:19 15744]
R3 vmxnet;VMware Ethernet Adapter Driver;c:\windows\system32\drivers\vmxnet.sys [12/08/2007 17:19 22528]

--- Autres Services/Pilotes en mémoire ---

*NewlyCreated* - MBR
*Deregistered* - mbr
.
.
------- Examen supplémentaire -------
.
uStart Page = hxxp://www.google.fr/
TCP: {440F4843-E2E5-4F10-BF49-C40179F015B6} = 80.10.246.1
.
- - - - ORPHELINS SUPPRIMES - - - -

HKLM-Run-WinVNC - c:\program files\UltraVNC\winvnc.exe
ShellExecuteHooks-{4F07DA45-8170-4859-9B5F-037EF2970034} -
c:\progra~1\TALLEM~1\ONLINE~1\oaevent.dll
AddRemove-HijackThis -
c:\docume~1\MALEKA~1\LOCALS~1\Temp\Rar$EX00.047\HijackThis.exe

**********

catchme 0.3.1398 W2K/XP/Vista - rootkit/stealth malware detector by Gmer, http://www.gmer.net
Rootkit scan 2009-11-11 03:44
Windows 5.1.2600 Service Pack 2 NTFS

Recherche de processus cachés ...

Recherche d'éléments en démarrage automatique cachés ...

Recherche de fichiers cachés ...

Scan terminé avec succès
Fichiers cachés: 0

**********

.
---------- Autres processus actifs ----------
.
c:\windows\system32\wscntfy.exe
.
**********

.
Heure de fin: 2009-11-11 3:45 - La machine a redémarré
ComboFix-quarantined-files.txt 2009-11-11 11:45

Avant-CF: 119 257 088 bytes free
Après-CF: 119 642 112 bytes free

- - End Of File - - 245B6C0FE4E3D154B882E34DB73E3792

---