Trojan:Win32/Opachki : redirections Google

Malekal_morte
Messages : 110339

Inscription : 10 sept. 2005 13:57

Contact :

Site internet

par **Malekal_morte** » 11 nov. 2009 12:31

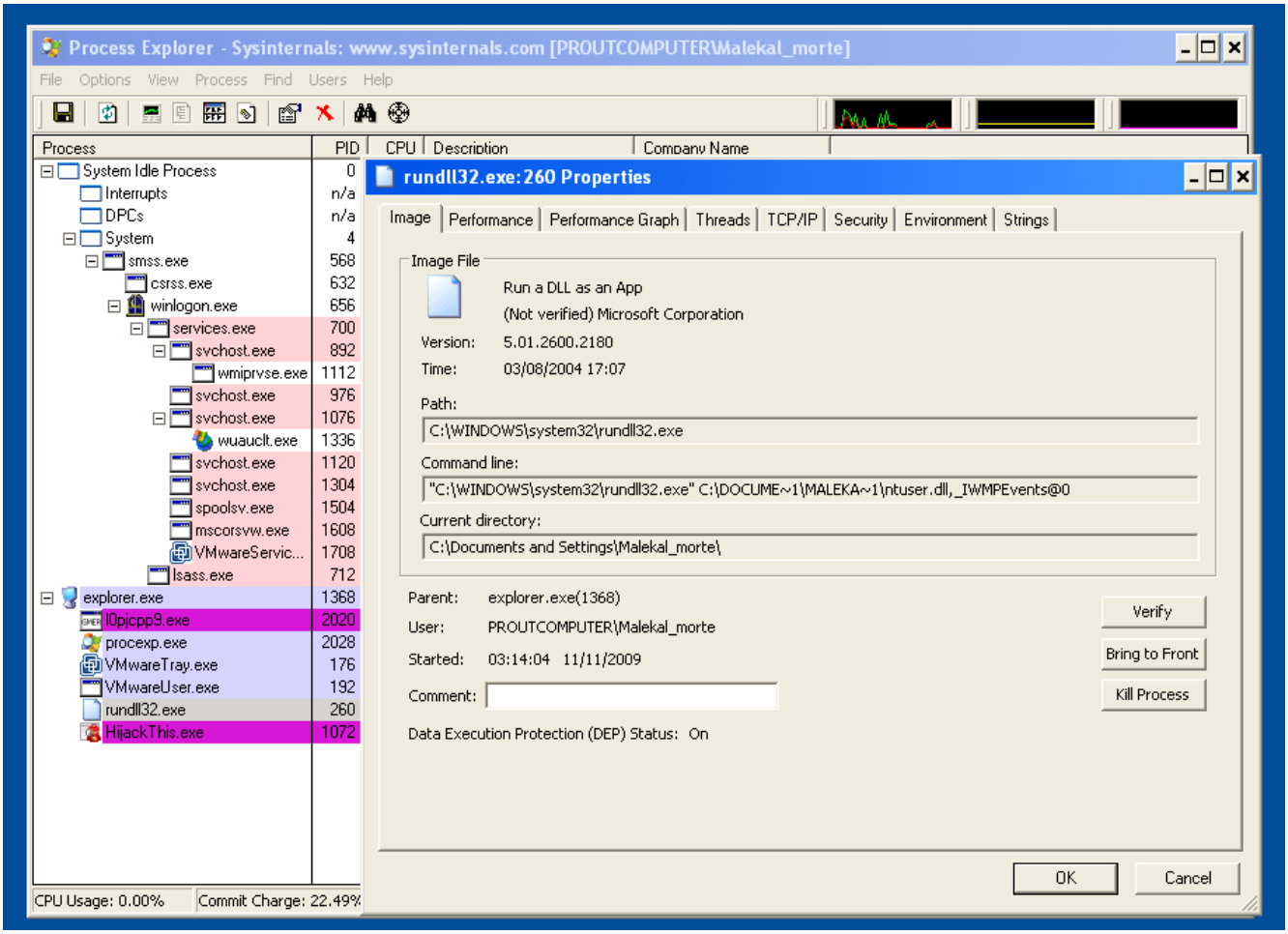
Trojan:Win32/Opachki est un malware actif depuis un an qui provoque des redirections lors des recherches Google
A l'heure où sont écrites ces lignes, les redirections ont lieux vers l'adresse thefeedwater.com
exemple :
hxx://thefeedwater.com/?do=rphp&sub=246&b=902152157&q=Logiciel%20espion%20-%20Wikip%E9dia&orig=http%3A//fr.wikipedia.org/wiki/Logiciel_espion

Trojan:Win32/Opachki est aussi associé à des infections avec des rogues, par exemple Security Tool, la famille Antivirus System Pro ou enfin seres.exe qui installe le rogueAntivirus Pro 2010

Trojan:Win32/Opachki se caractérise par des lignes avec des fichiers DLL qui sont chargées par le processus rundll32.

Exemple de lignes HiJackThis

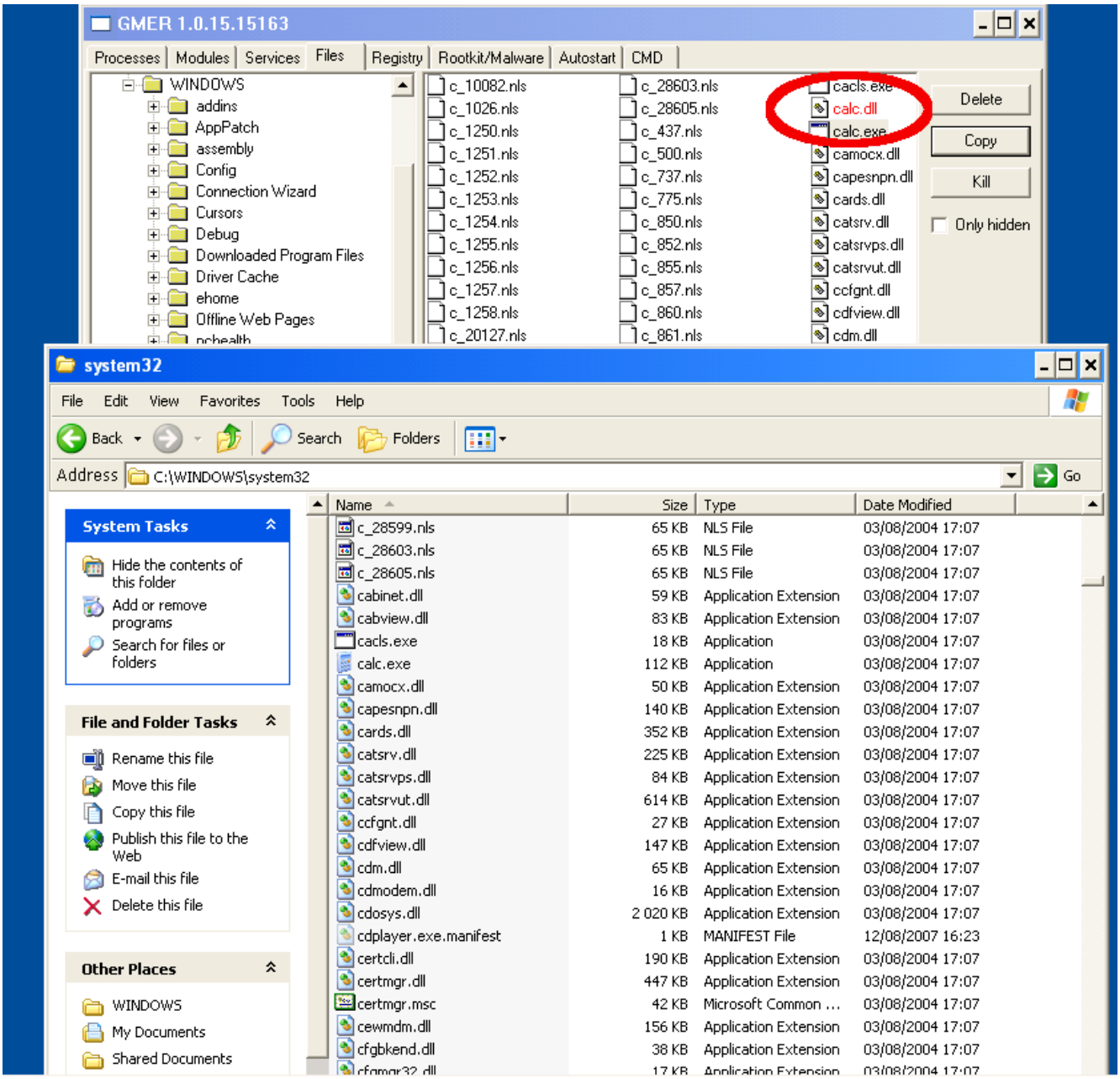
> O4 - HKLM\..\Run: [calc] rundll32.exe C:\WINDOWS\system32\calc.dll,
> O4 - HKCU\..\Run: [calc] rundll32.exe C:\DOCUME~1\MALEKA~1\ntuser.dll,

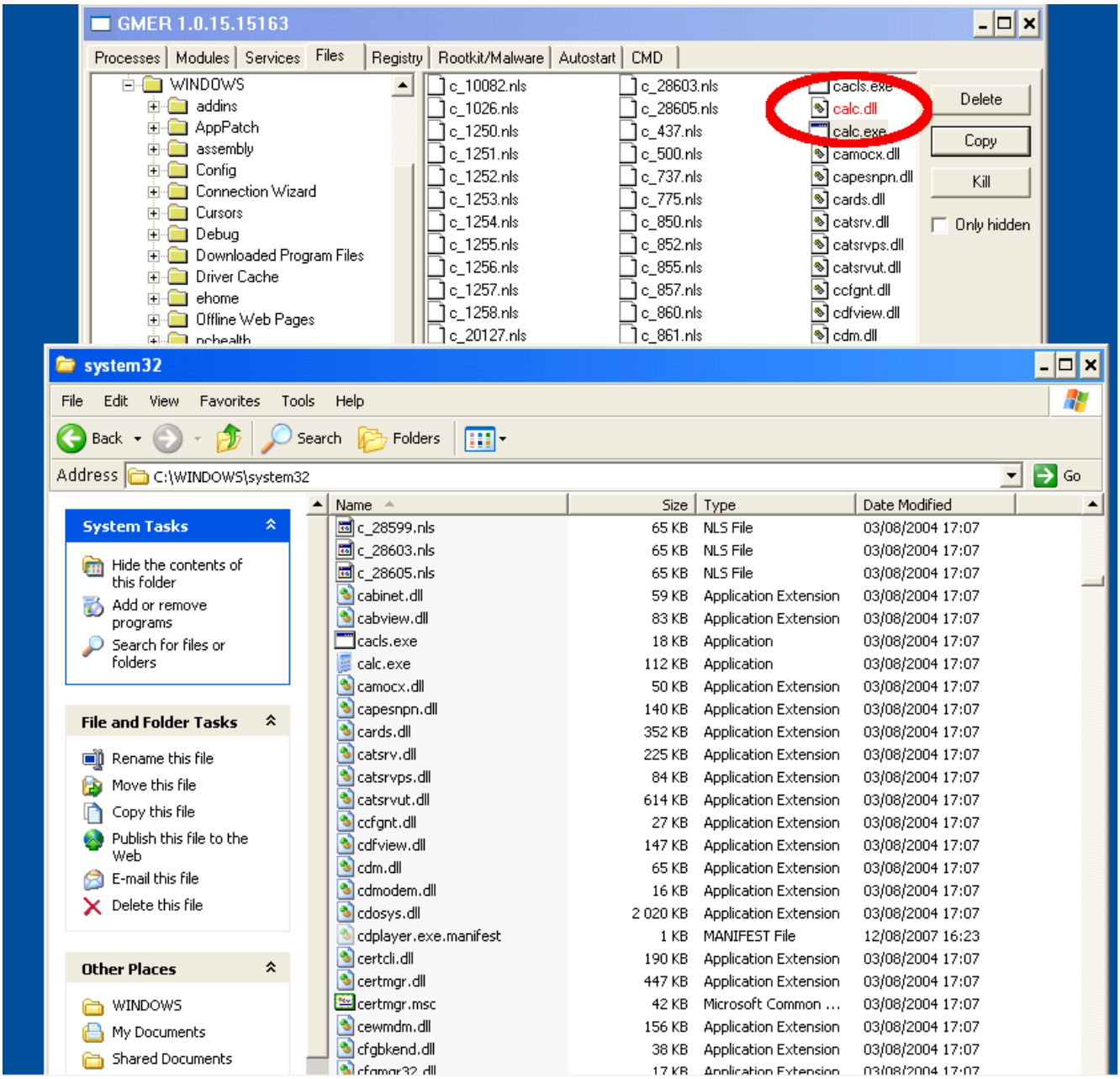


On retrouve les fichiers calc.dll, ntuser.dll mais aussi autochk.dll et scandisk.dll

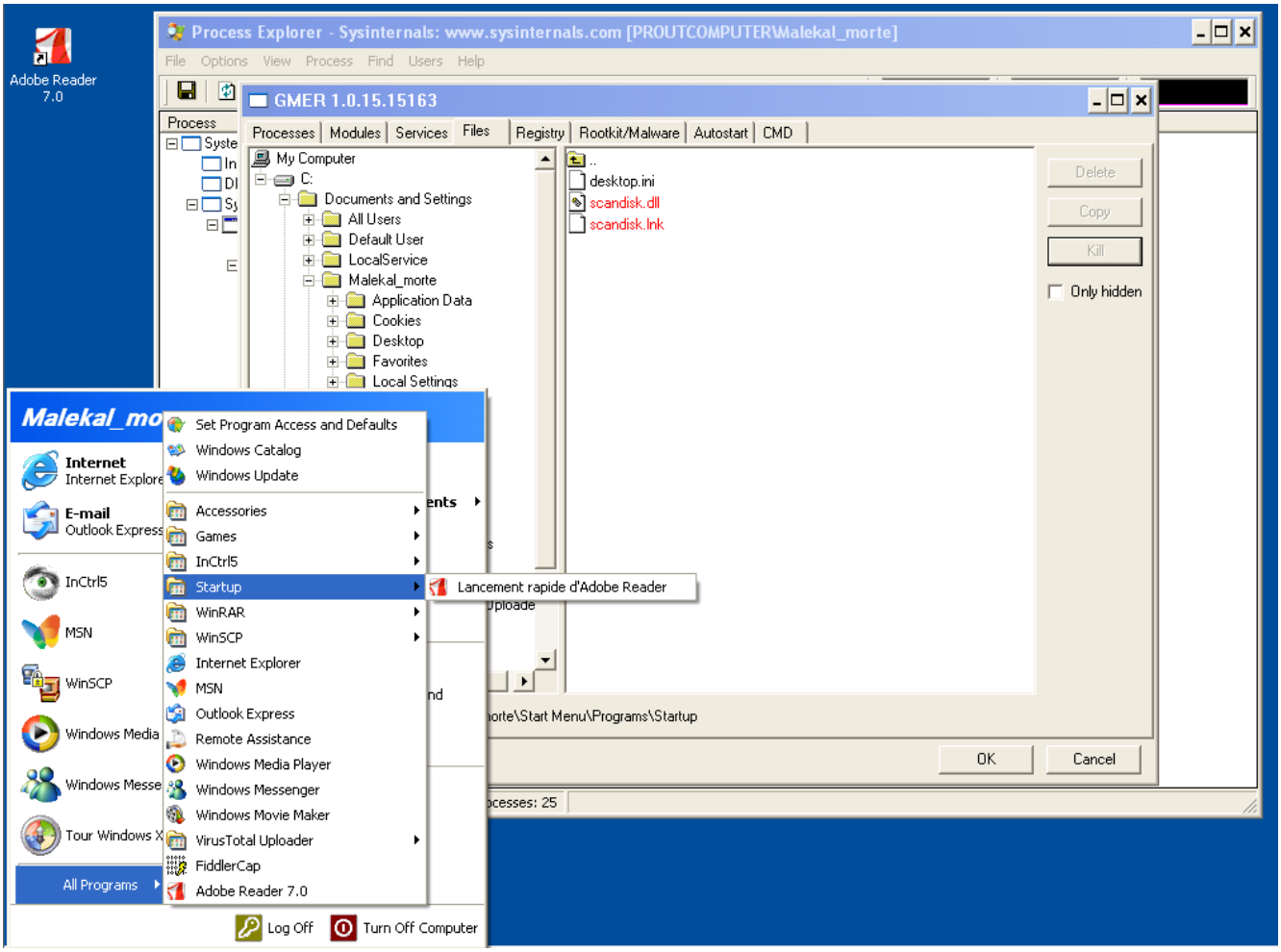
NOTE : il est impossible de tuer le processus rundll32 et fixer les lignes HijackThis ne sert à rien!
NOTE2 : il semblerait que SpyBot soit très fort pour imaginer des infections Trojan:Win32/Opachki imaginaire :
http://forum.malekal.com/cheval-troie-o ... 21803.html
http://forum.malekal.com/probleme-avec- ... ml#p179403

Les fichiers sont cachés du disque comme le montre les captures suivantes avec GMER qui montre le fichier en rouge.


GMER 1.0.15.15163
Processes
Modules
Services
Files
Registry
Rootkit/Malware
Autostart
CMD
WINDOWS
addins
AppPatch
assembly
Config
Connection Wizard
Cursors
Debug
Downloaded Program Files
Driver Cache
ehome
Offline Web Pages
c_10082.nls
c_1026.nls
c_1250.nls
c_1251.nls
c_1252.nls
c_1253.nls
c_1254.nls
c_1255.nls
c_1256.nls
c_1257.nls
c_1258.nls
c_20127.nls
c_28603.nls
c_28605.nls
c_437.nls
c_500.nls
c_737.nls
c_775.nls
c_850.nls
c_852.nls
c_855.nls
c_857.nls
c_860.nls
c_861.nls
cacls.exe
calc.dll
calc.exe
camocx.dll
capesnpn.dll
cards.dll
catsrv.dll
catsrvps.dll
catsrvut.dll
ccfgnt.dll
cdfview.dll
cdm.dll
Delete
Copy
Kill
Only hidden
system32
File
Edit
View
Favorites
Tools
Help
Back
Search
Folders
Address
C:\WINDOWS\system32
Go
System Tasks
Hide the contents of this folder
Add or remove programs
Search for files or folders
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
WINDOWS
My Documents
Shared Documents
Name
Size
Type
Date Modified
c_28599.nls 65 KB NLS File 03/08/2004 17:07
c_28603.nls 65 KB NLS File 03/08/2004 17:07
c_28605.nls 65 KB NLS File 03/08/2004 17:07
cabinet.dll 59 KB Application Extension 03/08/2004 17:07
cabview.dll 83 KB Application Extension 03/08/2004 17:07
cacls.exe 18 KB Application 03/08/2004 17:07
calc.exe 112 KB Application 03/08/2004 17:07
camocx.dll 50 KB Application Extension 03/08/2004 17:07
capesnpn.dll 140 KB Application Extension 03/08/2004 17:07
cards.dll 352 KB Application Extension 03/08/2004 17:07
catsrv.dll 225 KB Application Extension 03/08/2004 17:07
catsrvps.dll 84 KB Application Extension 03/08/2004 17:07
catsrvut.dll 614 KB Application Extension 03/08/2004 17:07
ccfgnt.dll 27 KB Application Extension 03/08/2004 17:07
cdfview.dll 147 KB Application Extension 03/08/2004 17:07
cdm.dll 65 KB Application Extension 03/08/2004 17:07
cdmodem.dll 16 KB Application Extension 03/08/2004 17:07
cdosys.dll 2 020 KB Application Extension 03/08/2004 17:07
cdplayer.exe.manifest 1 KB MANIFEST File 12/08/2007 16:23
certcli.dll 190 KB Application Extension 03/08/2004 17:07
certmgr.dll 447 KB Application Extension 03/08/2004 17:07
certmgr.msc 42 KB Microsoft Common ... 03/08/2004 17:07
cewmdm.dll 156 KB Application Extension 03/08/2004 17:07
cfgbkend.dll 38 KB Application Extension 03/08/2004 17:07



Trojan:Win32/Opachki se charche aussi via deux fichiers dans le menu Démarrer / Programmes / Démarrages qui sont aussi invisibles



GMER donne les lignes suivantes :

> GMER 1.0.15.15163 - http://www.gmer.net
> Rootkit scan 2009-11-11 03:16:35
> Windows 5.1.2600 Service Pack 2
> Running: l0pjcpp9.exe; Driver: C:\DOCUME~1\MALEKA~1\LOCALS~1\Temp\fwrcyaog.sys
>
> ---- Kernel code sections - GMER 1.0.15 ----
>
> ? C:\WINDOWS\system32\Drivers\PROCEXP100.SYS The system cannot find the file specified. !
>
> ---- Files - GMER 1.0.15 ----
>
> File C:\Documents and Settings\Malekal_morte\ntuser.dll 24064 bytes executable
> File C:\Documents and Settings\Malekal_morte\Start Menu\Programs\Startup\scandisk.dll 24064 bytes executable
> File C:\Documents and Settings\Malekal_morte\Start Menu\Programs\Startup\scandisk.lnk 655 bytes
> File C:\WINDOWS\system32\calc.dll 24064 bytes executable
>
> ---- EOF - GMER 1.0.15 ----

Exemple de détection VirusTotal même si dans l'exemple ci-dessus, ce n'est pas très parlant puisqu'on a des détections de paker, une famille FakeAlert et lême SinoMBR..
Le fait est que Trojan:Win32/Opachki est embarqué avec le rogue

File ~.exe received on 2009.11.07 04:39:49 (UTC)
Current status: finished

Result: 26/40 (65.00%)
Compact Print results
Antivirus Version Last Update Result
a-squared 4.5.0.41 2009.11.06 Packed.Win32.Krap!IK
AhnLab-V3 5.0.0.2 2009.11.06 -
AntiVir 7.9.1.61 2009.11.06 TR/Agent.AH.335
Antiy-AVL 2.0.3.7 2009.11.05 Packed/Win32.Krap
Authentium 5.2.0.5 2009.11.07 W32/Agent.IEZ
Avast 4.8.1351.0 2009.11.06 Win32:SinoMBR
AVG 8.5.0.423 2009.11.06 Generic15.AKJF
BitDefender 7.2 2009.11.07 -
CAT-QuickHeal 10.00 2009.11.06 Trojan.Krap.ah
ClamAV 0.94.1 2009.11.07 -
Comodo 2867 2009.11.07 UnclassifiedMalware
DrWeb 5.0.0.12182 2009.11.07 Trojan.Fakealert.4703
eTrust-Vet 35.1.7108 2009.11.06 -
F-Prot 4.5.1.85 2009.11.06 W32/Agent.IEZ
F-Secure 9.0.15370.0 2009.11.04 -
Fortinet 3.120.0.0 2009.11.06 W32/Krap.AH
GData 19 2009.11.07 Win32:SinoMBR
Ikarus T3.1.1.74.0 2009.11.06 Packed.Win32.Krap
Jiangmin 11.0.800 2009.11.06 -
K7AntiVirus 7.10.890 2009.11.06 Trojan.Win32.Malware.1
Kaspersky 7.0.0.125 2009.11.07 Packed.Win32.Krap.ah
McAfee 5794 2009.11.06 Generic.dx!gkv
McAfee+Artemis 5794 2009.11.06 Generic.dx!gkv
McAfee-GW-Edition 6.8.5 2009.11.06 Heuristic.LooksLike.Trojan.Agent.C
Microsoft 1.5202 2009.11.06 VirTool:Win32/Obfuscator.HG
NOD32 4580 2009.11.06 Win32/Adware.SpywareProtect2009
Norman 6.03.02 2009.11.06 -
nProtect 2009.1.8.0 2009.11.07 Trojan/W32.Krap.273920.B
Panda 10.0.2.2 2009.11.06 Trj/Zlob.KH
PCTools 7.0.3.5 2009.11.06 -
Prevx 3.0 2009.11.07 Medium Risk Malware
Rising 21.54.50.00 2009.11.07 -
Sophos 4.47.0 2009.11.07 Mal/Generic-A
Sunbelt 3.2.1858.2 2009.11.06 Trojan.Win32.Generic!BT
Symantec 1.4.4.12 2009.11.07 -
TheHacker 6.5.0.2.063 2009.11.06 -
TrendMicro 9.0.0.1003 2009.11.06 -
VBA32 3.12.10.11 2009.11.06 -
ViRobot 2009.11.6.2025 2009.11.06 -
VirusBuster 4.6.5.0 2009.11.06 Trojan.Agent.PKBP
Additional information

> File size: 273920 bytes
> MD5 : ebbd61a0c8129b405807f15007a56c3d
> SHA1 : ad7003c711555e6af70073c2d64fa6631c2b6d37
> SHA256: 77d507efbd7b691c3f5d25a970b23fddcca27cb8add487fabac7cbb44a60ba7c

Première règle élémentaire de sécurité : on réfléchit puis on clic et pas l'inverse - Les fichiers/programmes c'est comme les bonbons, quand ça vient d'un inconnu, on n'accepte pas !
➔ **Comment protéger son PC des virus**
➔ **Windows 11 : Compatibilité, Configuration minimale requise, télécharger ISO et installer Windows 11**

Comment demander de l'aide sur le forum
Partagez malekal.com : n'hésitez pas à partager les articles qui vous plaisent sur la page Facebook du site.
Malekal_morte
Messages : 110339

Inscription : 10 sept. 2005 13:57

Contact :

Site internet

Re: Trojan:Win32/Opachki : redirections Google

par **Malekal_morte** » 11 nov. 2009 12:46

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

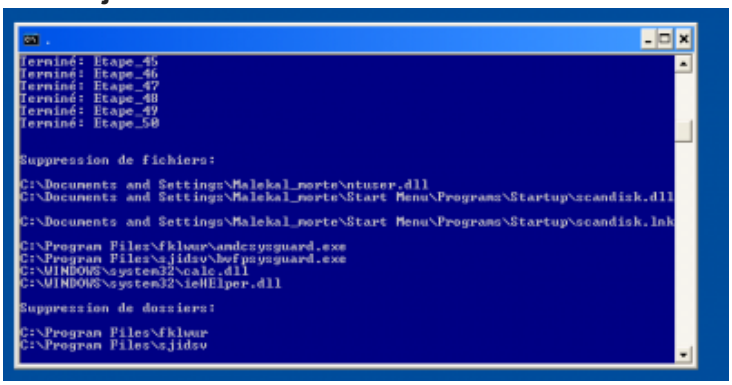
Recherche de processus cachés ...

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

Pièces jointes



Combofix supprime Opachki

Première règle élémentaire de sécurité : on réfléchit puis on clic et pas l'inverse - Les fichiers/programmes c'est comme les bonbons, quand ça vient d'un inconnu, on n'accepte pas !
➔ **Comment protéger son PC des virus**
➔ **Windows 11 : Compatibilité, Configuration minimale requise, télécharger ISO et installer Windows 11**

Comment demander de l'aide sur le forum
Partagez malekal.com : n'hésitez pas à partager les articles qui vous plaisent sur la page Facebook du site.

Répondre

Aperçu avant impression

---

2 messages • Page **1** sur **1**

Revenir à « Sécurité : Prévention, Désinfection autonome, virus & arnaques et dangers d'Internet »

Aller

- Présentations et règles du forum
- ↳ Comment demander de l'aide sur le forum
- ↳ Présentation des membres
- ↳ Je suis infecté que faire ?
- ↳ Supprimer les virus gratuitement
- ↳ Les dossiers et tutoriels du site
- ↳ Windows 11 : Compatibilité, Configuration minimale requise, Télécharger ISO et installer Windows 11
- ↳ Quel est le meilleur antivirus ?
- Windows
- ↳ Windows : Résoudre les problèmes
- ↳ Tutoriels Windows
- ↳ Accélérer Windows et problème de lenteur PC
- ↳ Réseau
- ↳ Tutoriels Réseau
- ↳ Supprimer/Desinfecter les virus (Trojan, Adwares, Ransomwares, Backdoor, Spywares)
- ↳ Sécurité : Prévention, Désinfection autonome, virus & arnaques et dangers d'Internet
- ↳ Rogues/Scareware & Programmes douteux
- ↳ Trojan.Win32.Alureon/Trojan.TDSS/Trojan.FakeAlert/Trojan.Renos et faux codec
- ↳ Adwares et PUPs (programmes indésirables)
- ↳ Ransomware
- ↳ Discussions/Aides Antivirus
- ↳ Tutoriel Antivirus
- GNU/Linux
- ↳ Tutoriels et annonces
- ↳ Utilisation de GNU/Linux
- ↳ Réseau sous GNU/Linux
- ↳ Configuration du matériel sous GNU/Linux
- Graphisme
- ↳ Galeries (Réalisations)
- ↳ Aides & Support
- ↳ Tutoriels & Ressources
- Hardware
- Général Informatique / Ressources
- ↳ Actualité & News Informatique
- ↳ Programmes utiles
- ↳ Blockulicious
- ↳ Papiers / Articles
- ↳ Sites et liens utiles
- ↳ Securite informatique
- ↳ Tech, Tips & Tricks
- ↳ Vie privée, antipub sur internet
- Général
- ↳ Questions/Commentaires sur le forum
- ↳ Discussions Générales (Autre qu'informatique).