

ComboFix 08-03-07.4 - Rold™ 2008-03-08 20:20:19.1 - NTFSx86  
Running from: C:\Documents and Settings\Rold™\Desktop\ComboFix.exe  
\* Created a new restore point

[color=red][b]WARNING -THIS MACHINE DOES NOT HAVE THE RECOVERY CONSOLE INSTALLED !![/b][/color]

(( Other Deletions ))

C:\WINDOWS\12.exe  
C:\WINDOWS\system32\pskill.exe

(( Files Created from 2008-02-08 to 2008-03-08 ))

2008-03-07 20:43 . 2008-03-07 20:43	<DIR> d-----	C:\WINDOWS\ERUNT
2008-03-07 20:42 . 2008-03-07 21:00	<DIR> d-----	C:\SDFix
2008-03-02 21:38 . 2008-03-02 21:38	35,363 --a-----	C:\WINDOWS\system32\windrvNT.sys
2008-03-02 21:29 . 2000-05-22 22:58	608,448 --a-----	C:\WINDOWS\system32\comctl32.ocx
2008-03-02 20:42 . 2008-03-02 21:39	<DIR> d-----	C:\Program Files\Folder Lock
2008-03-02 20:42 . 2005-04-11 16:40	73,728 --a-----	C:\WINDOWS\system32\FLKill.exe
2008-03-02 20:42 . 2008-03-02 20:42	53,248 --a-----	C:\WINDOWS\system32\suppdll.dll
2008-03-02 13:59 . 2008-03-02 13:58	502,368 --a-----	C:\WINDOWS\system32\drivers\amon.sys
2008-03-02 13:59 . 2008-03-02 13:58	270,336 --a-----	C:\WINDOWS\system32\imon.dll
2008-03-02 13:41 . 2008-03-02 13:41	<DIR> d-----	C:\WINDOWS\system32\QuickTimeVR.Resources
2008-03-02 13:41 . 2008-03-02 13:41	<DIR> d-----	C:\WINDOWS\system32\QuickTime.Resources
2008-03-02 13:41 . 2008-03-02 13:41	<DIR> d-----	C:\WINDOWS\system32\QuickTime
2008-03-02 13:41 . 2008-03-02 13:41	<DIR> d-----	C:\Program Files\QuickTime
2008-03-02 13:36 . 2008-03-07 20:42	<DIR> d-----	C:\Documents and Settings\Administrator\Application Data\U3
2008-02-26 19:04 . 2008-03-02 13:41	<DIR> d-----	C:\WINDOWS\system32\QuickTime(2)
2008-02-26 19:04 . 2008-03-02 13:41	<DIR> d-----	C:\Program Files\QuickTime(2)
2008-02-17 18:58 . 2008-02-17 19:01	78,999 --a-----	C:\WINDOWS\hpfins05.dat
2008-02-17 18:58 . 2005-05-24 03:44	1,395 -----	C:\WINDOWS\hpfmdl05.dat
2008-02-17 07:39 . 2008-02-17 07:39	0 --a-----	C:\Default.Bmp
2008-02-10 11:22 . 2008-02-10 11:23	<DIR> d-----	C:\Documents and Settings\Chen\Application Data\ViStart
2008-02-10 11:20 . 2008-02-10 11:20	<DIR> d-----	C:\Documents and Settings\Chen\Application Data\Styler
2008-02-09 19:53 . 2008-02-09 19:55	<DIR> d-----	C:\Documents and Settings\Rold™\Application Data\ViStart
2008-02-09 19:53 . 2008-02-09 19:55	<DIR> d-----	C:\Documents and Settings\Rold™\Application Data\ViStart



2008-01-31 19:35 ----- d----w C:\Documents and Settings\Rold™\Application Data\vlc  
2008-01-31 19:32 ----- d----w C:\Program Files\FLVPlayer  
2008-01-31 19:31 ----- d----w C:\Program Files\VideoLAN

----- Sigcheck -----

789a67335f801d6d429ae49ad82c5e57 C:\WINDOWS\system32\ntkrnlpa.exe  
----a-w 2,027,008 2004-08-04 01:07:00 C:\WINDOWS\system32\ntkrnlpa.exe  
----a-w 2,027,008 2004-08-04 01:07:00 C:\WINDOWS\system32\VITrans\ntkrnlpa.exe

5d0f5b34f58a6869b297228ef2405282 C:\WINDOWS\system32\ntoskrnl.exe  
----a-w 2,160,128 2004-08-04 01:07:00 C:\WINDOWS\system32\ntoskrnl.exe  
----a-w 2,160,128 2004-08-04 01:07:00 C:\WINDOWS\system32\VITrans\ntoskrnl.exe

4b0011b8e35843966a3ce5685058420f C:\WINDOWS\explorer.exe  
----a-w 1,422,336 2004-08-04 01:07:00 C:\WINDOWS\explorer.exe  
-c--a-w 1,032,192 2004-08-04 01:07:00 C:\WINDOWS\system32\dlldata\explorer.exe  
----a-w 1,422,336 2004-08-04 01:07:00 C:\WINDOWS\system32\VITrans\explorer.exe

(( Reg Loading Points ))

\*Note\* empty entries & legit default entries are not shown

REGEDIT4

[HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]  
"ctfmon.exe"="C:\WINDOWS\system32\ctfmon.exe" [2004-08-04 09:07 15360]  
"LClock"="C:\Program Files\LClock\LClock.exe" [2004-09-20 01:27 65536]  
"Vista Sidebar"="C:\Program Files\Vista Sidebar\sidebar.exe" [2007-11-20 13:51 524288]  
"RocketDock"="D:\installer\Software\vista package\RocketDock\RocketDock.exe" [2007-03-18 14:05 630784]

[HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run]  
"VTTimer"="VTTimer.exe" [2005-03-08 03:33 53248 C:\WINDOWS\system32\VTTimer.exe]  
"VTTrayp"="VTtrayp.exe" [2005-11-01 04:15 163840 C:\WINDOWS\system32\VTTrayp.exe]  
"NeroFilterCheck"="C:\WINDOWS\system32\NeroCheck.exe" [2001-07-09 11:50 155648]  
"InCD"="C:\Program Files\Ahead\InCD\InCD.exe" [2004-09-07 22:25 1400944]  
"RemoteControl"="C:\Program Files\CyberLink\PowerDVD\PDVDServ.exe" [2003-12-08 17:35 32768]  
"HP Software Update"="C:\Program Files\HP\HP Software Update\HPWuSchd2.exe" [2005-05-11 23:12 49152]  
"nod32upd"="C:\Program Files\Eset\fc\_upd.dll" [2007-05-12 03:39 3584]  
"Acrobat Assistant 7.0"="C:\Program Files\Adobe\Acrobat 7.0\Distillr\Acrotray.exe" [2004-12-14 02:12 483328]

"WindowNT"="c:\WINDOWS\system32\explorer.exe" [ ]  
"GrooveMonitor"="C:\Program Files\Microsoft Office\Office12\GrooveMonitor.exe" [2006-10-27 00:47 31016]  
"nav\_x"="c:\smss.exe" [ ]  
"SoundMan"="SOUNDMAN.EXE" [2006-03-01 16:22 577536 C:\WINDOWS\soundman.exe]  
"QuickTime Task"="C:\Program Files\QuickTime\qttask.exe" [2008-02-16 19:58 114688]  
"nod32kui"="C:\Program Files\Eset\nod32kui.exe" [2008-03-02 13:58 921600]  
"NVIDIA Display"="C:\WINDOWS\DisplayMonitor.exe" [ ]  
"Win32 Console"="C:\WINDOWS\cmd.exe" [ ]

[HKEY\_USERS\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Run]  
"CTFMON.EXE"="C:\WINDOWS\system32\CTFMON.EXE" [2004-08-04 09:07 15360]

C:\Documents and Settings\Chen\Start Menu\Programs\Startup\  
OneNote 2007 Screen Clipper and Launcher.lnk - C:\Program Files\Microsoft Office\Office12\ONENOTEM.EXE [2006-10-26 20:24:54 98632]

C:\Documents and Settings\Rold T\Start Menu\Programs\Startup\  
Adobe Gamma.lnk - C:\Program Files\Common Files\Adobe\Calibration\Adobe Gamma Loader.exe [2005-03-16 19:16:50 113664]  
OneNote 2007 Screen Clipper and Launcher.lnk - C:\Program Files\Microsoft Office\Office12\ONENOTEM.EXE [2006-10-26 20:24:54 98632]  
Thoojsje Vista Sidebar.lnk - C:\Program Files\Vista Sidebar\sidebar.exe [2008-02-09 19:46:35 524288]

C:\Documents and Settings\All Users\Start Menu\Programs\Startup\  
Adobe Acrobat Speed Launcher.lnk - C:\WINDOWS\Installer\{AC76BA86-1033-0000-7760-000000000002}\SC\_Acrobat.exe [2007-07-28 23:18:09 25214]  
HP Digital Imaging Monitor.lnk - C:\Program Files\HP\Digital Imaging\bin\hpqtra08.exe [2005-05-11 23:23:26 282624]  
Setup.exe [2008-03-04 09:13:05 86016]

[HKEY\_LOCAL\_MACHINE\software\microsoft\windows nt\currentversion\winlogon\notify\MCPClient]  
C:\Program Files\Common Files\Stardock\mcpsub.dll 2003-08-25 11:25 139264 C:\Program Files\Common Files\Stardock\MCPStub.dll

[HKLM\~\services\sharedaccess\parameters\firewallpolicy\standardprofile\AuthorizedApplications\List]  
"%windir%\system32\sessmgr.exe"=  
"C:\SIERRA\Half-Life\hl.exe"=  
"C:\Program Files\Microsoft Office\Office12\OUTLOOK.EXE"=  
"C:\Program Files\Microsoft Office\Office12\GROOVE.EXE"=  
"C:\Program Files\Microsoft Office\Office12\ONENOTE.EXE"=

R0 videX32;videX32;C:\WINDOWS\system32\DRIVERS\videX32.sys [2006-02-23 11:38]  
R0 xfilt;VIA SATA IDE Hot-plug Driver;C:\WINDOWS\system32\DRIVERS\xfilt.sys [2006-02-23 11:39]

[HKEY\_CURRENT\_USER\software\microsoft\windows\currentversion\explorer\mountpoints2\{05c6174e-1777-11dc-a175-0016ecf01d56}]  
\Shell\AutoRun\command - G:\LaunchU3.exe

```
[HKEY_CURRENT_USER\software\microsoft\windows\currentversion\explorer\mountpoints2\{e0b56d46-e390-11db-a14b-0016ecf01d56}]\Shell\AutoRun\command - I:\LaunchU3.exe
```

.

\*\*\*\*\*

catchme 0.3.1344 W2K/XP/Vista - rootkit/stealth malware detector by Gmer, <http://www.gmer.net>

Rootkit scan 2008-03-08 20:22:33

Windows 5.1.2600 Service Pack 2 NTFS

scanning hidden processes ...

scanning hidden autostart entries ...

scanning hidden files ...

disk error: C:\WINDOWS\

\*\*\*\*\*

.

Completion time: 2008-03-08 20:24:13

ComboFix-quarantined-files.txt 2008-03-08 12:23:19