Logfile of Trend Micro HijackThis v2.0.2
Scan saved at 12:01:06 PM, on 5/19/2010
Platform: Windows XP SP3 (WinNT 5.01.2600)
MSIE: Internet Explorer v7.00 (7.00.6000.17023)
Boot mode: Safe mode

Running processes:
C:\WINDOWS\System32\smss.exe
C:\WINDOWS\system32\winlogon.exe
C:\WINDOWS\system32\services.exe
C:\WINDOWS\system32\lsass.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\system32\svchost.exe
C:\WINDOWS\Explorer.EXE
C:\Documents and Settings\HERIBERTO MAZA\Desktop\TREND MICRO HijackThis\HijackThis.exe

R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Bar = http://us.rd.yahoo.com/customize/ie/defaults/sb/msgr9/*http://www.yahoo.com/ext/search/search.html
R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://www.supportforyourpc.com/
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/?LinkId=69157
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/?LinkId=69157
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = *.local
R3 - URLSearchHook: Answers.com Toolbar - {6341761b-babe-406d-b0d6-8d99b81c2ee5} - C:\Program Files\Answers.com\tbAnsw.dll
O2 - BHO: IDM Helper - {0055C089-8582-441B-A0BF-17B458C2A3A8} - D:\Program Files\Internet Download Manager\IDMIECC.dll
O2 - BHO: HelperObject Class - {00C6482D-C502-44C8-8409-FCE54AD9C208} - D:\Program Files\TechSmith\SnagIt 7\SnagItBHO.dll
O2 - BHO: &Yahoo! Toolbar Helper - {02478D38-C3F9-4efb-9B51-7695ECA05670} - C:\Program Files\Yahoo!\Companion\Installs\cpn3\yt.dll
O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - C:\Program Files\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll
O2 - BHO: RealPlayer Download and Record Plugin for Internet Explorer - {3049C3E9-B461-4BC5-8870-4C09146192CA} - C:\Program Files\Real\RealPlayer\rpbrowserrecordplugin.dll
O2 - BHO: Spybot-S&D IE Protection - {53707962-6F74-2D53-2644-206D7942484F} - D:\Program Files\Spybot - Search & Destroy\SDHelper.dll
O2 - BHO: Yahoo! IE Services Button - {5BAB4B5B-68BC-4B02-94D6-2FC0DE4A7897} - C:\Program Files\Yahoo!\Common\yiesrvc.dll
O2 - BHO: Answers.com Toolbar - {6341761b-babe-406d-b0d6-8d99b81c2ee5} - C:\Program Files\Answers.com\tbAnsw.dll
O2 - BHO: Windows Live ID Sign-in Helper - {9030D464-4C02-4ABF-8ECC-5164760863C6} - C:\Program Files\Common Files\Microsoft Shared\Windows Live\WindowsLiveLogin.dll
O2 - BHO: BHO Class - {9AD9826C-E2B6-4E24-A3AC-C49A505BD0EA} - D:\Program Files\CallingID\CallingID.dll
O2 - BHO: Google Toolbar Helper - {AA58ED58-01DD-4d91-8333-CF10577473F7} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll
O2 - BHO: Google Toolbar Notifier BHO - {AF69DE43-7D58-4638-B6FA-CE66B5AD205D} - C:\Program Files\Google\GoogleToolbarNotifier\5.5.4723.1820\swg.dll

O2 - BHO: MapQuest Toolbar Loader - {bd3fd433-147a-482e-a192-614f26e2310c} - C:\Program Files\MapQuest Toolbar\mapquesttb.dll
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files\Java\jre6\bin\jp2ssv.dll
O2 - BHO: JQSIEStartDetectorImpl - {E7E6F031-17CE-4C07-BC86-EABFE594F69C} - C:\Program Files\Java\jre6\lib\deploy\jqs\ie\jqs_plugin.dll
O2 - BHO: OToolbarHelper Class - {EAD3A971-6A23-4246-8691-C9244E858967} - C:\Program Files\PayPal\PayPal Plug-In\PayPalHelper.dll
O2 - BHO: SingleInstance Class - {FDAD4DA1-61A2-4FD8-9C17-86F7AC245081} - C:\Program Files\Yahoo!\Companion\Installs\cpn3\YTSingleInstance.dll
O3 - Toolbar: CallingID - {AC897D33-1DB7-4151-B425-2DA88D5A6BED} - D:\Program Files\CallingID\CallingID.dll
O3 - Toolbar: SnagIt - {8FF5E183-ABDE-46EB-B09E-D2AAB95CABE3} - D:\Program Files\TechSmith\SnagIt 7\SnagItIEAddin.dll
O3 - Toolbar: PayPal Plug-In - {DC0F2F93-27FA-4f84-ACAA-9416F90B9511} - C:\Program Files\PayPal\PayPal Plug-In\OToolbar.dll
O3 - Toolbar: Yahoo! Toolbar - {EF99BD32-C1FB-11D2-892F-0090271D4F88} - C:\Program Files\Yahoo!\Companion\Installs\cpn3\yt.dll
O3 - Toolbar: Google Toolbar - {2318C2B1-4965-11d4-9B18-009027A5CD4F} - C:\Program Files\Google\Google Toolbar\GoogleToolbar_32.dll
O3 - Toolbar: MapQuest Toolbar - {9302e698-7e00-43ab-b867-c6e759bc2ada} - C:\Program Files\MapQuest Toolbar\mapquesttb.dll
O3 - Toolbar: Answers.com Toolbar - {6341761b-babe-406d-b0d6-8d99b81c2ee5} - C:\Program Files\Answers.com\tbAnsw.dll
O4 - HKLM\..\Run: [StartupFaster] "D:\Program Files\Startup Faster\startuploader.exe" -run SFAURUN SFCURUN SFAUSTARTUP SFCUSTARTUP
O4 - HKLM\..\Run: [TkBellExe] "C:\Program Files\Common Files\Real\Update_OB\realsched.exe" -osboot
O4 - HKCU\..\Run: [ctfmon.exe] C:\WINDOWS\system32\ctfmon.exe
O4 - HKCU\..\Run: [Clipboard Buddy] D:\PROGRA~1\CLIPBO~1\CLIPBO~1.EXE
O4 - HKCU\..\Run: [IDMan] D:\Program Files\Internet Download Manager\IDMan.exe /onboot
O4 - HKCU\..\Run: [AccountLogon] D:\Program Files\AccountLogon\AccountLogon.exe
O4 - HKCU\..\Run: [AOL Fast Start] "D:\Program Files\AOL 9.5\AOL.EXE" -b
O4 - HKUS\S-1-5-20\..\RunOnce: [tscuninstall] %systemroot%\system32\tscupgrd.exe (User 'NETWORK SERVICE')
O4 - HKUS\S-1-5-18\..\RunOnce: [tscuninstall] %systemroot%\system32\tscupgrd.exe (User 'SYSTEM')
O4 - HKUS\.DEFAULT\..\RunOnce: [tscuninstall] %systemroot%\system32\tscupgrd.exe (User 'Default user')
O4 - Startup: StartupFaster
O4 - Global Startup: StartupFaster
O6 - HKCU\Software\Policies\Microsoft\Internet Explorer\Restrictions present
O6 - HKCU\Software\Policies\Microsoft\Internet Explorer\Control Panel present
O8 - Extra context menu item: AccountLogon - C:\WINDOWS\al-popup-heriberto maza.html
O8 - Extra context menu item: Answers... - file://C:\Program Files\1-Click Answers\Html\atiemenu.htm
O8 - Extra context menu item: Download all links with IDM - D:\Program Files\Internet Download Manager\IEGetAll.htm
O8 - Extra context menu item: Download FLV video content with IDM - D:\Program Files\Internet Download Manager\IEGetVL.htm
O8 - Extra context menu item: Download with IDM - D:\Program Files\Internet Download Manager\IEExt.htm
O9 - Extra button: Send to OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - D:\PROGRA~1\MICROS~1\Office12\ONBttnIE.dll
O9 - Extra 'Tools' menuitem: S&end to OneNote - {2670000A-7350-4f3c-8081-5663EE0C6C49} - D:\PROGRA~1\MICROS~1\Office12\ONBttnIE.dll
O9 - Extra button: Spyware Doctor - {2D663D1A-8670-49D9-A1A5-4C56B4E14E84} - C:\WINDOWS\system32\shdocvw.dll
O9 - Extra button: Yahoo! Services - {5BAB4B5B-68BC-4B02-94D6-2FC0DE4A7897} - C:\Program Files\Yahoo!\Common\yiesrvc.dll
O9 - Extra button: Research - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - D:\PROGRA~1\MICROS~1\Office12\REFIEBAR.DLL

O9 - Extra button: WinAVI FLV Manager - {DE365254-2F9B-4908-9E3A-7AAA6EC90BCC} - C:\WINDOWS\system32\shdocvw.dll
O9 - Extra 'Tools' menuitem: WinAVI FLV Manager - {DE365254-2F9B-4908-9E3A-7AAA6EC90BCC} - C:\WINDOWS\system32\shdocvw.dll
O9 - Extra button: (no name) - {DFB852A3-47F8-48C4-A200-58CAB36FD2A2} - D:\Program Files\Spybot - Search & Destroy\SDHelper.dll
O9 - Extra 'Tools' menuitem: Spybot - Search & Destroy Configuration - {DFB852A3-47F8-48C4-A200-58CAB36FD2A2} - D:\Program Files\Spybot - Search & Destroy\SDHelper.dll
O9 - Extra button: (no name) - {e2e2dd38-d088-4134-82b7-f2ba38496583} - C:\WINDOWS\Network Diagnostic\xpnetdiag.exe
O9 - Extra 'Tools' menuitem: @xpsp3res.dll,-20001 - {e2e2dd38-d088-4134-82b7-f2ba38496583} - C:\WINDOWS\Network Diagnostic\xpnetdiag.exe
O9 - Extra button: Yahoo! Messenger - {E5D12C4E-7B4F-11D3-B5C9-0050045C3C96} - C:\Program Files\Yahoo!\Messenger\YahooMessenger.exe
O9 - Extra 'Tools' menuitem: Yahoo! Messenger - {E5D12C4E-7B4F-11D3-B5C9-0050045C3C96} - C:\Program Files\Yahoo!\Messenger\YahooMessenger.exe
O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\WINDOWS\system32\shdocvw.dll
O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\WINDOWS\system32\shdocvw.dll
O9 - Extra button: AccountLogon - {1CB13C88-96B6-11d6-9AF5-D12D26EE1F36} - C:\WINDOWS\al-popup-heriberto maza.html (HKCU)
O9 - Extra 'Tools' menuitem: AccountLogon - {1CB13C88-96B6-11d6-9AF5-D12D26EE1F36} - C:\WINDOWS\al-popup-heriberto maza.html (HKCU)
O16 - DPF: {0742B9EF-8C83-41CA-BFBA-830A59E23533} (Microsoft Data Collection Control) - https://support.microsoft.com/OAS/ActiveX/MSDcode.cab
O16 - DPF: {0E5F0222-96B9-11D3-8997-00104BD12D94} (PCPitstop Utility) - http://www.pcpitstop.com/betapit/PCPitStop.CAB
O16 - DPF: {116D4961-37BF-4A0A-919E-673A1B2D89A0} (CSDVRS) - http://www.csdvrs.com/CSDVRS.ocx
O16 - DPF: {30528230-99f7-4bb4-88d8-fa1d4f56a2ab} (Installation Support) - C:\Program Files\Yahoo!\Common\Yinsthelper200711281.dll
O16 - DPF: {49232000-16E4-426C-A231-62846947304B} (SysData Class) - http://ipgweb.cce.hp.com/rdqaio/downloads/sysinfo.cab
O16 - DPF: {9732FB42-C321-11D1-836F-00A0C993F125} (mhLabel Class) - http://www.pcpitstop.com/mhLbl.cab
O16 - DPF: {D27CDB6E-AE6D-11CF-96B8-444553540000} (Shockwave Flash Object) - http://fpdownload2.macromedia.com/get/flashplayer/current/swflash.cab
O16 - DPF: {E77F23EB-E7AB-4502-8F37-247DBAF1A147} (Windows Live Hotmail Photo Upload Tool) - http://gfx2.hotmail.com/mail/w4/pr01/photouploadcontrol/MSNPUpld.cab
O17 - HKLM\System\CS103\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS105\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS106\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS107\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS108\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS109\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS110\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS111\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS112\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS113\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}: NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS114\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:

NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS115\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS116\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS117\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS118\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS119\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS120\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS121\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS122\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS123\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS124\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS125\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS126\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS127\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS128\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS129\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS130\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS131\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS132\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS133\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS134\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O17 - HKLM\System\CS135\Services\Tcpip\..\{25C53D09-25C7-4A50-8277-C26300DEADDD}:
NameServer = 208.67.222.222,208.67.220.220
O20 - Winlogon Notify: !SASWinLogon - D:\Program Files\SUPERAntiSpyware\SASWINLO.DLL
O23 - Service: Acronis Scheduler2 Service (AcrSch2Svc) - Acronis - C:\Program
Files\Common Files\Acronis\Schedule2\schedul2.exe
O23 - Service: Adobe Active File Monitor V5 (AdobeActiveFileMonitor5.0) - Unknown
owner - D:\Program Files\Adobe\Photoshop Elements 5.0\PhotoshopElementsFileAgent.exe
O23 - Service: AOL Connectivity Service (AOL ACS) - AOL LLC - C:\Program
Files\Common Files\AOL\ACS\AOLAcsd.exe
O23 - Service: Apple Mobile Device - Apple Inc. - C:\Program Files\Common
Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe
O23 - Service: Bonjour Service - Apple Inc. - C:\Program
Files\Bonjour\mDNSResponder.exe
O23 - Service: Canon Camera Access Library 8 (CCALib8) - Canon Inc. - C:\Program
Files\Canon\CAL\CALMAIN.exe
O23 - Service: Diskeeper - Diskeeper Corporation - D:\Program Files\Diskeeper
Corporation\Diskeeper\DkService.exe
O23 - Service: Google Update Service (gupdate1c9dd7a8df5dcfe)
(gupdate1c9dd7a8df5dcfe) - Google Inc. - C:\Program
Files\Google\Update\GoogleUpdate.exe
O23 - Service: Google Software Updater (gusvc) - Google - C:\Program
Files\Google\Common\Google Updater\GoogleUpdaterService.exe

O23 - Service: InstallDriver Table Manager (IDriverT) - Macrovision Corporation - C:\Program Files\Common Files\InstallShield\Driver\11\Intel 32\IDriverT.exe
O23 - Service: iPod Service - Apple Inc. - C:\Program Files\iPod\bin\iPodService.exe
O23 - Service: Java Quick Starter (JavaQuickStarterService) - Sun Microsystems, Inc. - C:\Program Files\Java\jre6\bin\jqs.exe
O23 - Service: LVCOMSer - Logitech Inc. - C:\Program Files\Common Files\LogiShrd\LVCOMSER\LVComSer.exe
O23 - Service: Process Monitor (LVPrcSrv) - Logitech Inc. - C:\Program Files\Common Files\LogiShrd\LVMVFM\LVPrcSrv.exe
O23 - Service: LVSrvLauncher - Logitech Inc. - C:\Program Files\Common Files\LogiShrd\SrvLnch\SrvLnch.exe
O23 - Service: Pml Driver HPZ12 - HP - C:\WINDOWS\system32\HPZipm12.exe
O23 - Service: Cyberlink RichVideo Service(CRVS) (RichVideo) - Unknown owner - C:\Program Files\CyberLink\Shared Files\RichVideo.exe
O23 - Service: Trend Micro Central Control Component (SfCtlCom) - Trend Micro Inc. - D:\Program Files\Trend Micro\Internet Security\SfCtlCom.exe
O23 - Service: Audio Service (STacSV) - IDT, Inc. - c:\program files\idt\intelxpv_v103\wdm\STacSV.exe
O23 - Service: Trend Micro Unauthorized Change Prevention Service (TMBMServer) - Trend Micro Inc. - D:\Program Files\Trend Micro\BM\TMBMSRV.exe
O23 - Service: Trend Micro Personal Firewall (TmPfw) - Trend Micro Inc. - D:\Program Files\Trend Micro\Internet Security\TmPfw.exe
O23 - Service: Trend Micro Proxy Service (TmProxy) - Trend Micro Inc. - D:\Program Files\Trend Micro\Internet Security\TmProxy.exe
O23 - Service: TomTomHOMEService - TomTom - D:\Program Files\TomTom HOME 2\TomTomHOMEService.exe
O23 - Service: TuneUp Drive Defrag Service (TuneUp.Defrag) - TuneUp Software - D:\Program Files\TuneUp Utilities 2010\TuneUpDefragService.exe
O23 - Service: TuneUp Utilities Service (TuneUp.UtilitiesSvc) - TuneUp Software - D:\Program Files\TuneUp Utilities 2010\TuneUpUtilitiesService32.exe
O23 - Service: Yahoo! Updater (YahooAUService) - Yahoo! Inc. - C:\Program Files\Yahoo!\SoftwareUpdate\YahooAUService.exe

--
End of file - 17105 bytes