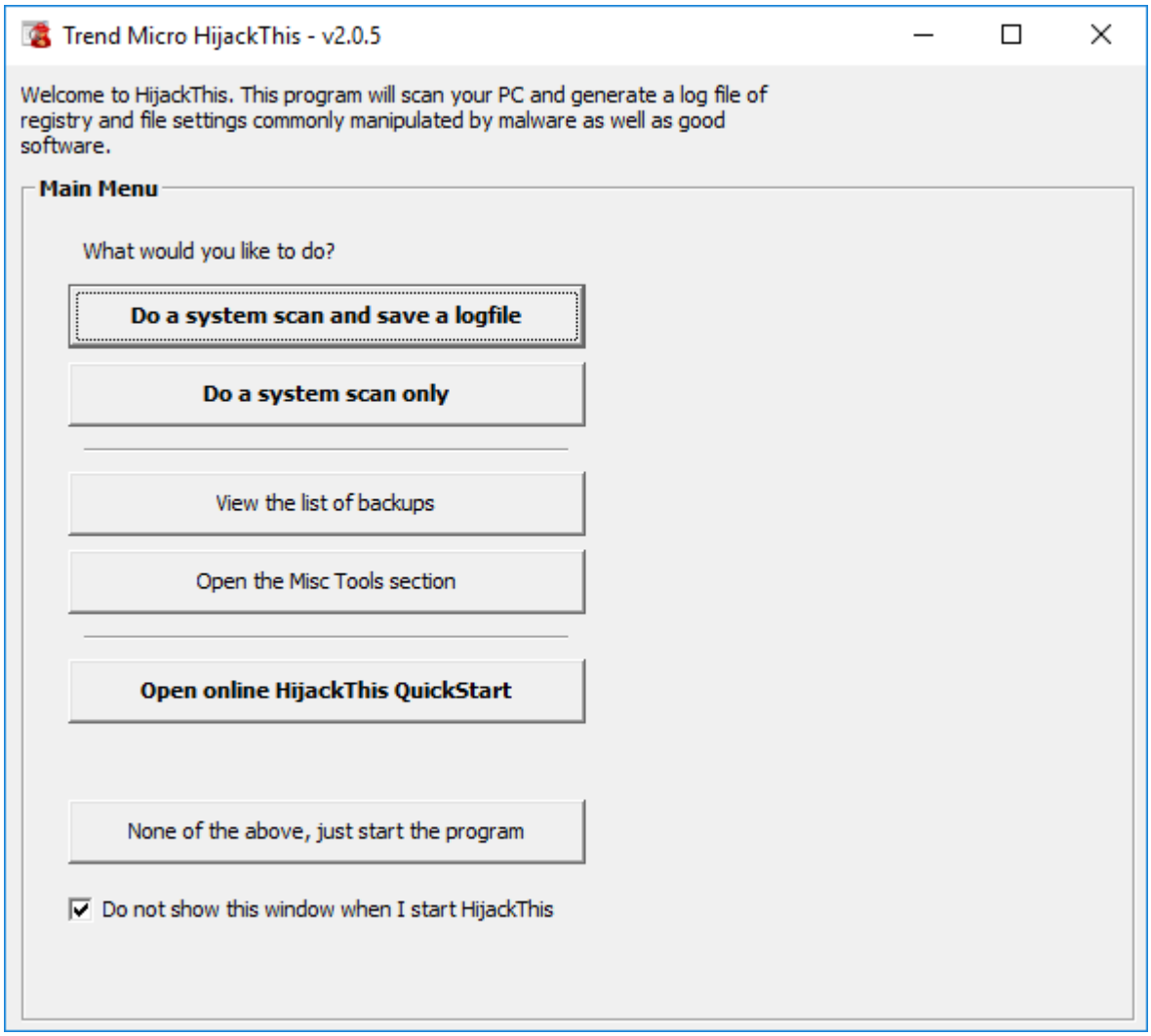
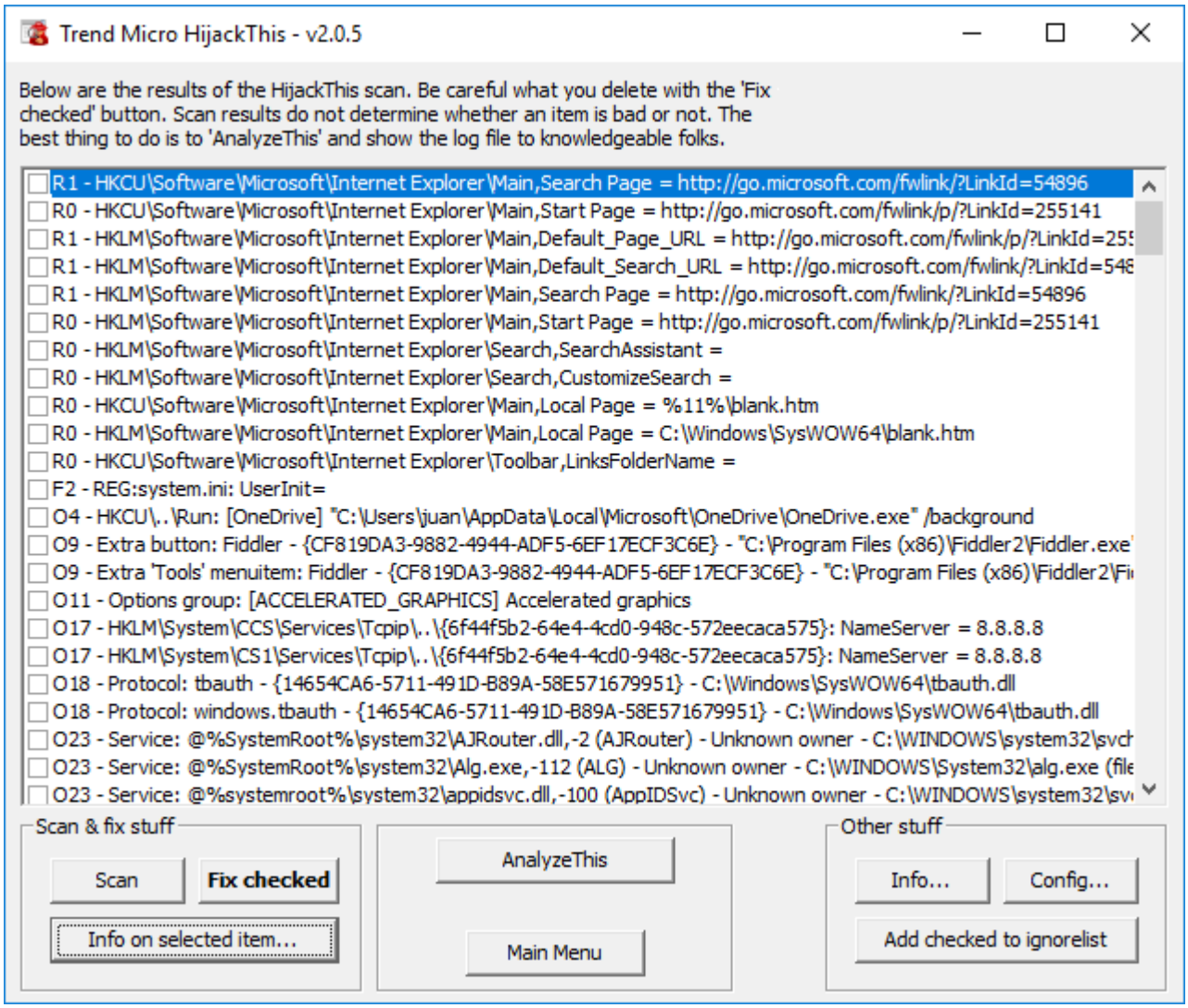
HiJackThis

HijackThis is a free utility that generates an in depth report of registry and file settings from your computer. HijackThis scan results make no separation between safe and unsafe settings , which gives you the ability to selectively remove items from your machine. In addition to scan and remove capabilities, HijackThis comes with several useful tools to manually remove malware from your computer. However, HijackThis does not make value based calls between what is considered good or bad. It is important to exercise caution and avoid making changes to your computer settings, unless you have expert knowledge. Source code is available SourceForge, under Code and also as a zip file under Files.




Trend Micro HijackThis - v2.0.5
Below are the results of the HijackThis scan. Be careful what you delete with the 'Fix checked' button. Scan results do not determine whether an item is bad or not. The best thing to do is to 'AnalyzeThis' and show the log file to knowledgeable folks.
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://go.microsoft.com/fwlink/p/?LinkId=255141
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/p/?LinkId=255
R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=548
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/p/?LinkId=255141
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =
R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =
R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Local Page = %11%\blank.htm
R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SysWOW64\blank.htm
R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =
F2 - REG:system.ini: UserInit=
O4 - HKCU\..\Run: [OneDrive] "C:\Users\juan\AppData\Local\Microsoft\OneDrive\OneDrive.exe" /background
O9 - Extra button: Fiddler - {CF819DA3-9882-4944-ADF5-6EF17ECF3C6E} - "C:\Program Files (x86)\Fiddler2\Fiddler.exe"
O9 - Extra 'Tools' menuitem: Fiddler - {CF819DA3-9882-4944-ADF5-6EF17ECF3C6E} - "C:\Program Files (x86)\Fiddler2\Fi
O11 - Options group: [ACCELERATED_GRAPHICS] Accelerated graphics
O17 - HKLM\System\CCS\Services\Tcpip\..\{6f44f5b2-64e4-4cd0-948c-572eecaca575}: NameServer = 8.8.8.8
O17 - HKLM\System\CS1\Services\Tcpip\..\{6f44f5b2-64e4-4cd0-948c-572eecaca575}: NameServer = 8.8.8.8
O18 - Protocol: tbauth - {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\SysWOW64\tbauth.dll
O18 - Protocol: windows.tbauth - {14654CA6-5711-491D-B89A-58E571679951} - C:\Windows\SysWOW64\tbauth.dll
O23 - Service: @%SystemRoot%\system32\AJRouter.dll,-2 (AJRouter) - Unknown owner - C:\WINDOWS\system32\svch
O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\WINDOWS\System32\alg.exe (file
O23 - Service: @%systemroot%\system32\appidsvc.dll,-100 (AppIDSvc) - Unknown owner - C:\WINDOWS\system32\sv
Scan & fix stuff
Scan
Fix checked
Info on selected item...
AnalyzeThis
Main Menu
Other stuff
Info...
Config...
Add checked to ignorelist