HijackThis.de Security

Direktdownload
Zur Herstellerseite

Automatische Auswertung Ihres HijackThis Logfiles

Mit Hilfe von HijackThis ist es möglich schädliche Eintragungen auf Ihrem Rechner zu finden und zu beheben.
Dazu werden spezielle Bereiche in der Registrierung und der Festplatte durchsucht und mit den Standardeinstellungen verglichen. Wird eine Abweichung festgestellt, so wird diese in einem Protokoll (Logfile) angezeigt. Um festzustellen, ob ein Eintrag schädlich ist oder bewusst vom Benutzer oder einer Software installiert worden ist benötigt man einige Hintergrundinformationen.
Ein Logfile ist oft auch für einen erfahrenen Anwender nicht so einfach auszuwerten. Mit Hilfe dieser automatischen Auswertung soll der Benutzer bei der Auswertung unterstützt werden. Kopieren Sie dazu einfach den Inhalt Ihres Logfiles in die untenstehende Textbox.
Aufgrund einiger Missverständnisse möchte ich nochmals darauf hinweisen, dass ich nur die Onlineauswertung entwickle und nicht das Tool HijackThis.

Service & Support

HijackThis.de Supportforum	Deutsch | English
Protecus Securityforum	board.protecus.de
Trojaner-Board	www.trojaner-board.com
Computerhilfen	www.computerhilfen.de

Wussten sie schon...?

..., dass die Auswertung auch MD5-Hashwerte, die mit HijackThis in das Logfile geschrieben wurden berücksichtigt?

Automatische Logfileauswertung

Kopieren Sie ein Logfile in die Textbox

oder wählen Sie ein Logfile von Ihrem Rechner aus

Datei auswählen Keine Date...usgewählt

Besucherbewertungen anzeigen

Auswerten

Helfen Sie uns diesen kostenlosen Dienst online zu erhalten! Bitte geben Sie uns eine kleine Spende über PayPal oder per Banküberweisung.

PayPal SPENDEN

Aktionen	Meldung	Art	Information
	Logfile of Trend Micro HijackThis v2.0.4		
	Platform: Windows 7 (WinNT 6.00.3504)		Ihre Version sollte aktuell sein.
	MSIE: Internet Explorer v8.00 (8.00.7600.16671)		
	Boot mode: Normal		Ihre Version sollte aktuell sein.
	C:\Program Files (x86)\Analog Devices\SoundMAX\SoundMAX.exe		
	C:\Program Files (x86)\Cloudmark\Desktop\Service\cdswin.exe		Sicher (3.63 / 5.00)
	C:\Program Files (x86)\C-CHANNEL\PayPen\PayPen.exe		Sicher (3.6 / 5.00)
	C:\Program Files (x86)\F-Secure\Common\FSM32.EXE		Sicher (4.28 / 5.00)
			Eventuell schädlich! Laut unserer Datenbank läuft dieser Prozess nomalerweise in c:\programme\f-secure.*\common\! überprüfen Sie, ob Sie die Datei kennen und führen Sie ggf. einen Virencheck durch.

ⓘ	C:\Program Files (x86)\Analog Devices\Core\smax4pnp.exe	✓	SoundMax Sound driver
ⓘ	C:\Program Files (x86)\ASUS\SmartDoctor\SmartDoctor.exe	✓	Asus SmartDoctor
ⓘ	C:\Program Files (x86)\ASUS\EPU-6 Engine\SixEngine.exe	✓	Sicher (4.33 / 5.00)
ⓘ	C:\Program Files (x86)\Microsoft Office\Office14\OUTLOOK.EXE	✓	E-Mail Client für Windows.
ⓘ	C:\Users\Lindenberg\AppData\Local\Google\Chrome\Application\chrome.exe	✓	Sicher (3.98 / 5.00)
ⓘ	C:\Users\Lindenberg\AppData\Local\Google\Chrome\Application\chrome.exe	✓	Sicher (3.98 / 5.00)
ⓘ	C:\Users\Lindenberg\AppData\Local\Google\Chrome\Application\chrome.exe	✓	Sicher (3.98 / 5.00)
ⓘ	C:\Users\Lindenberg\AppData\Local\Google\Chrome\Application\chrome.exe	✓	Sicher (3.98 / 5.00)
ⓘ	C:\Users\Lindenberg\AppData\Local\Google\Chrome\Application\chrome.exe	✓	Sicher (3.98 / 5.00)
ⓘ	C:\Users\Lindenberg\AppData\Local\Google\Chrome\Application\chrome.exe	✓	Sicher (3.98 / 5.00)
ⓘ	C:\Program Files (x86)\Mozilla Firefox\firefox.exe	✓	Internet Browser
ⓘ	C:\Users\Lindenberg\AppData\Local\Google\Chrome\Application\chrome.exe	✓	Sicher (3.98 / 5.00)
ⓘ	C:\Users\Lindenberg\AppData\Local\Google\Chrome\Application\chrome.exe	✓	Sicher (3.98 / 5.00)
ⓘ	D:\Users\Lindenberg\Downloads\HiJackThis204.exe	✓	Sicher (4.2 / 5.00)
ⓘ	R1 - HKCU\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896	✓	Diese Seite wurde als gut identifiziert!
ⓘ	R0 - HKCU\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/?LinkId=69157	✓	Diese Seite wurde als gut identifiziert!
ⓘ	R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Page_URL = http://go.microsoft.com/fwlink/?LinkId=69157	✓	Diese Seite wurde als gut identifiziert!
ⓘ	R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Default_Search_URL = http://go.microsoft.com/fwlink/?LinkId=54896	✓	Diese Seite wurde als gut identifiziert!
ⓘ	R1 - HKLM\Software\Microsoft\Internet Explorer\Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896	✓	Diese Seite wurde als gut identifiziert!
ⓘ	R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Start Page = http://go.microsoft.com/fwlink/?LinkId=69157	✓	Diese Seite wurde als gut identifiziert!
ⓘ	R0 - HKLM\Software\Microsoft\Internet Explorer\Search,SearchAssistant =	✓	
ⓘ	R0 - HKLM\Software\Microsoft\Internet Explorer\Search,CustomizeSearch =	✓	
ⓘ	R0 - HKLM\Software\Microsoft\Internet Explorer\Main,Local Page = C:\Windows\SysWOW64\blank.htm	✓	Diese Seite wurde als gut identifiziert!
ⓘ	R1 - HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings,ProxyOverride = *.local	?	Neutral (3.38 / 5.00)
ⓘ	R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName =	✓	
ⓘ	F2 - REG:system.ini: UserInit=userinit.exe	?	Neutral (3.36 / 5.00)
ⓘ	O2 - BHO: SnagIt Toolbar Loader - {00C6482D-C502-44C8-8409-FCE54AD9C208} - C:\Program Files (x86)\TechSmith\Snagit 9\SnagitBHO.dll	✓	SnagItBHO.dll - SnagIt, http://www.techsmith.com/products/snagit/default.asp
ⓘ	O2 - BHO: AcroIEHelperStub - {18DF081C-E8AD-4283-A596-FA578C2EBDC3} - C:\Program Files (x86)\Common Files\Adobe\Acrobat\ActiveX\AcroIEHelperShim.dll	✓	Sicher (4.07 / 5.00)
ⓘ	O2 - BHO: Canon Easy-WebPrint EX BHO - {3785D0AD-BFFF-47F6-BF5B-A587C162FED9} - C:\Program Files (x86)\Canon\Easy-WebPrint EX\ewpexbho.dll	?	Nicht bekanntes Programm.
ⓘ	O2 - BHO: URLRedirectionBHO - {B4F3A835-0E21-4959-BA22-42B3008E02FF} - C:\PROGRA~2\MICROS~1\Office14\URLREDIR.DLL	✓	Sicher (4.17 / 5.00)
ⓘ	O2 - BHO: LitmusBHO - {C6867EB7-8350-4856-877F-93CF8AE3DC9C} - C:\Program Files (x86)\F-Secure\NRS\iescript\baselitmus.dll	✓	Sicher (4.54 / 5.00)
ⓘ	O2 - BHO: FDMIECookiesBHO Class - {CC59E0F9-7E43-44FA-9FAA-8377850BF205} - C:\Program Files (x86)\Free Download Manager\iefdm2.dll	✓	iefdmcks.dll - Free Download Manager, http://www.freedownloadmanager.org/
ⓘ	O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files (x86)\Java\jre6\bin\jp2ssv.dll	✓	jp2ssv.dll - Sun_Java, http://java.sun.com/javase/downloads/index.jsp browser plugin
ⓘ	O3 - Toolbar: Browsing Protection Toolbar - {265EEE8E-3228-44D3-AEA5-F7FDF5860049} - C:\Program Files (x86)\F-Secure\NRS\iescript\baselitmus.dll	✓	Sicher (4.54 / 5.00)
ⓘ	O3 - Toolbar: Canon Easy-WebPrint EX - {759D9886-0C6F-4498-BAB6-4A5F47C6C72F} - C:\Program Files (x86)\Canon\Easy-WebPrint EX\ewpexhlp.dll	?	Nicht bekanntes Programm.
ⓘ	O3 - Toolbar: Snagit - {8FF5E183-ABDE-46EB-B09E-D2AAB95CABE3} - C:\Program Files (x86)\TechSmith\Snagit 9\SnagitIEAddin.dll	✓	SnagItIEAddin.dll - SnagIt, http://www.techsmith.com/products/snagit

	/default.asp
O4 - HKLM\..\Run: [F-Secure Manager] "C:\Program Files (x86)\F-Secure\Common\FSM32.EXE" /splash	F-Secure Antivirus - carry out scheduled virus scans automatically
O4 - HKLM\..\Run: [F-Secure TNB] "C:\Program Files (x86)\F-Secure\FSGUI\TNBUtil.exe" /CHECKALL /WAITFORSW	F-Secure antivirus
O4 - HKLM\..\Run: [SoundMAXPnP] C:\Program Files (x86)\Analog Devices\Core\smax4pnp.exe	SoundMax integrated sound. Required if you have custom settings for your sound, such as effects and environments
O4 - HKLM\..\Run: [BCSSync] "C:\Program Files (x86)\Microsoft Office\Office14\BCSSync.exe" /DelayServices	Sicher (4.15 / 5.00)
O4 - HKCU\..\Run: [Free Download Manager] "C:\Program Files (x86)\Free Download Manager\fdm.exe" -autorun	"Free Download Manager" See here
O4 - HKUS\S-1-5-19\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun (User 'LOKALER DIENST')	Desktop Sidebar
O4 - HKUS\S-1-5-19\..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe (User 'LOKALER DIENST')	Sicher (4 / 5.00)
O4 - HKUS\S-1-5-20\..\Run: [Sidebar] %ProgramFiles%\Windows Sidebar\Sidebar.exe /autoRun (User 'NETZWERKDIENST')	Desktop Sidebar
O4 - HKUS\S-1-5-20\..\RunOnce: [mctadmin] C:\Windows\System32\mctadmin.exe (User 'NETZWERKDIENST')	Sicher (4 / 5.00)
O4 - HKUS\S-1-5-21-454838297-1072622876-3536584524-1003\..\Run: [Google Update] "C:\Users\Lindenberg\AppData\Local\Google\Update\GoogleUpdate.exe" /c (User 'Lindenberg')	Sicher (3.5 / 5.00)
O4 - Startup: Adobe Gamma.lnk = C:\Program Files (x86)\Common Files\Adobe\Calibration\Adobe Gamma Loader.exe	Adjusts monitor colours across all programs, including Photoshop. It is needed by some graphics professionals who want their monitor calibrated. Most home users will not need it. In my case I can verify this as Photoshop loads fine
O4 - Global Startup: Cloudmark DesktopOne.lnk = C:\Program Files (x86)\Cloudmark\Desktop\Service\cdswin.exe	Sicher (3.6 / 5.00)
O4 - Global Startup: PayPen.lnk = ?	Nicht bekanntes Programm. Der Eintrag ist unnötig und kann entfernt werden!
O8 - Extra context menu item: Alles mit FDM herunterladen - file://C:\Program Files (x86)\Free Download Manager\dlall.htm	Der Eintrag Alles mit FDM herunterladen wurde als Gut erkannt.
O8 - Extra context menu item: Auswahl mit FDM herunterladen - file://C:\Program Files (x86)\Free Download Manager\dlselected.htm	Der Eintrag Auswahl mit FDM herunterladen wurde als Gut erkannt.
O8 - Extra context menu item: Datei mit FDM herunterladen - file://C:\Program Files (x86)\Free Download Manager\dllink.htm	Der Eintrag Datei mit FDM herunterladen wurde als Gut erkannt.
O8 - Extra context menu item: E&xport to Microsoft Excel - res://C:\PROGRA~2\MICROS~1\Office14\EXCEL.EXE/3000	Der Eintrag E&xport to Microsoft Excel wurde als Gut erkannt.
O8 - Extra context menu item: Nach Microsoft &Excel exportieren - res://C:\PROGRA~2\MICROS~1\OFFICE11\EXCEL.EXE/3000	Der Eintrag Nach Microsoft &Excel exportieren wurde als Gut erkannt.
O8 - Extra context menu item: Se&nd to OneNote - res://C:\PROGRA~2\MICROS~1\Office14\ONBttnIE.dll/105	Sicher (4.17 / 5.00)
O8 - Extra context menu item: Videos mit FDM herunterladen - file://C:\Program Files (x86)\Free Download Manager\dlfvideo.htm	Der Eintrag Videos mit FDM herunterladen wurde als Gut erkannt.
O9 - Extra button: An OneNote senden - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\Program Files (x86)\Microsoft Office\Office14\ONBttnIE.dll	Der Eintrag An OneNote senden wurde als Gut erkannt.
O9 - Extra 'Tools' menuitem: An OneNote s&enden - {2670000A-7350-4f3c-8081-5663EE0C6C49} - C:\Program Files (x86)\Microsoft Office\Office14\ONBttnIE.dll	Der Eintrag An OneNote s&enden wurde als Gut erkannt.
O9 - Extra button: @C:\Windows\WindowsMobile\INetRepl.dll,-222 - {2EAF5BB1-070F-11D3-9307-00C04FAE2D4F} - C:\Windows\WindowsMobile\INetRepl.dll	Der Eintrag @C:\Windows\WindowsMobile\INetRepl.dll, wurde als Gut erkannt.
O9 - Extra button: (no name) - {2EAF5BB2-070F-11D3-9307-00C04FAE2D4F} - C:\Windows\WindowsMobile\INetRepl.dll	Der Eintrag wurde als Gut erkannt.
O9 - Extra 'Tools' menuitem: @C:\Windows\WindowsMobile\INetRepl.dll,-223 - {2EAF5BB2-070F-11D3-9307-00C04FAE2D4F} - C:\Windows\WindowsMobile\INetRepl.dll	Der Eintrag @C:\Windows\WindowsMobile\INetRepl.dll, wurde als Gut erkannt.
O9 - Extra button: Verknüpfte &OneNote-Notizen - {789FE86F-6FC4-46A1-9849-EDE0DB0C95CA} - C:\Program Files (x86)\Microsoft Office\Office14\ONBttnIELinkedNotes.dll	Der Eintrag Verknüpfte &OneNote wurde als Gut erkannt.
O9 - Extra 'Tools' menuitem: Verknüpfte &OneNote-Notizen - {789FE86F-6FC4-46A1-9849-EDE0DB0C95CA} - C:\Program Files (x86)\Microsoft Office\Office14\ONBttnIELinkedNotes.dll	Der Eintrag Verknüpfte &OneNote wurde als Gut erkannt.
O9 - Extra button: Recherchieren - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~2\MICROS~1\OFFICE11\REFIEBAR.DLL	Der Eintrag Recherchieren wurde als Gut erkannt.
O18 - Filter hijack: text/xml - {807573E5-5146-11D5-A672-00B0D022E945} - C:\Program Files (x86)\Common Files\Microsoft Shared\OFFICE14\MSOXMLMF.DLL	Sicher (3.87 / 5.00)
O23 - Service: Acronis Scheduler2 Service (AcrSch2Svc) - Unknown owner - C:\Program Files (x86)\Common Files\Acronis\Schedule2\schedul2.exe	Dieser Dienst (schedul2.exe) wurde als gut identifiziert.
O23 - Service: Adobe LM Service - Adobe Systems - C:\Program Files (x86)\Common Files\Adobe Systems Shared\Service\Adobelmsvc.exe	Dieser Dienst (Adobelmsvc.exe) wurde als gut identifiziert.
O23 - Service: Adobe Active File Monitor V8 (AdobeActiveFileMonitor8.0) - Adobe Systems Incorporated - C:\Program Files (x86)\Adobe\Elements Organizer 8.0\PhotoshopElementsFileAgent.exe	Dieser Dienst (PhotoshopElementsFileAgent.exe) wurde als gut identifiziert.

O23 - Service: Andrea ADI Filters Service (AEADIFilters) - Unknown owner - C:\Windows\system32\AEADISRV.EXE (file missing)	Sicher (3.71 / 5.00)
O23 - Service: Acronis Nonstop Backup service (afcdpsrv) - Acronis - C:\Program Files (x86)\Common Files\Acronis\CDP\afcdpsrv.exe	Sicher (4.39 / 5.00)
O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\Windows\System32\alg.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (alg.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: Apple Mobile Device - Apple Inc. - C:\Program Files (x86)\Common Files\Apple\Mobile Device Support\AppleMobileDeviceService.exe	Dieser Dienst (AppleMobileDeviceService.exe) wurde als gut identifiziert.
O23 - Service: ASDR - Unknown owner - C:\Windows\SysWOW64\ASDR.exe	Sicher (3.76 / 5.00)
O23 - Service: ASUS System Control Service (AsSysCtrlService) - Unknown owner - C:\Program Files (x86)\ASUS\AsSysCtrlService\1.00.02\AsSysCtrlService.exe	Unbekannter Dienst. (AsSysCtrlService.exe)
O23 - Service: ATK Fast User Switch Service (ATKFUSService) - Unknown owner - C:\Windows\system32\ATKFUSService.exe (file missing)	Unbekannter Dienst. (ATKFUSService.exe)
O23 - Service: Dienst "Bonjour" (Bonjour Service) - Apple Inc. - C:\Program Files (x86)\Bonjour\mDNSResponder.exe	Dieser Dienst (mDNSResponder.exe) wurde als gut identifiziert.
O23 - Service: @%SystemRoot%\system32\efssvc.dll,-100 (EFS) - Unknown owner - C:\Windows\System32\lsass.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (lsass.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: FSGKHS (F-Secure Gatekeeper Handler Starter) - Unknown owner - C:\Program Files (x86)\F-Secure\Anti-Virus\fsgk32st.exe	Dieser Dienst (fsgk32st.exe) wurde als gut identifiziert.
O23 - Service: @%systemroot%\system32\fxsresm.dll,-118 (Fax) - Unknown owner - C:\Windows\system32\fxssvc.exe (file missing)	Dieser Dienst (fxssvc.exe) wurde als gut identifiziert.
O23 - Service: FLEXnet Licensing Service - Acresso Software Inc. - C:\Program Files (x86)\Common Files\Macrovision Shared\FLEXnet Publisher\FNPLicensingService.exe	Dieser Dienst (FNPLicensingService.exe) wurde als gut identifiziert.
O23 - Service: F-Secure Anti-Virus Firewall Daemon (FSDFWD) - F-Secure Corporation - C:\Program Files (x86)\F-Secure\FWES\Program\fsdfwd.exe	Dieser Dienst (fsdfwd.exe) wurde als gut identifiziert.
O23 - Service: F-Secure Management Agent (FSMA) - F-Secure Corporation - C:\Program Files (x86)\F-Secure\Common\FSMA32.EXE	Dieser Dienst (FSMA32.EXE) wurde als gut identifiziert.
O23 - Service: F-Secure ORSP Client (FSORSPClient) - F-Secure Corporation - C:\Program Files (x86)\F-Secure\ORSP Client\fsorsp.exe	Sicher (4.65 / 5.00)
O23 - Service: Google Update Service (gupdate) (gupdate) - Google Inc. - C:\Program Files (x86)\Google\Update\GoogleUpdate.exe	Sicher (3.82 / 5.00)
O23 - Service: Sentinel HASP License Manager (hasplms) - Unknown owner - C:\Windows\system32\hasplms.exe (file missing)	Unbekannter Dienst. (hasplms.exe)
O23 - Service: InstallDriver Table Manager (IDriverT) - Macrovision Corporation - C:\Program Files (x86)\Common Files\InstallShield\Driver\11\Intel 32\IDriverT.exe	Dieser Dienst (IDriverT.exe) wurde als gut identifiziert.
O23 - Service: iPod-Dienst (iPod Service) - Apple Inc. - C:\Program Files\iPod\bin\iPodService.exe	Dieser Dienst (iPodService.exe) wurde als gut identifiziert.
O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	Dieser Dienst (lsass.exe) wurde als gut identifiziert.
O23 - Service: LightScribeService Direct Disc Labeling Service (LightScribeService) - Hewlett-Packard Company - C:\Program Files (x86)\Common Files\LightScribe\LSSrvc.exe	Dieser Dienst (LSSrvc.exe) wurde als gut identifiziert.
O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner - C:\Windows\System32\msdtc.exe (file missing)	Dieser Dienst (msdtc.exe) wurde als gut identifiziert.
O23 - Service: Nero BackItUp Scheduler 4.0 - Nero AG - C:\Program Files (x86)\Common Files\Nero\Nero BackItUp 4\NBService.exe	Dieser Dienst (NBService.exe) wurde als gut identifiziert.
O23 - Service: @%SystemRoot%\System32\netlogon.dll,-102 (Netlogon) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (lsass.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: NitroPDFDriverCreatorReadSpool (NitroDriverReadSpool) - Nitro PDF Software - C:\Program Files\Common Files\Nitro PDF\Professional\6.0\NitroPDFDriverServicex64.exe	Sicher (4.31 / 5.00)
O23 - Service: NVIDIA Display Driver Service (nvsvc) - Unknown owner - C:\Windows\system32\nvvsvc.exe (file missing)	Sicher (4.85 / 5.00)
O23 - Service: O&O Defrag (OODefragAgent) - O&O Software GmbH - C:\Program Files\OO Software\Defrag\oodag.exe	Dieser Dienst (oodag.exe) wurde als gut identifiziert.
O23 - Service: @%systemroot%\system32\psbase.dll,-300 (ProtectedStorage) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (lsass.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: ProtexisLicensing - Unknown owner - C:\Windows\SysWOW64\PSIService.exe	Dieser Dienst (PSIService.exe) wurde als gut identifiziert.
O23 - Service: @%systemroot%\system32\Locator.exe,-2 (RpcLocator) - Unknown owner - C:\Windows\system32\locator.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (locator.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: @%SystemRoot%\system32\samsrv.dll,-1 (SamSs) -	Der angebliche Systemprozess läuft nicht

O23 - Service: @%SystemRoot%\system32\SamSrv.dll,-1 (SamSs) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (lsass.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: SiSoftware Deployment Agent Service (SandraAgentSrv) - SiSoftware - C:\Program Files\SiSoftware\SiSoftware Sandra Lite 2009.SP2\RpcAgentSrv.exe	Sicher (4.08 / 5.00)
O23 - Service: SBSD Security Center Service (SBSDWSCService) - Safer Networking Ltd. - C:\Program Files (x86)\Spybot - Search & Destroy\SDWinSec.exe	Sicher (4.68 / 5.00)
O23 - Service: @%SystemRoot%\system32\snmptrap.exe,-3 (SNMPTRAP) - Unknown owner - C:\Windows\System32\snmptrap.exe (file missing)	Sicher (4.25 / 5.00)
O23 - Service: @%systemroot%\system32\spoolsv.exe,-1 (Spooler) - Unknown owner - C:\Windows\System32\spoolsv.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (spoolsv.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: @%SystemRoot%\system32\sppsvc.exe,-101 (sppsvc) - Unknown owner - C:\Windows\system32\sppsvc.exe (file missing)	Sicher (4.17 / 5.00)
O23 - Service: TuneUp Utilities Service (TuneUp.UtilitiesSvc) - TuneUp Software - C:\Program Files (x86)\TuneUp Utilities 2011\TuneUpUtilitiesService64.exe	Sicher (4.48 / 5.00)
O23 - Service: @%SystemRoot%\system32\ui0detect.exe,-101 (UI0Detect) - Unknown owner - C:\Windows\system32\UI0Detect.exe (file missing)	Sicher (4.09 / 5.00)
O23 - Service: @%SystemRoot%\system32\vaultsvc.dll,-1003 (VaultSvc) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (lsass.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: @%SystemRoot%\system32\vds.exe,-100 (vds) - Unknown owner - C:\Windows\System32\vds.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (vds.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: @%systemroot%\system32\vssvc.exe,-102 (VSS) - Unknown owner - C:\Windows\system32\vssvc.exe (file missing)	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Dienst (vssvc.exe) scheint schädlich zu sein. Prozess läuft nicht im System32 Ordner!
O23 - Service: @%SystemRoot%\system32\Wat\WatUX.exe,-601 (WatAdminSvc) - Unknown owner - C:\Windows\system32\Wat\WatAdminSvc.exe (file missing)	Unbekannter Dienst. (WatAdminSvc.exe)
O23 - Service: @%systemroot%\system32\wbengine.exe,-104 (wbengine) - Unknown owner - C:\Windows\system32\wbengine.exe (file missing)	Dieser Dienst (wbengine.exe) wurde als gut identifiziert.
O23 - Service: @%Systemroot%\system32\wbem\wmiapsrv.exe,-110 (wmiApSrv) - Unknown owner - C:\Windows\system32\wbem\WmiApSrv.exe (file missing)	Dieser Dienst (WmiApSrv.exe) wurde als gut identifiziert.
O23 - Service: @%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-101 (WMPNetworkSvc) - Unknown owner - C:\Program Files (x86)\Windows Media Player\wmpnetwk.exe (file missing)	Dieser Dienst (wmpnetwk.exe) wurde als gut identifiziert.

Kurzauswertung

Die Durchführung dieser Tipps erfolgt auf eigene Verantwortung!