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.

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

..., dass schädliche Einträge oft nach einem Rechnerneustart wieder vorhanden sind, solange nicht alle Dateien, die mit dem Eintrag in Verbindung stehen, gelöscht sind?

Kopieren Sie ein Logfile in die Textbox

oder wählen Sie ein Logfile von Ihrem Rechner aus

Auswählen...

Besucherbewertungen anzeigen

Auswerten

In Ihrem Logfile findet sich kein aktiver Prozess, der auf eine aktive Firewall hindeutet. Mögliche Gründe:
(1.) Sie benutzen eine Firewall, die in Ihr Betriebssystem integriert und im Logfile nicht zu erkennen ist bzw. eine Hardware-Firewall.
(2.) Sie benutzen eine Firewall, die uns nicht bekannt ist.
(3.) Zur Zeit ist keine Firewall auf ihrem System aktiv oder
(4.) sie verwenden keine Firewall.
Wir empfehlen Ihnen das Benutzen einer Firewall. Laden Sie sich ggf. eine herunter oder verwenden Sie die Windows XP eigene. Aktivieren Sie ggf. Ihre Firewall. Wenn Sie eine uns unbekannte Firewall verwenden, melden Sie das bitte hier

Aktionen	Meldung	Art	Besucherbewertung	Information
	Logfile of Trend Micro HijackThis v2.0.4			Ihre Version sollte aktuell sein.
	Platform: Windows 7 SP3 (WinNT 6.00.3504)			
	MSIE: Internet Explorer v8.00 (8.00.7600.16700)			Ihre Version sollte aktuell sein.
	Boot mode: Normal		Sehr sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	C:\Program Files\Alienware\Command Center \AlienwareAlienFXController.exe		Sehr sicher	**Eventuell schädlich!** Laut unserer Datenbank läuft dieser Prozess nomalerweise in c:\programme \alienware\alienware alienfx\! überprüfen Sie, ob Sie die Datei kennen und führen Sie ggf. einen Virencheck durch. Alienware LED Controller
	C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology\IAStorIcon.exe		Sehr sicher	Sicher (4.07 / 5.00)
	C:\Program Files (x86)\Elaborate Bytes \VirtualCloneDrive\VCDDaemon.exe		Sehr sicher	
	C:\Program Files (x86)\avmwlanstick\WLanGUI.exe		Sehr sicher	FRITZ!WLAN
	C:\Program Files (x86)\HTC\HTC Sync 3.0\htcUPCTLoader.exe			Sicher (4.31 / 5.00)
	C:\Program Files\Logitech\GamePanel Software\Applets \LCDMedia.exe		Sicher	Part of Logitech G15
	C:\Program Files (x86)\Windows Media Player \wmplayer.exe		Sehr sicher	
	C:\Program Files\Alienware\Command Center \AlienFXHook32Mngr.exe			Sicher (4.92 / 5.00)
	C:\Program Files\Alienware\Command Center \AlienFusionController.exe		Sehr sicher	Sicher (4.92 / 5.00)
	C:\Users\Alex\Downloads\HiJackThis204.exe			Sicher (4.12 / 5.00)
	R1 - HKCU\Software\Microsoft\Internet Explorer \Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896		Sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.

R0 - HKCU\Software\Microsoft\Internet Explorer \Main,Start Page = http://www.google.de/	✓	Sehr sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
R1 - HKLM\Software\Microsoft\Internet Explorer \Main,Search Page = http://go.microsoft.com/fwlink/?LinkId=54896	✓	Sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
R0 - HKLM\Software\Microsoft\Internet Explorer \Main,Start Page = about:blank	✓	Sehr sicher	Diese Seite wurde als gut identifiziert!
R0 - HKLM\Software\Microsoft\Internet Explorer \Search,SearchAssistant =	✓	Sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
R0 - HKLM\Software\Microsoft\Internet Explorer \Search,CustomizeSearch =	✓	Sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
R0 - HKLM\Software\Microsoft\Internet Explorer \Main,Local Page = C:\Windows\SysWOW64\blank.htm	✓	Sehr sicher	Diese Seite wurde als gut identifiziert!
R1 - HKCU\Software\Microsoft\Windows\CurrentVersion \Internet Settings,ProxyOverride = fritz.box	✓	Sehr sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
R0 - HKCU\Software\Microsoft\Internet Explorer \Toolbar,LinksFolderName =	✓	Sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
R3 - URLSearchHook: (no name) - {ba14329e-9550-4989-b3f2-9732e92d17cc} - (no file)	?		Sollte gefixt werden, wenn kein (bekanntes) Programm in der Fehlermeldung steht. Sollte gefixt werden, wenn kein bekanntes (oder gar kein) Programm erwähnt wird.
F2 - REG:system.ini: UserInit=userinit.exe	✓	Sicher	Nicht bekanntes Programm. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
O2 - BHO: Java(tm) Plug-In 2 SSV Helper - {DBC80044-A445-435b-BC74-9C25C1C588A9} - C:\Program Files (x86)\Java\jre6\bin\jp2ssv.dll	✓	Neutral	jp2ssv.dll - Sun_Java, http://java.sun.com/javase/downloads/ind ex.jsp browser plugin
O3 - Toolbar: BitDefender Toolbar - {381FFDE8-2394-4f90-B10D-FC6124A40F8C} - "C:\Program Files\BitDefender\BitDefender 2010\Antispam32\IEToolbar.dll" (file missing)	✗	Sehr sicher	Unnötiger (unwirksamer) Eintrag der entfernt werden kann! IEToolbar.dll - BitDefender 2008 Toolbar, http://news.bitdefender.com/NW550-en--BitDefender-2008-Provides-Industry%E2%80%9 9s-Most-Powerful-Protection-from-Interne t-Security-Threats.html
O4 - HKLM\..\Run: [IAStorIcon] C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology \IAStorIcon.exe	✓		Sicher (4.07 / 5.00)
O4 - HKLM\..\Run: [StartCCC] "c:\Program Files (x86)\ATI Technologies\ATI.ACE\Core-Static\CLIStart.exe" MSRun	✓		ATI Core Component
O4 - HKLM\..\Run: [THX Audio Control Panel] "C:\Program Files (x86)\Creative\THX TruStudio PC \THXAudioCP\THXAudio.exe" /r	?	Sehr sicher	Nicht bekanntes Programm.
O4 - HKLM\..\Run: [UpdReg] C:\Windows\UpdReg.EXE	✓		Nicht gefährlich aber unnötig. Reminder to register Creative Labs SoundBlaster Live! cards
O4 - HKLM\..\Run: [VirtualCloneDrive] "C:\Program Files (x86)\Elaborate Bytes\VirtualCloneDrive \VCDDaemon.exe" /s	✓	Sicher	
O4 - HKLM\..\Run: [AVMWlanClient] C:\Program Files (x86)\avmwlanstick\wlangui.exe	✓	Sicher	Fritz!WLAN
O4 - HKLM\..\Run: [HTC Sync Loader] "C:\Program Files (x86)\HTC\HTC Sync 3.0\htcUPCTLoader.exe" -startup	✓		Sicher (4.31 / 5.00)
O4 - HKLM\..\RunOnce: [Launcher] C:\Program Files (x86)\AlienRespawn\Components\Scheduler \Launcher.exe	✗	Sicher	Unbedingt fixen! Spyware component related to DownloadWare and found in Program FilesKFH
O4 - HKCU\..\Run: [Sidebar] C:\Program Files\Windows Sidebar\sidebar.exe /autoRun	✓	Sicher	Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
O9 - Extra button: ICQ7.2 - {72EFBFE4-C74F-4187-AEFD-73EA3BE968D6} - C:\Program Files (x86)\ICQ7.2\ICQ.exe	✓		Sicher (4.1 / 5.00)
O9 - Extra 'Tools' menuitem: ICQ7.2 - {72EFBFE4-C74F-4187-AEFD-73EA3BE968D6} - C:\Program Files (x86)\ICQ7.2\ICQ.exe	✓		Sicher (4.1 / 5.00)
O16 - DPF: {E2883E8F-472F-4FB0-9522-AC9BF37916A7} - http://platformdl.adobe.com/NOS/getPlusPlus/1.6/gp.cab	✓	Sicher	Prüfen ob Sie diese Seite kennen und ggf. fixen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
O17 - HKLM\System\CCS\Services\Tcpip\..\{04357F1E-35B3-4C7D-815A-56247C07B511}: NameServer = 192.168.178.51,192.168.178.1	✓		Die Eingegebene IP oder Domäne **'192.168.178.51,192.168.178.1'** wurde als gut identifiziert.
O17 - HKLM\System\CS1\Services\Tcpip\..\{04357F1E-35B3-4C7D-815A-56247C07B511}: NameServer = 192.168.178.51,192.168.178.1	✓		Die Eingegebene IP oder Domäne **'192.168.178.51,192.168.178.1'** wurde als gut identifiziert.
O17 - HKLM\System\CS2\Services\Tcpip\..\{04357F1E-35B3-4C7D-815A-56247C07B511}: NameServer = 192.168.178.51,192.168.178.1	✓		Die Eingegebene IP oder Domäne **'192.168.178.51,192.168.178.1'** wurde als gut identifiziert.
O23 - Service: @%SystemRoot%\system32\Alg.exe,-112 (ALG) - Unknown owner - C:\Windows\System32\alg.exe (file missing)	✓	Sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
O23 - Service: Alienware Fusion Service (AlienFusionService) - Alienware - C:\Program Files \Alienware\Command Center\AlienFusionService.exe	✓	Sehr sicher	Sicher (4.92 / 5.00)
O23 - Service: AMD External Events Utility - Unknown owner - C:\Windows\system32\atiesrxx.exe (file missing)	✓	Sehr sicher	Unbekannter Dienst. (atiesrxx.exe) Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
O23 - Service: BitDefender Arrakis Server (Arrakis3) - BitDefender S.R.L. http://www.bitdefender.com - C:\Program Files\Common Files\BitDefender\BitDefender Arrakis Server\bin\arrakis3.exe	✓	Sehr sicher	Sicher (4.55 / 5.00)
O23 - Service: AVM WLAN Connection Service - AVM Berlin - C:\Program Files (x86)\avmwlanstick \WlanNetService.exe	✓	Sicher	Dieser Dienst (WlanNetService.exe) wurde als gut identifiziert.
O23 - Service: Broadcom Power monitoring service (BPowMon) - Broadcom Corp. - C:\Program Files \Broadcom\BPowMon\BPowMon.exe	✓		Sicher (3.59 / 5.00)

	O23 - Service: @%SystemRoot% \system32\efssvc.dll,-100 (EFS) - Unknown owner - C:\Windows\System32\lsass.exe (file missing)	✓	Sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%systemroot% \system32\fxsresm.dll,-118 (Fax) - Unknown owner - C:\Windows\system32\fxssvc.exe (file missing)	✓	Sicher	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	✓	Sehr sicher	Dieser Dienst (FNPLicensingService.exe) wurde als gut identifiziert.
	O23 - Service: Intel(R) Rapid Storage Technology (IAStorDataMgrSvc) - Intel Corporation - C:\Program Files (x86)\Intel\Intel(R) Rapid Storage Technology \IAStorDataMgrSvc.exe	✓		Sicher (4.07 / 5.00)
	O23 - Service: InstallDriver Table Manager (IDriverT) - Macrovision Corporation - C:\Program Files (x86) \Common Files\InstallShield\Driver\1150\Intel 32\IDriverT.exe	✓		Dieser Dienst (IDriverT.exe) wurde als gut identifiziert.
	O23 - Service: @keyiso.dll,-100 (KeyIso) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	✓	Sicher	Dieser Dienst (lsass.exe) wurde als gut identifiziert.
	O23 - Service: BitDefender Desktop Update Service (LIVESRV) - BitDefender S.R.L. - C:\Program Files \Common Files\BitDefender\BitDefender Update Service \livesrv.exe	✓	Sehr sicher	Dieser Dienst (livesrv.exe) wurde als gut identifiziert.
	O23 - Service: @comres.dll,-2797 (MSDTC) - Unknown owner - C:\Windows\System32\msdtc.exe (file missing)	✓	Sehr sicher	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	✓	Sicher	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)	✓	Sehr sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: Internet Pass-Through Service (PassThru Service) - Unknown owner - C:\Program Files (x86) \HTC\Internet Pass-Through\PassThruSvr.exe	?	Sehr sicher	Unbekannter Dienst. (PassThruSvr.exe)
	O23 - Service: PnkBstrA - Unknown owner - C:\Windows\system32\PnkBstrA.exe	✓	Sehr sicher	Dieser Dienst (PnkBstrA.exe) wurde als gut identifiziert. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%systemroot% \system32\psbase.dll,-300 (ProtectedStorage) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	✓	Sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%systemroot% \system32\Locator.exe,-2 (RpcLocator) - Unknown owner - C:\Windows\system32\locator.exe (file missing)	✓	Sehr sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%SystemRoot% \system32\samsrv.dll,-1 (SamSs) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	✓	Sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: SoftThinks Agent Service (SftService) - SoftThinks - C:\Program Files (x86)\AlienRespawn \sftservice.EXE	?		Unbekannter Dienst. (sftservice.EXE)
	O23 - Service: @%SystemRoot% \system32\snmptrap.exe,-3 (SNMPTRAP) - Unknown owner - C:\Windows\System32\snmptrap.exe (file missing)	✓	Sicher	Unbekannter Dienst. (snmptrap.exe) Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%systemroot% \system32\spoolsv.exe,-1 (Spooler) - Unknown owner - C:\Windows\System32\spoolsv.exe (file missing)	✓	Sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%SystemRoot% \system32\sppsvc.exe,-101 (sppsvc) - Unknown owner - C:\Windows\system32\sppsvc.exe (file missing)	✓	Sicher	Unbekannter Dienst. (sppsvc.exe) Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: Steam Client Service - Valve Corporation - C:\Program Files (x86)\Common Files\Steam \SteamService.exe	✓	Sehr sicher	Unbekannter Dienst. (SteamService.exe) Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%SystemRoot% \system32\ui0detect.exe,-101 (UI0Detect) - Unknown owner - C:\Windows\system32\UI0Detect.exe (file missing)	✓	Sicher	Unbekannter Dienst. (UI0Detect.exe) Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%SystemRoot% \system32\vaultsvc.dll,-1003 (VaultSvc) - Unknown owner - C:\Windows\system32\lsass.exe (file missing)	✓	Sehr sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%SystemRoot% \system32\vds.exe,-100 (vds) - Unknown owner - C:\Windows\System32\vds.exe (file missing)	✓	Sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%systemroot% \system32\vssvc.exe,-102 (VSS) - Unknown owner - C:\Windows\system32\vssvc.exe (file missing)	✓	Sicher	Der angebliche Systemprozess läuft nicht im System32 Ordner und ist deshalb als schädlich einzustufen. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: BitDefender Virus Shield (VSSERV) - BitDefender S.R.L. - C:\Program Files\BitDefender \BitDefender 2010\vsserv.exe	✓	Sehr sicher	Dieser Dienst (vsserv.exe) wurde als gut identifiziert.
	O23 - Service: @%systemroot% \system32\wbengine.exe,-104 (wbengine) - Unknown owner - C:\Windows\system32\wbengine.exe (file missing)	✓	Sehr sicher	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)	✓	Sehr sicher	Dieser Dienst (WmiApSrv.exe) wurde als gut identifiziert. Dieser Eintrag wurde von unseren Besuchern als gut eingestuft.
	O23 - Service: @%PROGRAMFILES%\Windows Media Player\wmpnetwk.exe,-101 (WMPNetworkSvc) -	✓	Sehr sicher	Dieser Dienst (wmpnetwk.exe) wurde als gut identifiziert.

Unknown owner - C:\Program Files (x86)\Windows Media Player\wmpnetwk.exe (file missing)

Kurzauswertung

Die Durchführung dieser Tipps erfolgt auf eigene Verantwortung!