Hijack This

Hijack This e un utile accessorio per listare tutti i processi attivi nel nostro sistema. Serve per controllare e rimuovere manualmente i programmi malware, come: dialer, dirottatori, spyware, trojan, che non si riescono a rimuovere con gli appositi programmi di sicurezza. Questo programma però e rivolto a professionisti, leggete la descrizione dove trovate tutte le indicazioni per l'uso.

In questo articolo, oltre a descrivere l'utilizzo di Hijack This per rimuovere eventuali problemi di spyware, vi descrivo anche la procedura da eseguire prima di inviare il log, tale procedura è consigliata anche come prevenzione ai problemi.

Prevenzione dei problemi

Prima di utilizzare Hijack This**, seguite questi consigli:**

1) Fate una scansione antivirus completa del vostro sistema;

2) Se la scansione antivirus rileva dei file infetti, o se comunque riscontrate dei problemi nel sistema, disattivate il Ripristino di Configurazione;

3) Riavvia il sistema in modalità provvisoria;

4) Eliminare i file inutili;

6) Fate una scansione del sistema con gli anti-spyware , se la scansione con questi programmi rintraccia dei problemi, ripetete la scansione fino a che non compaiono più problemi, casomai riavviate nuovamente in **Modalità Provvisoria** prima di fare la seconda e successive scansioni.

7) Nel caso i problemi non vengono risolti con i programmi appena indicati, utilizzate **Hijack This**, come indicato di seguito.

Per effettuare correttamente quanto detto sopra, si consiglia di utilizzare le tecniche ed i metodi già esposti nelle fasi precedenti di cui alla pagina:

Sicurezza: come avere il PC SICURO e GRATIS del sito www.istitutomajotana.it, ossia:

http://www.istitutomajorana.it/index.php?option=com_content&task=view&id=128&Itemid=64

In particolare: **Fase- 2 – Istalliamo un Buon Antivirus Gratuito**, seconda parte, *TECNICA CORRETTA PER UNA SCANSIONE EFFICACE,* di cui alla pagina:

http://www.istitutomajorana.it/index.php?option=com_content&task=view&id=152&Itemid=64

Istruzioni per l'uso di Hijack

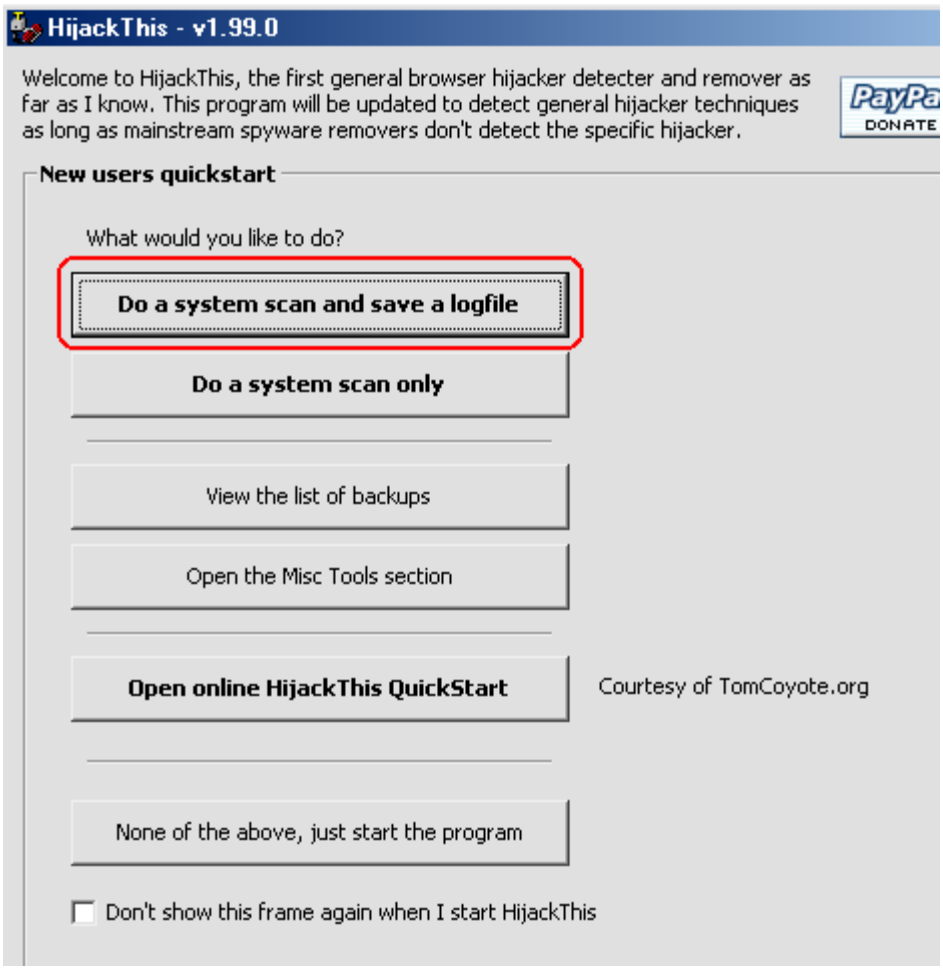
Nel caso il vostro computer presenta dei problemi con dialer, pagine internet che cambiano indirizzo da sole, o strani comportamenti dove, ne Antivirus, ne programmi anti-Spyware riescono a risolvere il problema, questo programma vi permette di controllare e rimuovere manualmente il problema.

Però l'utilizzo di questo programma é piuttosto complicato in quanto é necessario saper riconoscere processi legittimi di Windows da quelli che non lo sono. Non preoccupatevi, se non siete esperti vi aiutiamo noi, seguite scrupolosamente le indicazioni che seguono.

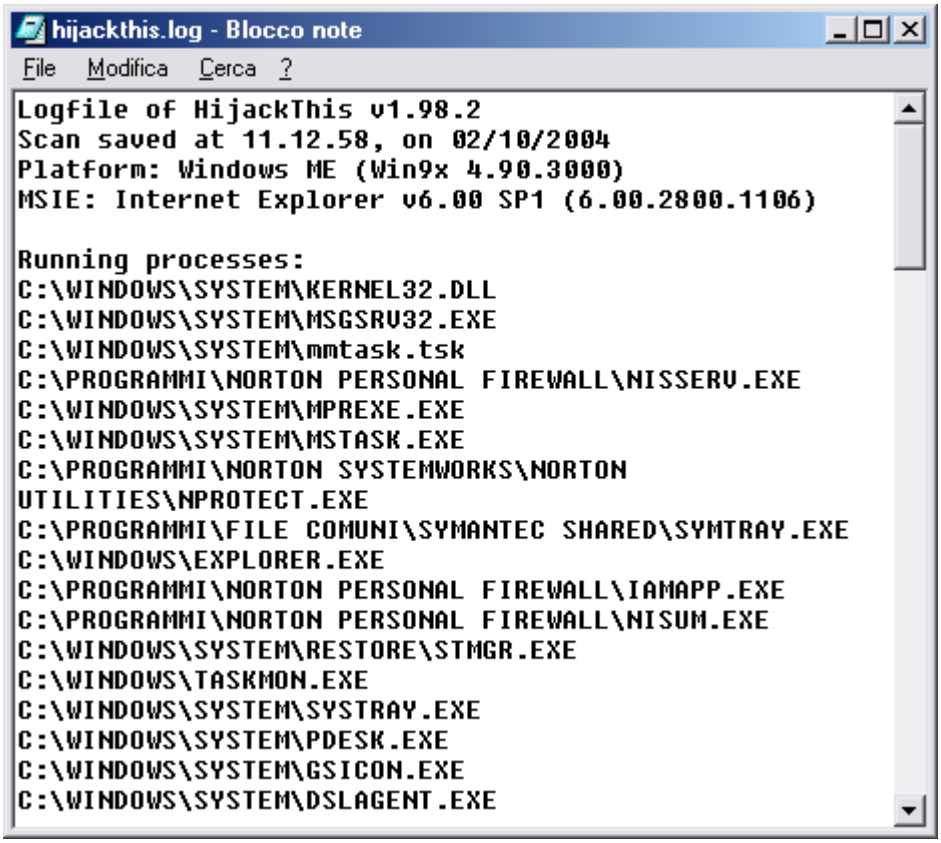
La nuova versione di Hijack This e contenuto in un archivio ZIP, una volta decompresso il programma, clicchiamo sull'eseguibile HijackThis.exe, (non richiede installazione), comparirà questa finestra, dobbiamo cliccare sul primo pulsante **Do a systemscan and save a logfile**.

Il LOG di HijackThis va eseguito in **avvio normale** e non in modalità provvisoria, altrimenti non compariranno i problemi nella lista.

HijackThis va eseguito in Modalità Provvisoria, solo per rimuovere i problemi.

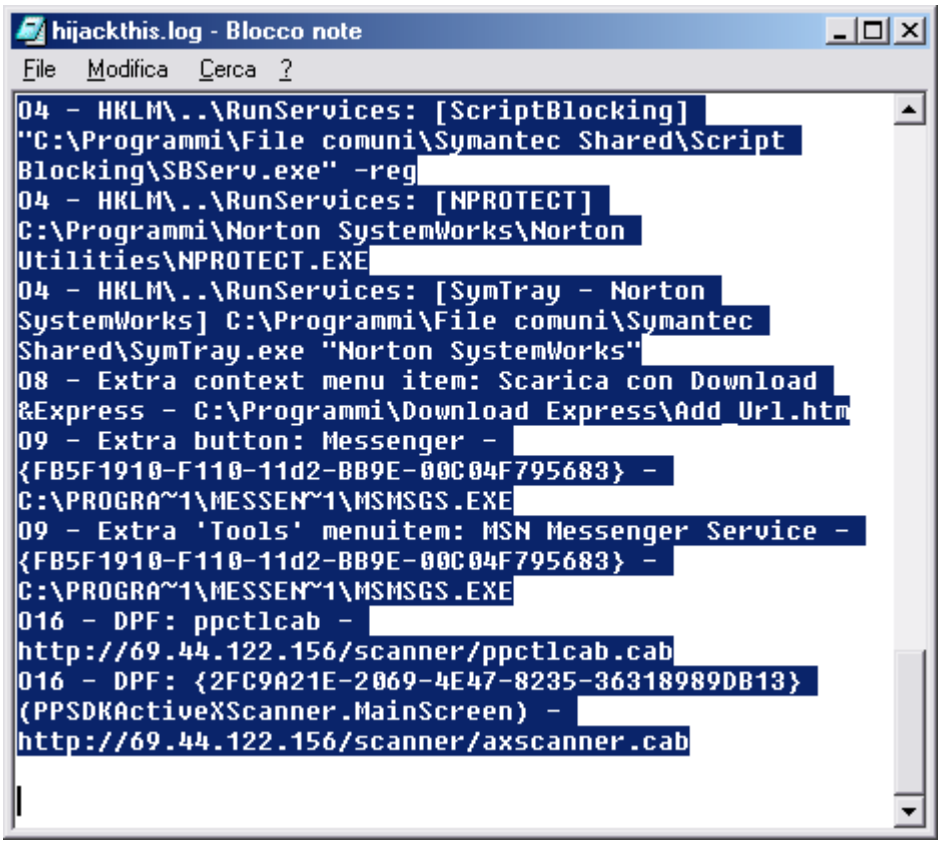


questa operazione lancerà il programma HijackThis, farà la scansione automatica e ci presenterà la lista con il Blocco Note di Windows, come vediamo qui sotto, con il codice del LOG (un elenco di cose che il programma ha trovato).



Adesso dobbiamo selezionare tutto il testo, facendo attenzione a non dimenticare ne la parte iniziale, ne quella finale.

Basterà, in blocco notes fare click su ***Modifica*** e quindi su ***Seleziona tutto***, quindi portarsi, col mouse, sopra il testo selezionato ed ancora click col destro e scegliere ***Copia*** o ***Taglia***. Tutto quanto era selezionato si trova ora negli ***Appunti di Windows*** (in pratica è memorizzato e può essere restituito con un semplice ***Incolla***).



Adesso basterà andare alla pagina:

http://hijackthis.de/index.php

ed incollare quanto avevamo precedentemente copiato.

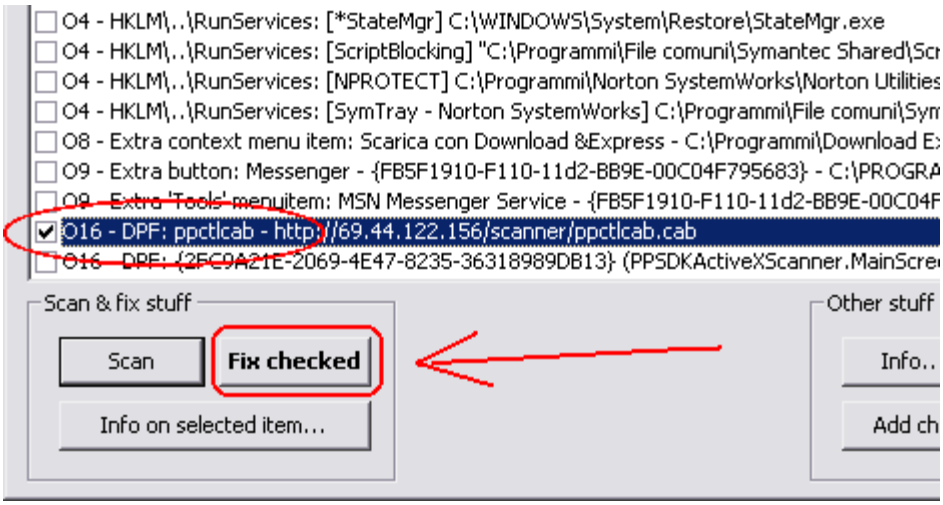
Quindi faremo click su **Analizza** ed attenderemo che la verifica abbia termine.

Terminata l'analisi la pagina, prima bloccata, potrà scorrere verso il basso facendoci vedere i risultati. Tutte le voci con la spunta verde o col simbolo di qualche programma (tipo Windows), sono sicure. Le voci col punto interrogativo giallo sono sconosciute da Hijack This e non è detto che siano "cattive". Controlliamole con attenzione perché, magari, sono dei programmo da noi istallati e sicuri. Facendo click a destra del punto interrogativo (dove ci sono 5 quadratini) si aprirà una finestra con i commenti degli utenti. In caso di dubbio sarà utilile effettuare una ricerca in internet. In caso di croce gialla (vedi figura sotto) vale quanto detto per il punto interrogativo (magari trattasi di elementi non necessari). Se, invece, la croce dovesse essere **rossa** allora siamo in presenza di elementi da eliminare.

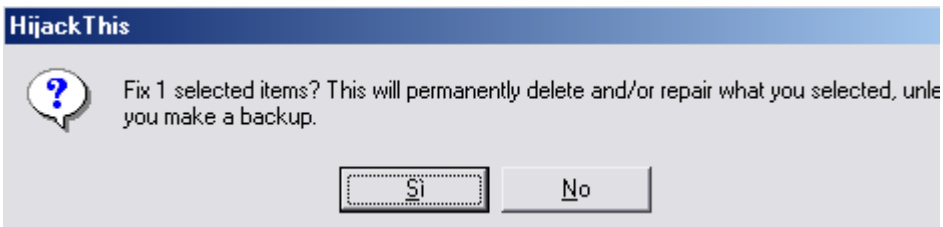
O8 - Extra context menu item: Scarica con il Wizard di LeechGet - file://C:ProgrammiLeechGet 2006\Wizard.html	✓		L'elemento Scarica con il Wizard di LeechGet è stato identificato come sicuro.
O8 - Extra context menu item: Scarica con LeechGet - file://C:ProgrammiLeechGet 2006\AddUrl.html	✓		L'elemento Scarica con LeechGet è stato identificato come sicuro.
O8 - Extra context menu item: Scarica pagina con LeechGet - file://C:ProgrammiLeechGet 2006\Parser.html	✓		L'elemento Scarica pagina con LeechGet è stato identificato come sicuro.
O9 - Extra button: (no name) - {08B0E5C0-4FCB-11CF-AAA5-00401C608501} - C:\Programmi\Java\jre1.6.0_05\bin\ssv.dll	✓		L'elemento è stato identificato come sicuro.
O9 - Extra 'Tools' menuitem: Sun Java Console - {08B0E5C0-4FCB-11CF-AAA5-00401C608501} - C:\Programmi\Java\jre1.6.0_05\bin\ssv.dll	✓		L'elemento Sun Java Console è stato identificato come sicuro.
O9 - Extra button: Ricerche - {92780B25-18CC-41C8-B9BE-3C9C571A8263} - C:\PROGRA~1\MICROS~2\OFFICE11\REFIEBAR.DLL	✓	Davvero sicuro	L'elemento Ricerche è stato identificato come sicuro.
O9 - Extra button: (no name) - SolidConverterPDF - (no file) (HKCU)	✗	Sicuro	Gli elementi non necessari (disattivati) dovrebbero essere eliminati. Questa voce è stata classificata dai nostri visitatori come sicura.
O9 - Extra button: (no name) - {31CDE000-0E77-48b8-A1F6-B2101670A16E} - C:\Programmi\BrowserTweaks\IEScreenshotPro\iescreenshotpro.dll (HKCU)	?		Da eliminare se non conoscete l'oggetto ''. Pulsanti sconosciuti o gli elementi nel menù 'Extras' dovrebbero essere eliminati.
O9 - Extra 'Tools' menuitem: Make Advanced Screenshot - {31CDE000-0E77-48b8-A1F6-B2101670A16E} - C:\Programmi\BrowserTweaks\IEScreenshotPro\iescreenshotpro.dll (HKCU)	?		Da eliminare se non conoscete l'oggetto **'Make Advanced Screenshot '**. Pulsanti sconosciuti o gli elementi nel menù 'Extras' dovrebbero essere eliminati.
O9 - Extra button: IE Screenshot Pro - {75D74791-9D1E-4baf-B4BD-C91976BEBEF6} - C:\Programmi\BrowserTweaks\IEScreenshotPro\iescreenshotpro.dll (HKCU)	?		Da eliminare se non conoscete l'oggetto **'IE Screenshot Pro '**. Pulsanti sconosciuti o gli elementi nel menù 'Extras' dovrebbero essere eliminati.
O9 - Extra button: NeoTrace It! - {9885224C-1217-4c5f-83C2-00002E6CEF2B} - C:\PROGRA~1\NEOTRA~1\NTXtoolbar.htm (HKCU)	✓	Davvero sicuro	L'elemento NeoTrace It! è stato identificato come sicuro.
O9 - Extra button: easyWebSave - {ECC5777A-6E88-BFCE-13CE-81F134789E7B} - C:\Programmi\easyWebSave\bin\ezsvcfg.exe (HKCU)	✓		L'elemento easyWebSave è stato identificato come sicuro.
O9 - Extra 'Tools' menuitem: easyWebSave - {ECC5777A-6E88-BFCE-13CE-81F134789E7B} - C:\Programmi\easyWebSave\bin\ezsvcfg.exe (HKCU)	✓		L'elemento easyWebSave è stato identificato come sicuro.
O16 - DPF: {7F8B2500-3B5D-474C-B828-C766ECE3AB3C} (ATLmosquito1 Class) - http://voceviva-vip.tiscali.it/netphone/ocx/mosquito.cab	✓	Sicuro	Controllate se conoscete il sito web altrimenti eliminatelo (Fix). Questa voce è stata

Leggi, con molta attenzione, tutti gli elementi da eliminare.

Con altrettanta attenzione vai al programma (che hai lasciato aperto, magari ridotto ad icona) ed inserisci il segno di spunta nel quadratino davanti alla riga indicata (vedi immagine sotto), fai molta attenzione che la riga indicata sia identica a quella che compare nella pagina internet di HijackThis, alcune righe possono sembrare uguali, leggi attentamente tutti i caratteri, altrimenti elimini qualcosa che non devi.



Bisogna che selezionate tutte le caselle degli elementi da eliminare, non una per volta, perché dopo si chiude la maschera e se avete dimenticato di selezionarne qualcuna dovrete ricominciare da capo. Una volta selezionata la casella o le caselle, se sono più di una, cliccate il tasto **Fix checked** per procedere all'eliminazione, comparirà la finestra qui sotto, cliccate su **SI** per accettare e l'operazione e conclusa.



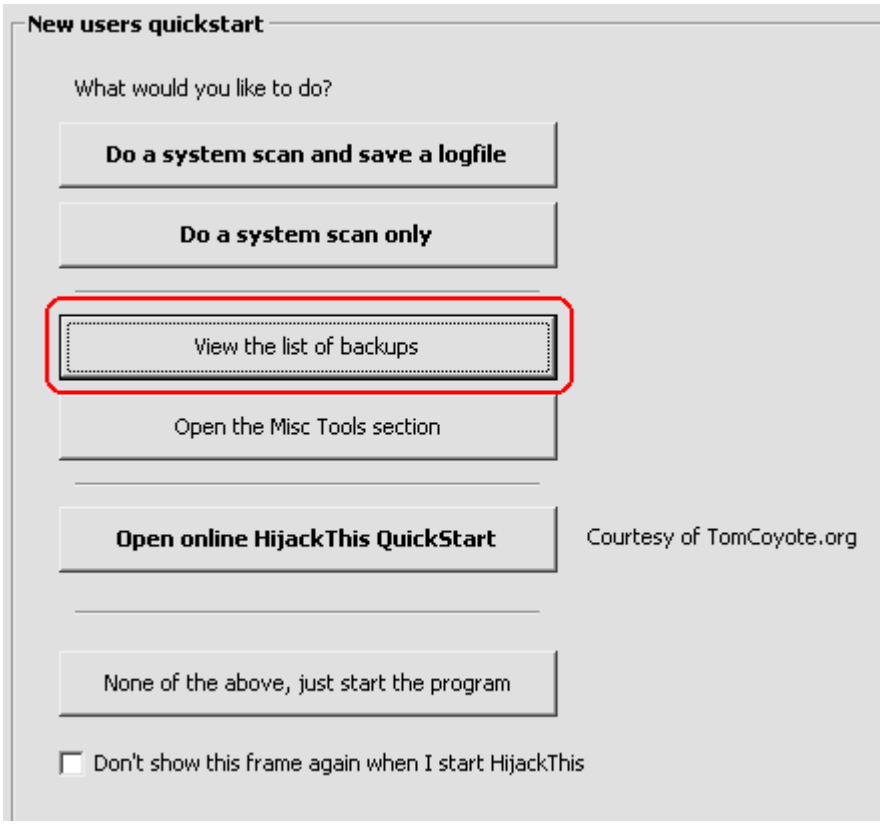
Le righe eliminate dal LOG verranno inserite in una cartella dal nome **backups** e si troverà nello stesso percorso dove si trova il programma HijackThis, volendo possono essere recuperate se cancellate per errore. Gli effetti del backup si otterranno dopo il riavvio del computer.

Chiudiamo Hijack e riavviamo il computer in modalità normale.

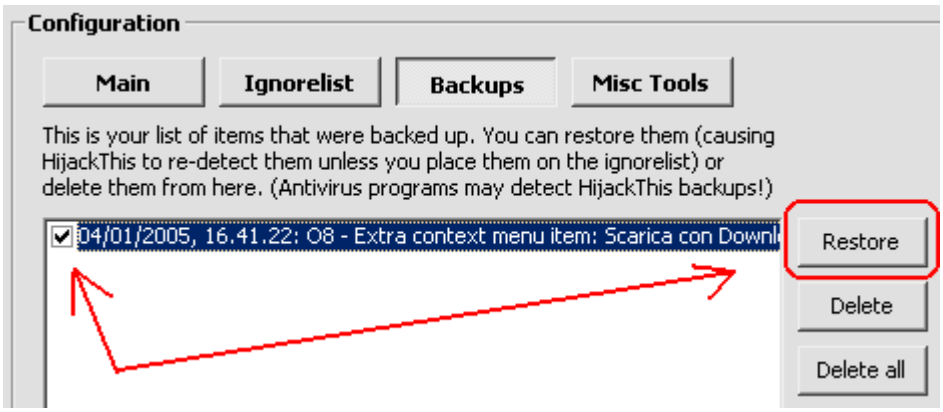
Recupero Backups

Nel caso abbiamo eliminato qualche riga per errore o se il sistema presenta problemi, possiamo ripristinare le righe di codice eliminate in precedenza, basta solo non aver cancellato la cartella backups.

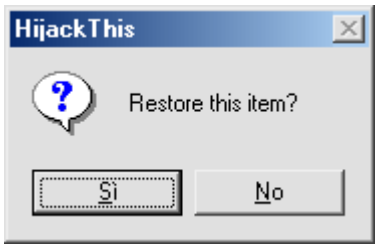
Per ripristinare il backup aprite il programma HijackThis e cliccate sul terzo pulsante **View the list of backups**



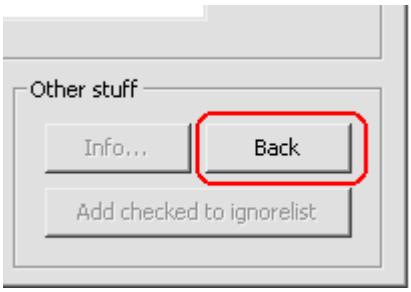
Comparirà la finestra qui sotto con elencate tutte le righe eliminate, spuntate prima la casellina delle righe che volete ripristinare e quindi cliccate il pulsante **Restore**



vi si chiederà una conserma, cliccate su **SI**



a questo punto la riga e stata reinserita nel log, possiamo uscire cliccando sulla X in alto della finestra o cliccare su **Back** per tornare alla finestra di scansione e quindi cliccare su **Scan** per controllare se tale riga e stata ripristinata, per finire **riavviamo il computer** in modo che i cambiamenti siano letti dal sistema.



Servizi* *di controllo LOG

se siete esperti potete controllare il vostro log a questo indirizzo **http://www.hijackthis.de/index.php** ma fate molta attenzione, alcune volte vengono segnalati programmi che sono legittimi di windows e rimuovendoli potreste avere dei problemi, se non siete esperti fatevi aiutare dal forum di Aiutamici.com.

Questo servizio risulta comodo per un controllo periodico dove non si presentano problemi ma si vuole essere certi che il sistema sia pulito.