CSBNO – SUPPORTO TECNICO
NOTA TECNICA

Numero:	018
Oggetto:	Procedura rimozione virus e spyware
Data:	17 gennaio 2007
Validità:	indefinita
Rif. a N.T. precedenti	
Autore:	Mistrali claudio

La seguente è una guida pensata per tentare la pulizia e rimozione di virus e altri programmi dannosi da pc che risultano infetti.
La procedura è composta da 5 passi per la manutenzione e pulizia periodica (consigliamo di eseguirli almeno una volta al mese) e 2 passi aggiuntivi per situazioni più gravi o nel caso in cui le prime operazioni non abbiamo dato i risultati sperati.
Tutte le operazioni qui descritte sono spiegate in modo semplice ed accompagnate da figure esplicative. E' sufficiente seguire passo passo quanto scritto di seguito per eventualmente risolvere in totale autonomia e con facilità situazioni apparentemente gravi senza dover necessariamente spedire il computer in assistenza con notevole risparmio di tempo.
E' tuttavia necessario avere un **minimo** di dimestichezza con l'utilizzo del personal computer per effettuare le seguenti operazioni

NOTA1: E' necessario effettuare le seguente operazioni, in particolare l'installazione dei software qui descritti, da Administrator.
NOTA2: E' consigliabile, se possibile, effettuare un backup dei dati personali su cd o chiavetta prima di effettuare le operazioni qui descritte per quanto siano tutte operazioni a basso rischio.

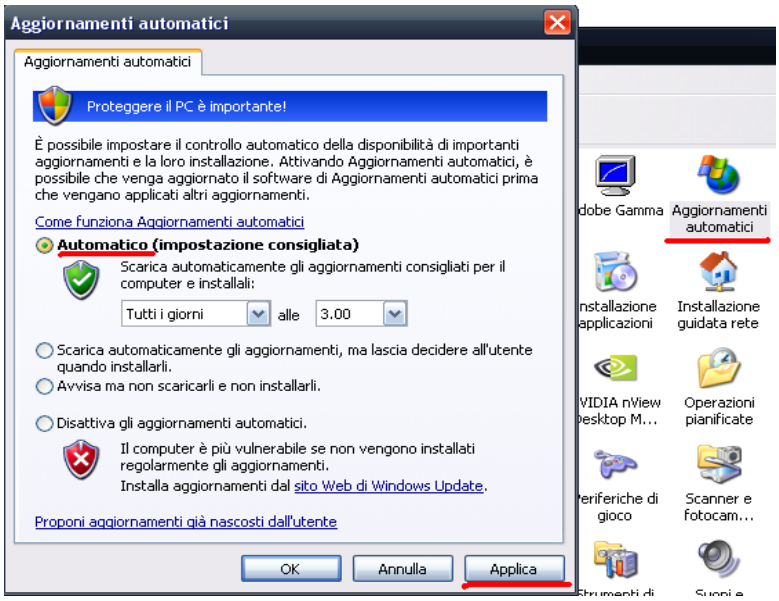
I SINTOMI CHE SI POSSONO RISCONTRARE SU UN PERSONAL COMPUTER INFETTATO DA VIRUS, SPYWARE O QUANT'ALTRO SONO I SEGUENTI:

- Rallentamenti improvvisi del PC e comportamenti fuori dalla norma
- Utilizzo anomalo della CPU o delle risorse di sistema in generale
- Impossibilità di accedere ad alcuni siti e/o avviare programmi soprattutto inerenti la sicurezza
- Pagina iniziale di Internet explorer modificata e impossibile da ripristinare
- Messaggi pubblicitari/immagini pornografiche o di errore all' apertura di programmi o nella navigazione in internet etc

Tutti i software trattati sono specifici per la risoluzione di questo tipo di situazioni e possono essere scaricati direttamente dai link presenti in questa guida.
Di seguito, per ogni programma trattato, troverete il corrispondente link da dove prelevare il file e installarlo sul personal computer . E' sufficiente posizionare il mouse sulla dicitura **QUI** **e cliccare per scaricare il file.**

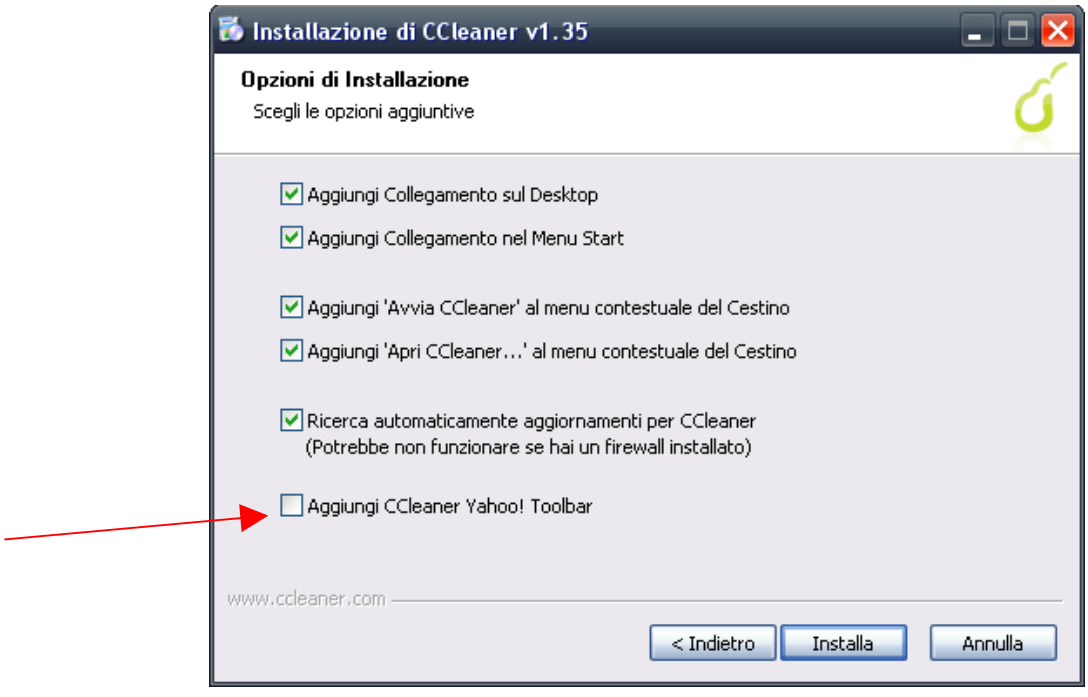
Prima di INIZIARE LA PROCEDURA ASSICURARSI CHE IL PC IN QUESTIONE ABBIA GLI AGGIORNAMENTI AUTOMATICI ATTIVATI:

Andiamo su START-PANNELLO DI CONTROLLO-AGGIORNAMENTI AUTOMATICI E CONTROLLARE CHE SIA SPUNTATA LA VOCE AUTOMATICO.



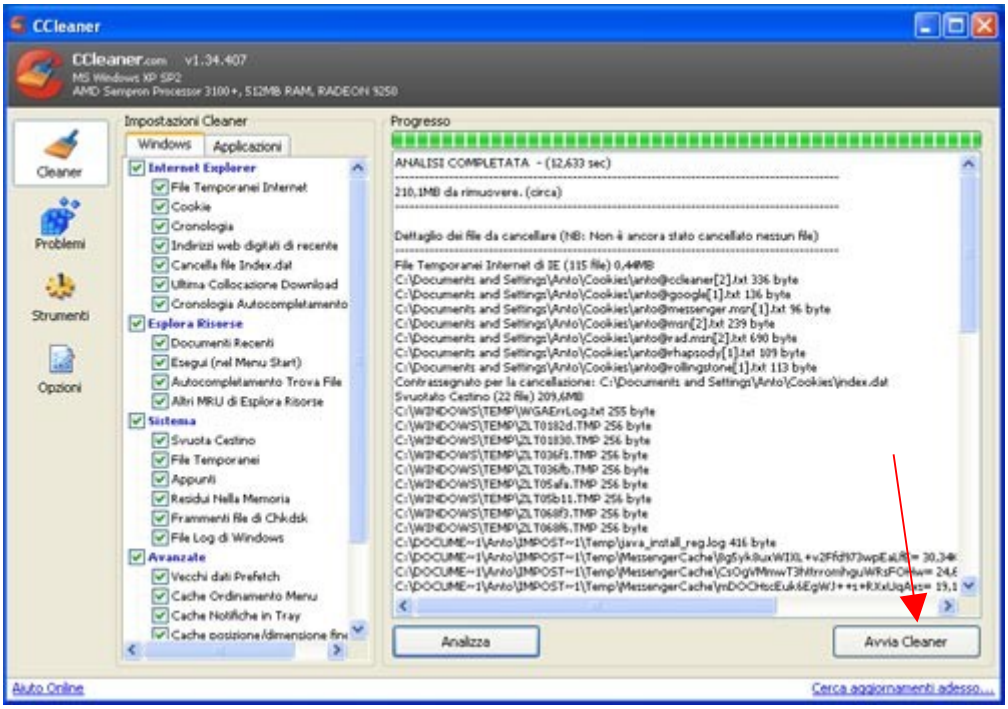
PROCEDURA DA SEGUIRE PER TENTARE LA PULIZIA E RIMOZIONE DI EVENTUALI PROGRAMMI MALEVOLI:

1 PASSO: **INSTALLARE CCLEANER** un tool di rimozione e pulizia di tutti i file temporanei, cookie etc . Una volta scaricato il file ccleaner.exe da **QUI** avviare l'installazione selezionando sempre la voce "avanti" fino alla maschera sottostante dove **VA DESELEZIONATA LA VOCE AGGIUNGI YAHOO TOOLBAR**!



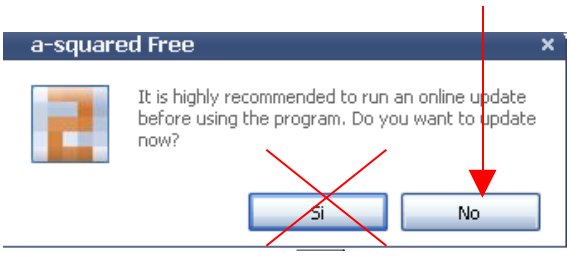
Una volta terminata l'installazione, avviare il programma cliccando sull'icona CCleaner che troverete sul Desktop o sotto START-PROGRAMMI- .

Selezionare "**Analizza**" e lasciare che scansioni il sistema alla ricerca dei file da eliminare.
Terminata la scansione cliccare su "**avvia cleaner**" come da figura!

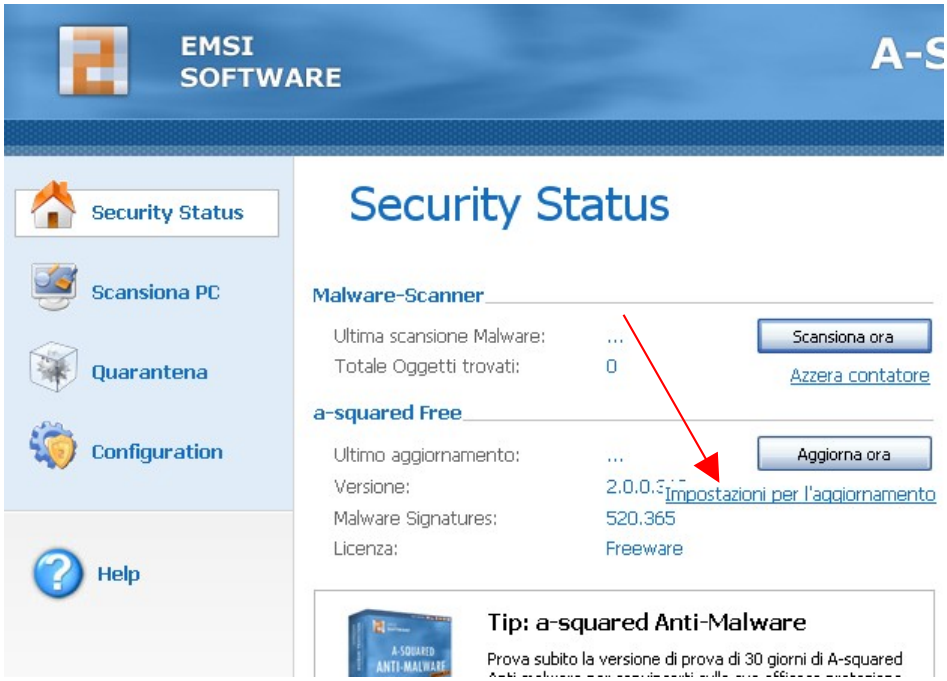


LA STESSA OPERAZIONE VA RIPETUTA ACCEDENDO CON IL PROFILO UTENTE CHE SI UTILIZZA NORMALMENTE PER LAVORARE (staff,utente,internet...etc).

2 PASSO: **INSTALLARE ASQUARED** il secondo tool per la rimozione di spyware/trojan/virus, scaricando il file da **QUI** . L'installazione è molto semplice è sufficiente selezionare sempre avanti, accettare il contratto e infine la voce "installa".
Una volta installato il software ci viene richiesto se vogliamo scaricare subito gli aggiornamenti **SELEZIONARE NO**! (vedi figura sottostante)



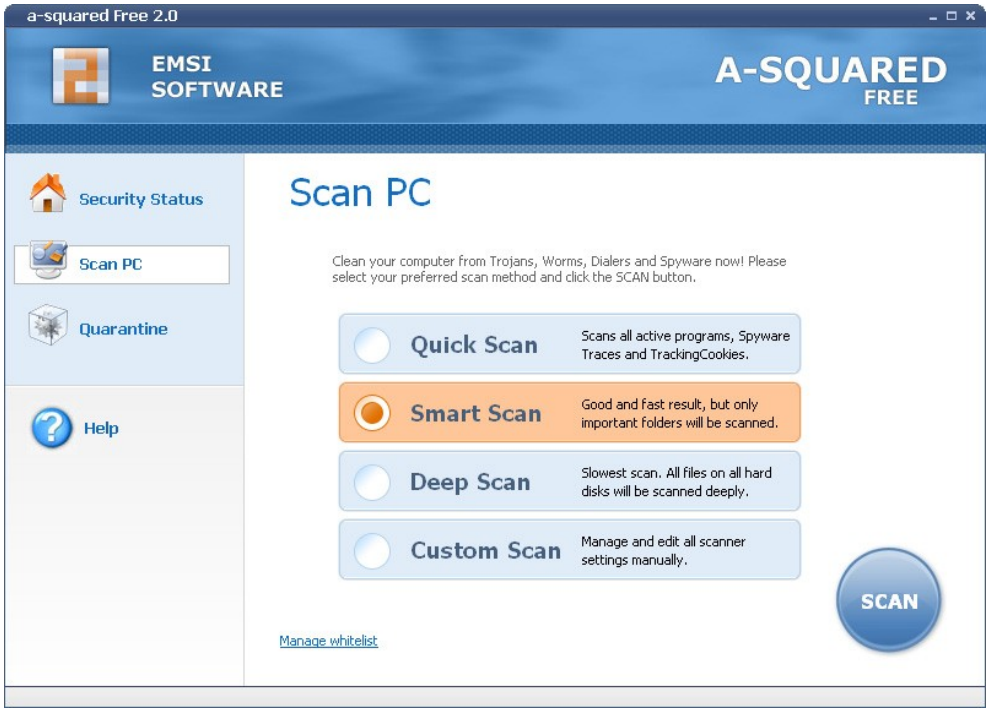
Cliccare su Security status e selezionare "**Impostazioni per l'aggiornamento**" come da figura:



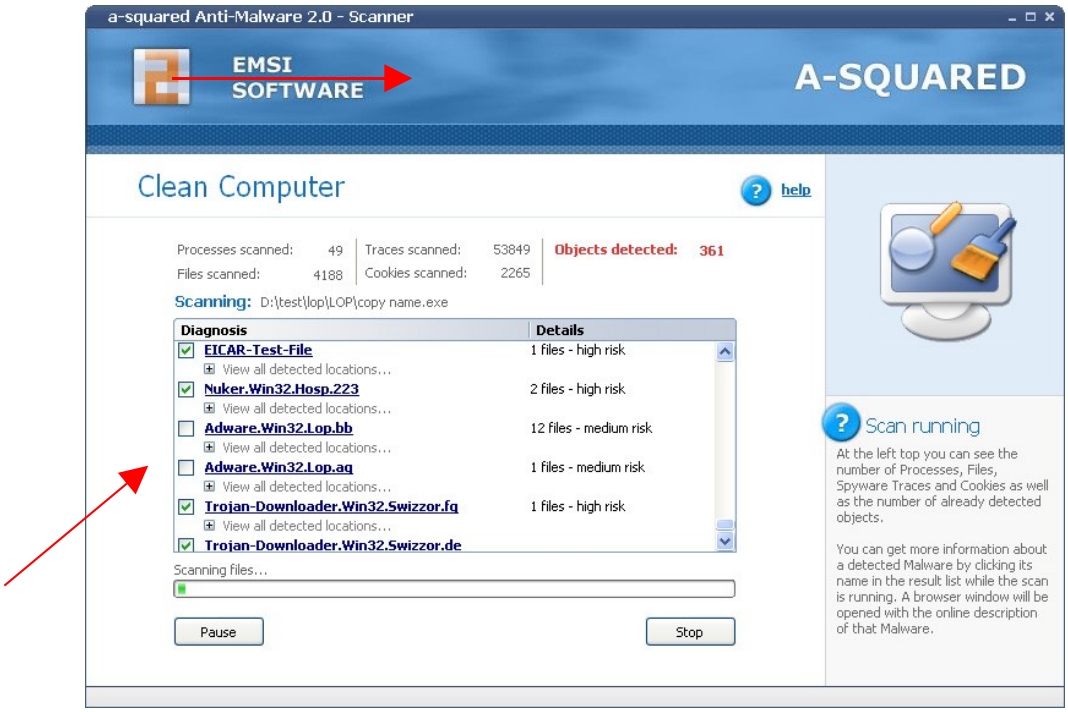
A questo punto selezioniamo "impostazioni di connessione" e mettendo la spunta su utilizza proxy inseriamo l'indirizzo del proxy e la porta 3128 come da figura:

NOTA BENE: L'INDIRIZZO DEL PROXY CAMBIA DA BIBLIOTECA A BIBLIOTECA!!
SE NON LO CONOSCETE è POSSIBILE RECUPERARLO DA INTERNET EXPLORER SEGUENDO IL PERCORSO : STRUMENTI-OPZIONI INTERNET-CONNESSIONE-IMPOSTAZIONI LAN-
L'INDIRIZZO DEL PROXY è SCRITTO NELLA PARTE INFERIORE DELLA MASCHERA.

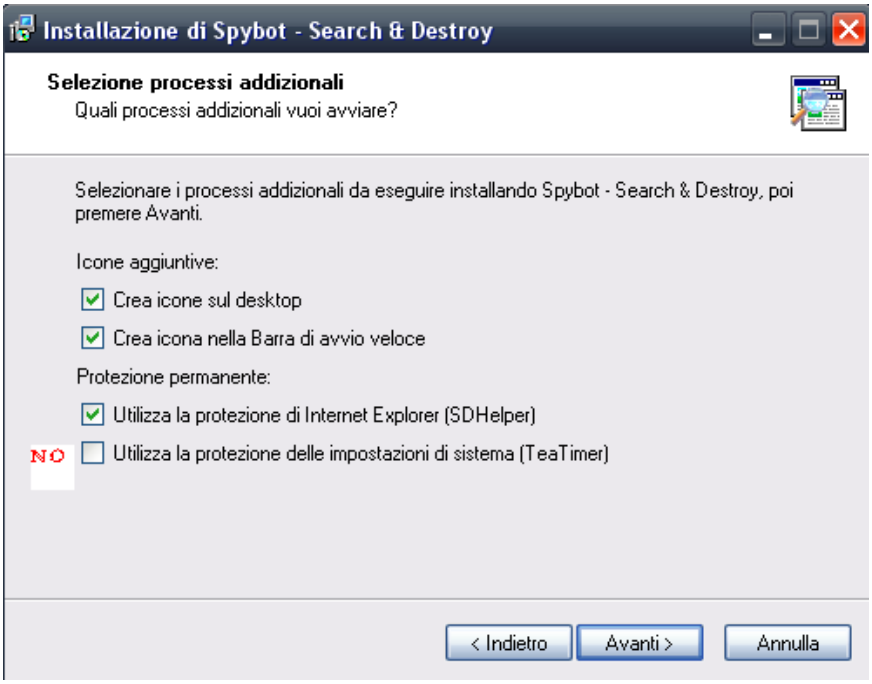
Diamo ok e torniamo alla pagina iniziale riselezionando Security status.
Clicchiamo ora la voce "aggiorna ora" e attendiamo che si scarichino gli aggiornamenti.
Terminato l'aggiornamento il programma ci chiede se vogliamo riavviarlo per rendere effettivi gli aggiornamenti. Diamo di si, A squared dovrebbe chiudersi e riaprirsi da solo dopo qualche secondo.
A questo punto posizionarsi su SCAN PC selezionare DEEP SCAN (per una scansione più profonda) e cliccare su SCAN (ATTENDERE CHE COMPLETI LA SCANSIONE)



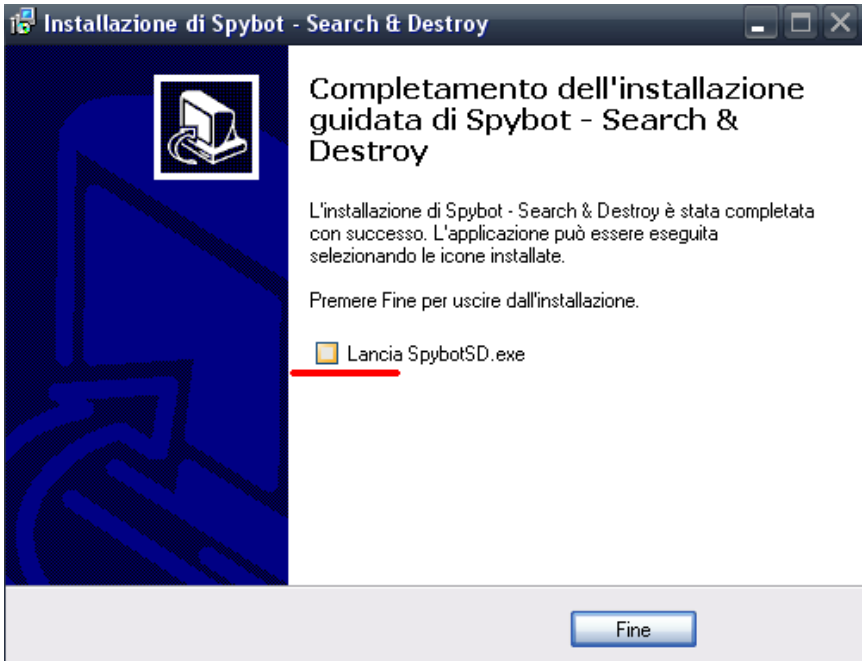
Terminata la scansione spuntare tutte le voci trovate e cliccare su ELIMINA OGGETTI SELEZIONATI



3 PASSO: INSTALLARE **SPYBOT** tool per la rimozione di spyware da **QUI**
L'installazione è del tutto simile a quella dei programmi fin qui esaminati , è sufficiente lasciare selezionate le opzioni di default e controllare che giunti al passo qui sotto siano selezionate tutte le opzioni tranne l'ultima, esattamente come da figura:



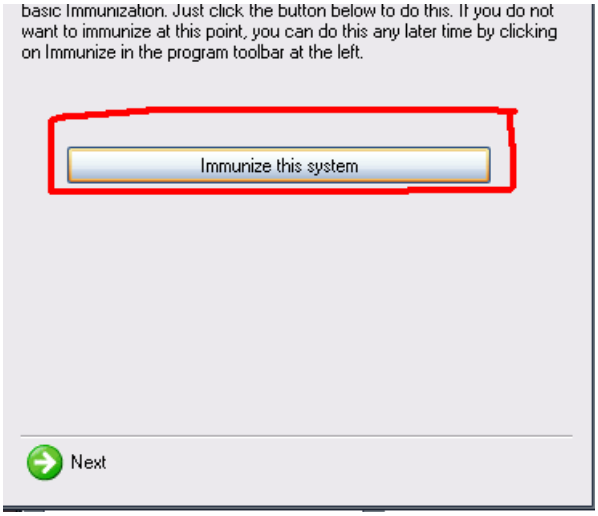
Prima di terminare LEVARE LA SPUNTA DALLA VOCE LANCIA SPYBOT ADESSO:



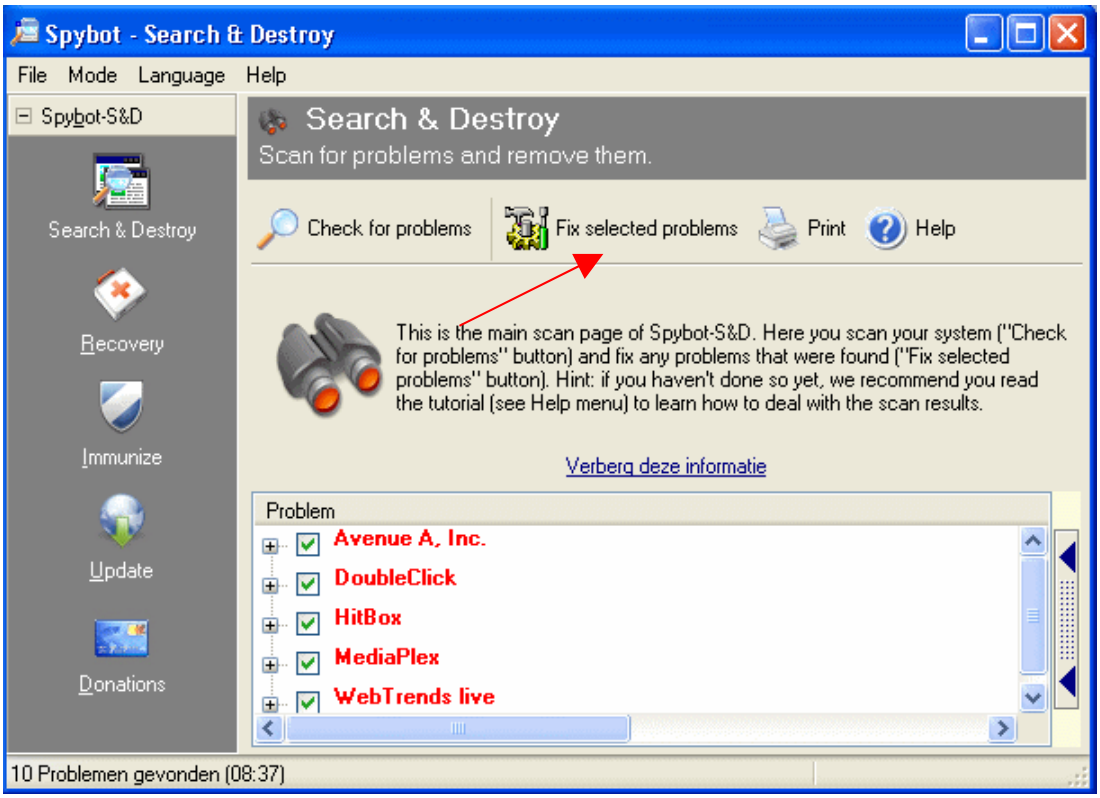
PRIMA DI AVVIARE SPYBOT E' INFATTI NECESSARIO SCARICARE IL PACCHETTO DEGLI AGGIORNAMENTI spybot-AGGIORNA.exe da QUI .. ED INSTALLARLO.

TERMINATA L'INSTALLAZIONE avviare spybot ed ignorare i primi due passi della procedura iniziale selezionando "NEXT" come da figura:

Fino a quando non ci chiede se vogliamo IMMUNIZZARE IL SISTEMA a questo punto clicchiamo sulla voce corrispondente per dare la nostra conferma:



Finalmente è possibile avviare una scansione selezionando "Check for problems o in caso sia in italiano "Controlla ora"

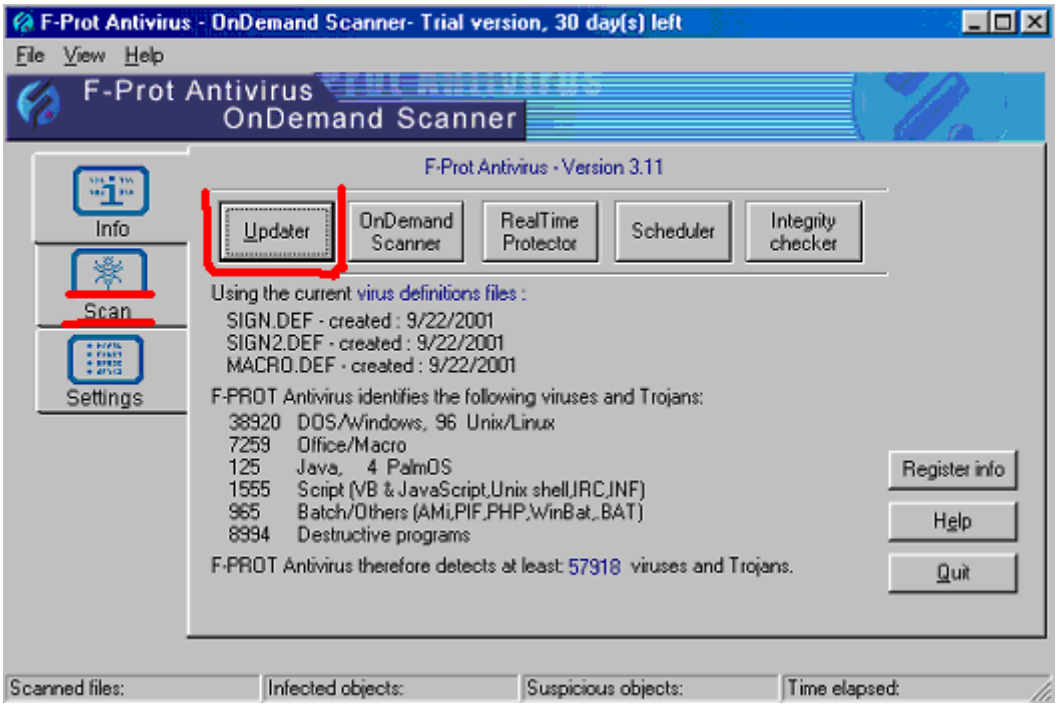


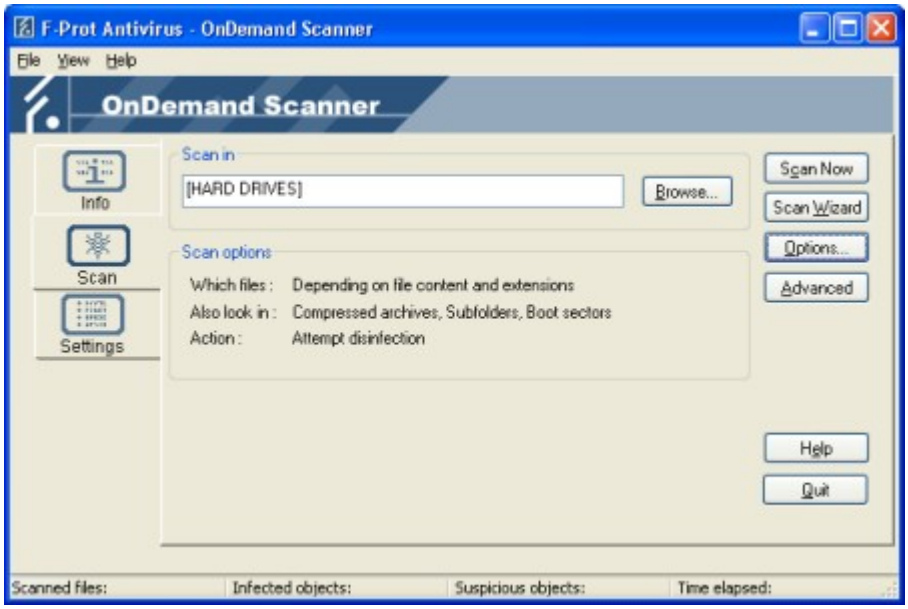
Terminata la scansione SELEZIONARE/SPUNTARE TUTTE LE VOCI RILEVATE E cliccare su FIX Selected problems

5 PASSO: Il quinto ed ultimo passo consiste nel effettuare una scansione completa del pc con **FPROT ANTIVIRUS** (che comunque viene effettuata in automatico settimanalmente)
Andare su START-PROGRAMMI-FPROT ANTIVIRUS – e cliccare su **ON DEMAND SCANNER**

Selezionare "updater" e controllare nella voce "Setting" che sia specificato l'indirizzo corretto del vostro proxy ed eventualmente cliccare sulla voce "UPDATE" per scaricare gli ultimi aggiornamenti.

Dopodiché Cliccare su SCAN, assicurarsi che sia selezionato HARD DRIVE E cliccare infine su **SCAN NOW**



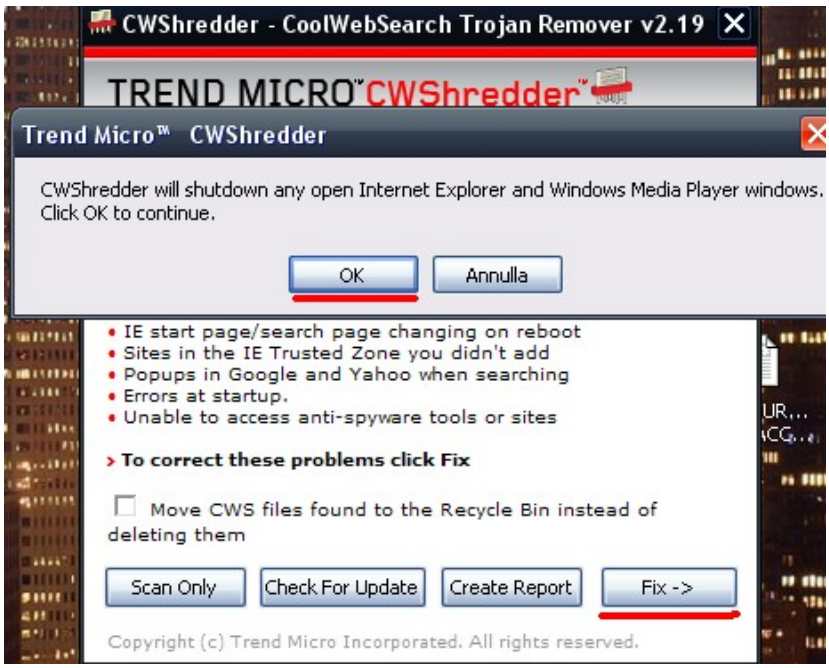


Attendere che finisca la scansione che potrebbe durare anche un ora o più. FProt elimina automaticamente i virus rilevati.

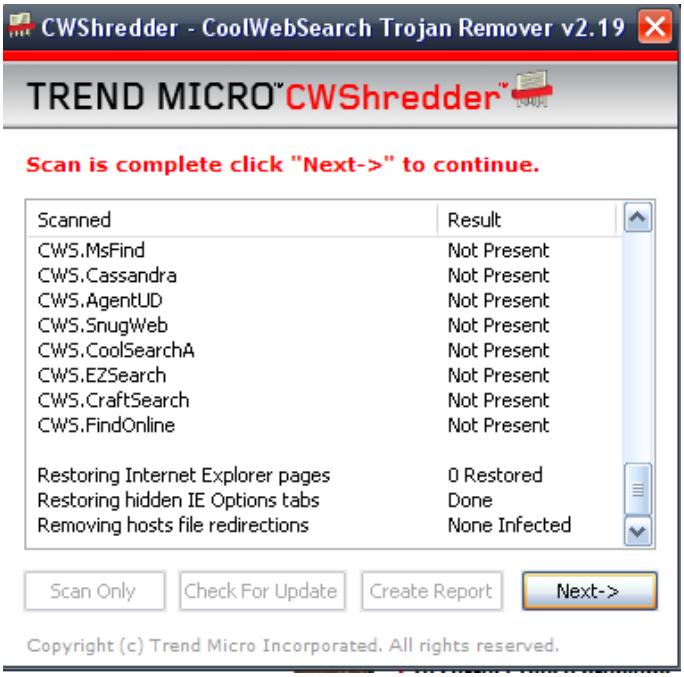
OPERAZIONI AGGIUNTIVE PER SITUAZIONI PIU' GRAVI:

Nel caso in cui le operazioni seguite finora non siano sufficienti e risulti chiaro che il computer è ancora affetto da virus , presenta ancora problematiche gravi come l'impossibilità di installare delle applicazioni anche con diritti di amministratore o pagine iniziali di internet explorer modificate e impossibili da eliminare , seguire i due passi aggiuntivi:

6 PASSO: SCARICARE **CWSHREDDER** da **QUI**
Il tool in questione non ha nessuna procedura di installazione è sufficiente avviare il file scaricato e ciccare su FIX come da figura:



Chiudiamo eventuali pagine di internet explorer o di Media Player e diamo OK.
Cwshredder ricerca ED ELIMINA una serie di programmi malevoli che modificano la pagina iniziale di internet explorer , causano errori all'avvio del pc , aprono pop up pubblicitari durante la navigazione.



clicchiamo infine su NEXT E POI EXIT.

7 PASSO:scaricare ed installare il file **SARSFX**.exe da **QUI**
Avviare il file scaricato e seguire la procedura di installazione.
Aprire la directory C:\SOPHTEMP e avviare il file sargui.exe come da figura:

Cliccare su START SCAN.
Attendere che termini la scansione e nel caso rilevi degli oggetti spuntarli tutti ed eliminarli.

Consigliamo infine caldamente l'utilizzo di MOZILLA FIREFOX come browser per la navigazione a posto di Internet Explorer essendo quest'ultimo molto più soggetto ad intrusioni dannose di vario tipo.

L'utilizzo di MOZILLA rappresenta già un ottimo passo in avanti per quanto riguarda la sicurezza e la protezione del computer.

L'ultima versione di Mozilla firefox è scaricabile da QUI

Grazie.