

Progetto Sicurezza su Reti

Corso Sicurezza su Reti anno 2003/04 Prof. Alfredo De Santis

Spychecker e Xp-AntiSpy



Alfredo Di Marco
Danilo Sabato

Sommario

- [Introduzione](#)
- [Un esempio di spionaggio](#)
- [Le origini dello Spyware](#)
- [Lo Spyware](#)
- [Spychecker](#)
- [Xp-AntiSpy](#)



Sommario

- **Introduzione** ←
- Un esempio di spionaggio
- Le origini dello Spyware
- Lo Spyware
- Spychecker
- Xp-AntiSpy



Introduzione

- Gli Spyware raccolgono informazioni sull'utente a sua insaputa e le inviano a delle società
- Tali spyware entrano nei PC solitamente mediante programmi gratuiti
- Un esempio sono i programmi di programmi spyware: Kazaa e IMesh, Gozilla e il Codec Divx 5 Pro Real Player

Introduzione

- Il nostro scopo è fornire una conoscenza di base degli spyware e dei pericoli che comportano
- Spychecker e Xp-AntiSpy aiutano l'utente a prevenire e proteggersi da questo fenomeno



Sommario

- Introduzione
- **Un esempio di spionaggio** ←
- Le origini dello Spyware
- Lo Spyware
- Spychecker
- Xp-AntiSpy



Un esempio di spionaggio

- Le origini della raccolta delle informazioni sono radicate nella storia
- La conoscenza di informazioni riservate è sempre stato un obiettivo prioritario in campo:
 - Bellico
 - Antiterroristico
 - Economico-industriale
 - ecc.
- Echelon è sicuramente tra i più eclatanti

Un esempio di spionaggio

Echelon è una rete di monitoraggio globale che gli Stati Uniti gestiscono insieme a:

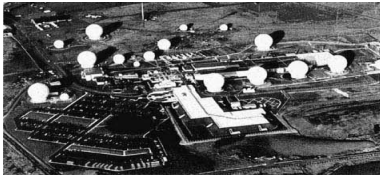
- Gran Bretagna
- Canada
- Australia
- Nuova Zelanda

- Secondo un rapporto del Security Technological Option Assessment (STOA), ogni telefonata, fax, email, può essere intercettato e inserito in un data base comune



Un esempio di spionaggio

- In Europa:
 - Le telefonate
 - I fax
 - Le emailsono regolarmente intercettati dal centro inglese di Menwith Hill e trasferite alla National Security Agency (NSA)



(Menwith Hill)

Sommario

- Introduzione
- Un esempio di spionaggio
- Le origini dello Spyware ←
- Lo Spyware
- Spychecker
- Xp-AntiSpy



Le origini dello Spyware

- Lo spyware nasce, molto probabilmente, dal fallimento dell'idea legata ai programmi shareware
- Un programma shareware è gratuito per un determinato periodo di prova, scaduto il quale necessita l'acquisto di una licenza d'uso
- Si riescono a reperire sulla rete applicazioni illegali (i Crack) che permettono un utilizzo completo del software, evitando l'acquisto della licenza

Le origini dello Spyware

- Tramite l'inserimento dei banner pubblicitari è possibile diffondere il programma gratuitamente
- La maggior parte dei programmi che utilizzano banner pubblicitari si affidano al tool della Aureate (ora diventata Radiate)
- Questo tool permette di visualizzare banner pubblicitari sempre diversi. Il programmatore percepisce un compenso dalla Radiate sulla base dei click sui banner stessi



Le origini dello Spyware

- Cosa c'è di male?



- Oltre al nome dei siti visitati facendo click sul banner pubblicitario vengono inviate anche altre informazioni di carattere privato



- Ad esempio nome utente di Windows, indirizzo IP, nome del provider, lista del software installato, download effettuato, numero di telefono del provider, ecc

Sommario

- Introduzione
- Un esempio di spionaggio
- Le origini dello Spyware
- Lo Spyware
- Spychecker
- Xp-AntiSpy



Spyware

- Gli spyware al momento dell'installazione del software in cui sono contenuti entrano in azione inserendo nuovi componenti nel registro di sistema
- Si attivano al momento dell'esecuzione
- Da questo momento, alcune aziende entrano in possesso dei nostri dati personali
- Le informazioni raccolte spaziano:
 - dal tipo di processore utilizzato
 - al sistema operativo
 - ai programmi che si utilizzano
 - dal numero e dal tipo di file che si scaricano dalla rete
 - ai siti visitati
 - etc.

Spyware

- Quindi è un sistema per i programmatori di software gratuito per ricavare soldi dal prodotto, piuttosto che venderlo
- Oltre ai banner vengono installati software aggiuntivi che inviano informazioni personali
- Una vera e propria spia sul vostro Pc che invia continuamente informazioni su di voi e sulle vostre abitudini ai server destinatari!
- Non tutti i programmi adware installano software spia, ma la maggior parte dei casi è così

Spyware

- Raccogliere dati a vostra insaputa per fini non eccessivamente chiari è una cosa al limite della legalità, ma non è illegale, almeno negli USA
- Lo spyware non apporta nessuna modifica al vostro pc e dunque non può essere considerato un virus
- In Italia è di sicuro in contrasto con la legge sulla privacy
- NESSUNO obbliga l'utente a installarli sul proprio pc

Spyware

- Lo Spyware dovrebbe essere una fonte di guadagno per chi scrive programmi gratuiti
- Lo Spyware è diventato un punto d'incontro, molto discutibile, tra chi scrive programmi e chi invece vuole usufruire di applicazioni free
- Fanno eccezione i programmi Open Source del tutto privi di spyware o di pubblicità...
- ...ma questi possono essere l'eccezione e non la regola!



Spyware

- Le principali aziende che si occupano di spyware sottolineano con grande attenzione il rispetto della privacy
- Tuttavia, ciò è affidabile?
- Queste aziende potrebbero facilmente tracciare un profilo molto preciso dei PC di milioni di utenti pieni di dati personali
- Siamo nel campo dei sospetti, e ognuno li può interpretare come meglio crede

Spyware

- Ecco un pò di nomi a cui vengono inviati i dati ottenuti mediante lo spyware:
 - Radiate
 - Conducent
 - Cydoor
 - Cometcursor
 - Web3000
 - Gator
- In realtà l'utente diventa un'incosciente pedina di una infinita indagine di mercato e non solo.

Sommario

- Introduzione
- Un esempio di spionaggio
- Le origini dello Spyware
- Lo Spyware
- Spychecker ←
- Xp-AntiSpy



Spychecker



- Spychecker aiuta l'utente a scoprire se le applicazioni contengono spyware prima di scaricarle
- Esso riconosce oltre 1000 programmi

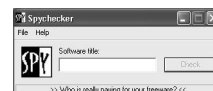
Spychecker

- L'applicazione Spychecker è distribuita tramite l'eseguibile:
 - Spychecker.exe
- Scaricabile da:
 - www.spychecker.com
- Con l'installazione viene creata una cartella in "C:\Programmi\Spychecker" e un suo collegamento nel Menu Avvio Start contenete:



Spychecker

- Se non siete sicuri che il programma freeware sia tale, basta inserire il nome nel apposito campo in Spychecker ed inviare la richiesta al sito www.spychecker.com tramite il tasto "Check":



Spychecker

- Il risultato della richiesta vi verrà fornito attraverso una pagine web nel vostro browser insieme ad un link alla politica sulla privacy adottata dalla compagnia ed altre informazioni
- Il sito di Spychecker localizza i componenti spyware attraverso l'aiuto di altri siti come Aureate/Radiate, Web3000, Conducent/TimeSink,Cydoor e altri



Spychecker

- All'avvio del programma vi comparirà un'icona nella Tray Icon:



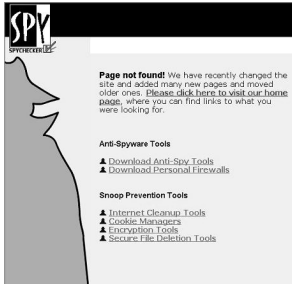
- Cliccando su quest'ultima vi apparirà una piccola finestra con un campo nel quale è possibile inserire il nome del programma da cercare:



- Cliccando il pulsante "Check" si avvierà la ricerca al database del sito, dopodichè si aprirà una pagina nel vostro browser contenente i risultati della ricerca

Spychecker

- Abbiamo testato Spychecker per diversi mesi (da Aprile 2004 a Febbraio 2005), usando come prova il noto programma "Kazaa"
- Tuttavia il risultato della ricerca, sfortunatamente, è stato sempre lo stesso:



Spychecker

- Come si può vedere, il risultato della ricerca è fallimentare, in quanto il sito è oggetto di aggiornamenti

- In realtà ci sembra molto deludente che dopo quasi un anno di ripetuti test il risultato sia sempre lo stesso, non riuscendo ad usufruire del servizio promesso

- **Conclusioni:**

- In conclusione l'idea di base del programma ci sembra molto originale ed utile, purtroppo ci sembra impensabile che il sito tutt'oggi non funzioni correttamente



Sommario

- Introduzione
- Un esempio di spionaggio
- Le origini dello Spyware
- Lo Spyware
- Spychecker
- Xp-AntiSpy ←



Xp-AntiSpy

- L'Xp-AntiSpy è una piccola utility freeware che permette di disabilitare alcune caratteristiche di aggiornamento ed autenticazione già presenti in Windows Xp



- Funzioni MediaPlayer
- Segnalazioni errori
- Impostazioni varie
- Internet Explorer 6
- Servizi
- Windows Messenger
- Regsvr32
- Menù special



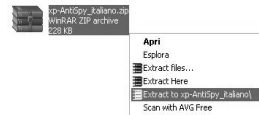
Xp-AntiSpy

- Xp-AntiSpy è ormai famosissimo fra tutti gli utilizzatori di Windows XP
- Offre la possibilità di modificare alcuni parametri nativi del Sistema Operativo
- Con pochi click è possibile modificare alcuni parametri relativi alla sicurezza e alla privacy con estrema facilità senza accedere al registro di sistema



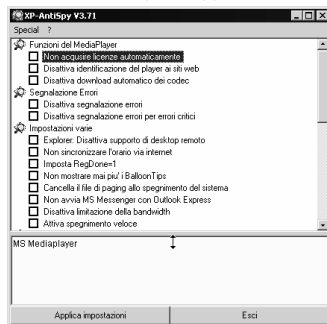
Xp-AntiSpy

- Il programma è completamente gratuito e l'ideatore continua a svilupparlo grazie alle donazioni libere degli utenti
- Il software non richiede installazione, è contenuto in un file zip di soli 227kb
- Scaricabile da:
 - <http://xp-antispy.org>
- Una volta scaricato procedete all'estrazione dello stesso:



Xp-AntiSpy

- Dopo aver avviato il programma, vi troverete di fronte l'unica effettiva finestra di Xp-AntiSpy



Xp-AntiSpy

- Il programma vi proporrà delle semplici caselline (o punti esclamativi) da spuntare per selezionare ciò che intendete modificare
- Dopo aver fatto le vostre scelte, applicate le impostazioni e chiudete il programma
- Eseguite tutte le operazioni, si dovrà riavviare il sistema



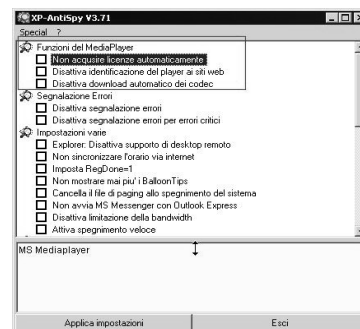
Xp-AntiSpy

- Le possibilità di intervento:
 - Funzioni MediaPlayer
 - Segnalazioni errori
 - Impostazioni varie
 - Internet Explorer 6
 - Servizi
 - Windows Messenger
 - Regsvr32
 - Opzioni "Special"



Xp-AntiSpy

- Funzioni Media Player



Xp-AntiSpy

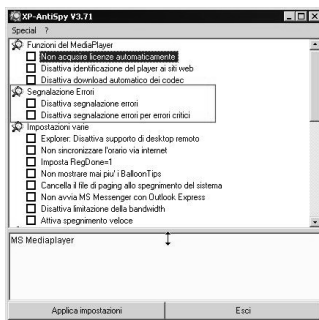
- **Non acquisire licenze automaticamente:** Il MediaPlayer potrebbe inviare informazioni personali per la gestione delle licenze multimediali.
Consiglio: selezionare
- **Disattiva identificazione del Player:** Il lettore viene riconosciuto dai siti Web in base al proprio identificativo di prodotto.
Consiglio: selezionare
- **Disattiva download automatico dei codec:** Il lettore può autonomamente prelevare i codec necessari per la riproduzione di determinato contenuto multimediale.
Consiglio: indifferente
- Tutte queste modifiche sono comunque possibili anche nelle opzioni di configurazione dello stesso Media Player

Xp-AntiSpy

- Le possibilità di intervento:
 - Funzioni MediaPlayer
 - Segnalazioni errori ←
 - Impostazioni varie
 - Internet Explorer 6
 - Servizi
 - Windows Messenger
 - Regsvr32
 - Opzioni "Special"

Xp-AntiSpy

- Segnalazione errori



Xp-AntiSpy

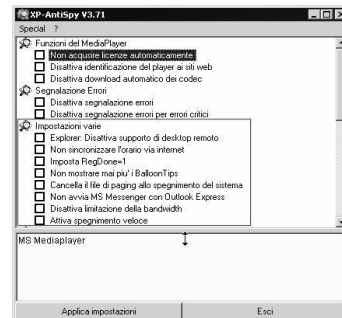
- **Disattiva segnalazione errori:** Windows XP crea un report per gli errori di sistema, che poi possono essere direttamente inviati a Microsoft.
Consiglio: selezionare, non si tratta di errori di grosso impatto
- **Disattiva segnalazione errori per errori critici:** Medesima situazione, ma per gli errori di rilevanza maggiore.
Consiglio: indifferente. Con l'accortezza di non inviare la segnalazione a Microsoft, può forse essere utile l'avviso relativo ad un errore critico

Xp-AntiSpy

- Le possibilità di intervento:
 - Funzioni MediaPlayer
 - Segnalazioni errori
 - Impostazioni varie ←
 - Internet Explorer 6
 - Servizi
 - Windows Messenger
 - Regsvr32
 - Opzioni "Special"

Xp-AntiSpy

- Impostazioni varie



Xp-AntiSpy



- **Explorer - disattiva supporto di Desktop Remoto:** Funzione di condivisione remota.
Consiglio: selezionare (anche se la funzione richiede in ogni caso l'autorizzazione dell'utente)
- **Non sincronizzare l'orario via Internet:** Funzione di regolazione automatica dell'orologio.
Consiglio: indifferente, personalmente attivata
- **Imposta RegDone=1:** Si modifica il registro di configurazione in modo da far apparire come eseguita la registrazione in linea del prodotto. NON relativo alla procedura di attivazione.
Consiglio: selezionare
- **Non mostrare più i Balloon Tips:** Evita la visualizzazione dei suggerimenti automatici di XP.
Consiglio: lasciare inalterato, a volte fanno comodo, specie all'inizio

6. Xp-AntiSpy



- **Cancella il file di paging allo spegnimento del sistema:** Svuotamento della memoria virtuale allo spegnimento.
Consiglio: lasciare inalterato, la funzione attivata comporta inoltre un notevole rallentamento nella chiusura del sistema
- **Non avviare Messenger con Outlook Express:** Significato evidente e funzione comodissima.
Consiglio: selezionare
- **Disattiva limitazione di banda QOS:** Limitazione in realtà non effettiva se non in particolari condizioni, e generalmente non riguardante PC domestici.
Consiglio: indifferente
- **Attiva spegnimento veloce:** Si spiega da solo.
Consiglio: indifferente

Xp-AntiSpy

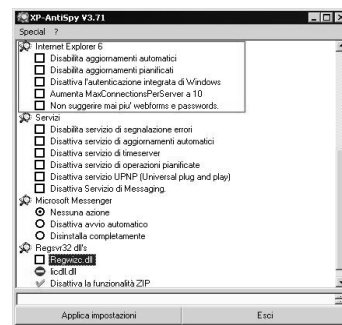


- Le possibilità di intervento:
 - Funzioni MediaPlayer
 - Segnalazioni errori
 - Impostazioni varie
 - Internet Explorer 6
 - Servizi
 - Windows Messenger
 - Regsvr32
 - Opzioni "Special"

Xp-AntiSpy



- Internet Explorer 6



Xp-AntiSpy



- **Disabilita aggiornamenti automatici:** Meglio sapere sempre cosa installare e cosa no.
Consiglio: selezionare
- **Disabilita aggiornamenti pianificati:** Come la precedente, con controllo degli aggiornamenti disponibili.
Consiglio: selezionare
- **Disabilita autenticazione integrata di Windows:** Possibilità di identificazione di Windows da parte dei siti Web.
Consiglio: selezionare
- **Aumenta MaxConnectionsPerServer a 10:** possibilità di aumentare il numero di download contemporanei di IE, in questo caso sino a 10.
Consiglio: selezionare con connessioni a banda larga, apparentemente inutile in analogico

Xp-AntiSpy



- **Non suggerire mai più webforms e password:** Inibizione di determinate funzioni del Completamento Automatico di IE.
Consiglio: non selezionare, preferibile intervenire direttamente su Completamento Automatico dal menù Opzioni Internet di IE, per poter meglio definire cosa ci interessa e cosa no

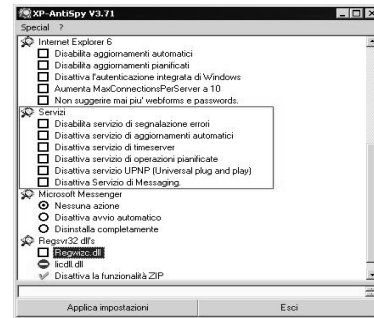
Xp-AntiSpy

- Le possibilità di intervento:
 - Funzioni MediaPlayer
 - Segnalazioni errori
 - Impostazioni varie
 - Internet Explorer 6
 - SERVIZI ←
 - Windows Messenger
 - Regsvr32
 - Opzioni "Special"



Xp-AntiSpy

- Servizi



Xp-AntiSpy

- Disabilita servizio di Segnalazione Errori:** La funzione che invia le segnalazioni errori (viste prima) a Microsoft.
Consiglio: selezionare
- Disabilita servizio di Aggiornamento Automatico:** Aggiornamento di Windows in automatico.
Consiglio: selezionare, meglio utilizzare Windows Update manualmente
- Disattiva servizio di Timeserver:** Sincronizzazione dell'orologio, già spiegato in precedenza
- Disattiva servizio di Operazioni Pianificate:** Necessario per alcuni programmi in background, e in ogni caso non particolarmente probante per il sistema.
Consiglio: lasciare inalterato



Xp-AntiSpy

- Disattiva servizio UPNP:** Universal Plug&Play, oggetto di una vecchia vulnerabilità ora risolta. A sistema aggiornato, tutto sotto controllo.
Consiglio: lasciare inalterato, previa verifica. In ogni caso piuttosto indifferente se appunto a sistema aggiornato
- Disattiva servizio di Messaging:** Messaggi diretti istantanei, specialmente a livello Intranet, ora in certi casi sfruttati a livello pubblicitario.
Consiglio: selezionare, specie se utente privato
- Anche in questo caso, certe opzioni sono configurabili da Windows stesso



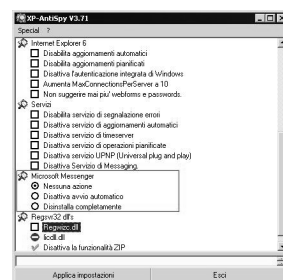
Xp-AntiSpy

- Le possibilità di intervento:
 - Funzioni MediaPlayer
 - Segnalazioni errori
 - Impostazioni varie
 - Internet Explorer 6
 - Servizi
 - Windows Messenger ←
 - Regsvr32
 - Opzioni "Special"



Xp-AntiSpy

- Windows Messenger



Xp-AntiSpy

- **Nessuna azione:** Usando Messenger, bene lasciare inalterato
- **Disattiva avvio automatico:** Impedisce a Messenger di avviarsi ad ogni boot. Selezionabile anche da Messenger stesso. Consiglio: secondo il vostro gusto, personalmente l'avvio automatico è inibito
- **Disinstalla completamente:** Disinstalla completamente il software. Consiglio: Scelta dell'utente



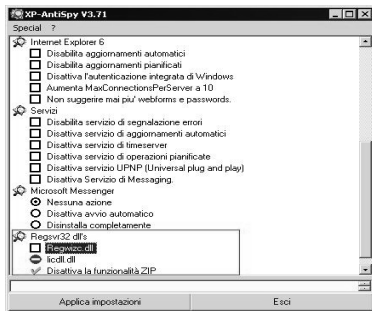
Xp-AntiSpy

- Le possibilità di intervento:
 - Funzioni MediaPlayer
 - Segnalazioni errori
 - Impostazioni varie
 - Internet Explorer 6
 - Servizi
 - Windows Messenger
 - Regsvr32 ←
 - Opzioni "Special"



Xp-AntiSpy

- Regsvr32 (eseguibile di registrazione e deregistrazione delle librerie dinamiche DLL)



Xp-AntiSpy

- **Regwizc.dll:** DLL che dovrebbe controllare i dati e l'avvenuta registrazione del prodotto. Consiglio: selezionare
- **licdll.dll:** Deregistrandola, si inibisce la procedura di attivazione di Windows XP. Non sarà possibile attivare nuovamente XP se non dopo averla riportata a default. Inoltre la funzione diventa accessibile solo tramite il menù "Special" di XP AntiSpy, menù di cui ci occuperemo tra poco. Non influente su OS Corporate Edition. Consiglio: lasciare inalterata



Xp-AntiSpy

- **Disattiva la funzionalità ZIP:** Rimuove l'associazione default di Cartelle Compresse per i file ZIP. Generalmente già inibita se usiamo un decompressore a cui abbiamo già associato l'estensione. Consiglio: dipende dalla presenza o meno di un decompressore di terze parti, comunque fortemente suggerito



Xp-AntiSpy

- Le possibilità di intervento:
 - Funzioni MediaPlayer
 - Segnalazioni errori
 - Impostazioni varie
 - Internet Explorer 6
 - Servizi
 - Windows Messenger
 - Regsvr32
 - Opzioni "Special" ←



Xp-AntiSpy

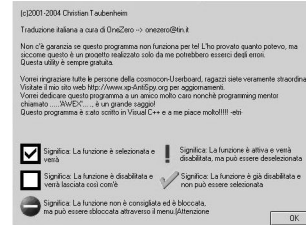
- Le Opzioni "Special" di XP AntiSpy



- Da qui si accede a funzioni supplementari, e più specificatamente:

Xp-AntiSpy

- Controlla Stato di Sistema:** Mostra le spiegazioni delle icone associate alle opzioni configurabili



Xp-AntiSpy

- Reset Stato di Sistema:** Possibilità di ripristinare a default le voci modificate, tranne le modifiche relative ad eliminazione di determinati elementi
- Scegli Impostazioni Consigliate:** Passa il controllo delle impostazioni alla scelta predefinita di XP AntiSpy. Evitabile
- Attiva Impostazioni da Esperto:** Permette la modifica delle voci originariamente non modificabili, come ad esempio la funzione di deregistrazione della lic.dll, vista in precedenza

Xp-AntiSpy

- Imposta Timeserver:** Per aggiungere e selezionare server di regolazione automatica dell'orologio, oltre a quelli presenti per default



Xp-AntiSpy

- Conclusioni**
 - Eccellente programma, che permette con pochi click di impostare opzioni altrimenti configurabili solo navigando fra differenti menù di Windows XP
 - La natura freeware e le svariate localizzazioni multilinguaggio ne hanno determinato una vasta diffusione e il giusto apprezzamento da parte degli utilizzatori
 - Ovviamente è bene usarlo in modo da essere ben consapevoli delle modifiche che si stanno apportando
- Programma che senza alcun dubbio non deve mancare su un sistema XP-based, sia per facilità di utilizzo, sia per i vantaggi che certe funzionalità offerte possono innegabilmente portare

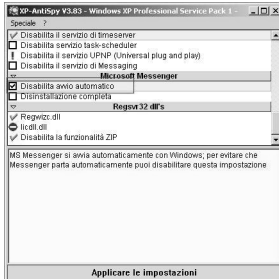
Xp-AntiSpy

- Un nostro test**

Adesso vi mostreremo passo per passo come con semplici click facciamo in modo che venga disabilitato l'avvio automatico di Windows Messenger

6. Xp-AntiSpy

- Andando nella categoria dedicata al Messenger in Xp-AntiSpy spuntiamo la casella "Disattiva avvio automatico":



Xp-AntiSpy

- Mostriamo qui la Tray Icons prima del riavvio del pc:



- A questo punto applichiamo le impostazioni con l'apposito tasto in basso e riavviamo il sistema.
- Al riavvio notiamo che nella tray non è più presente l'icona del programma:



- Il Xp-AntiSpy ha funzionato correttamente