



ADWARE & SPYWARE: tecniche e contromisure

A cura di: Iannone Annalisa e Maffei Lucia

1

Indice:

✓ Adware e spyware



- Come funzionano
- Come si diffondono
- Cosa causano

✓ Strumenti di difesa

- Programmi Anti-Spyware
- Ad-Aware
- Firewall

2

Adware e spyware

L'adware è una variante dello spyware, il quale è suddiviso in sei categorie:

- ❑ **Adware**: software che visualizza banner pubblicitari in base alle preferenze dell'utente
- ❑ **Keylogger**: software che cattura, memorizza ed invia a terze parti quello che l'utente digita per recuperare informazioni private
- ❑ **Trojan**: software all'apparenza innocui ma che possono causare perdite dei dati del computer dell'utente a vantaggio di terze parti
- ❑ **Scumware**: software che, cambiando i link, ridirigono l'utente su altri siti web
- ❑ **Dialer**: software usato per diffondere materiale pornografico su internet
- ❑ **Browser Hijacker**: software che tenta di modificare le impostazioni dei browser web dell'utente

3

Adware e spyware

- L'adware differisce dagli altri spyware poiché si limita esclusivamente a visualizzare banner pubblicitari su cui riceve informazioni da internet, per cui c'è un passaggio di dati dal server al programma.
- Gli altri spyware sono più dannosi poiché possono spiare i dati personali dell'utente per cui c'è anche un passaggio di dati dal programma al server.


4

- L'adware può usufruire dell'utilizzo dei cookie per effettuare una "profilazione" dettagliata degli utenti che navigano in Rete.
- Un cookie è un file di testo di piccole dimensioni, nel quale viene memorizzato un numero identificativo, che i siti che visitiamo ci lasciano sul PC senza causare alcun danno.
- I cookie vengono distribuiti tra i vari siti web che costituiscono il network pubblicitario, ed è il server pubblicitario che stila un elenco di tutti i siti web che uno stesso utente ha visitato utilizzando le informazioni raccolte per crearne un profilo dettagliato in modo da proporgli i banner che più lo possono interessare.

5

Indice:

✓ Adware e spyware

- Come funzionano 
- Come si diffondono
- Cosa causano

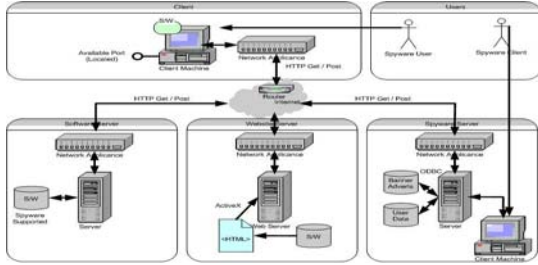
✓ Strumenti di difesa

- Programmi Anti-Spyware
- Ad-Aware
- Firewall

6

Adware e spyware: come funzionano

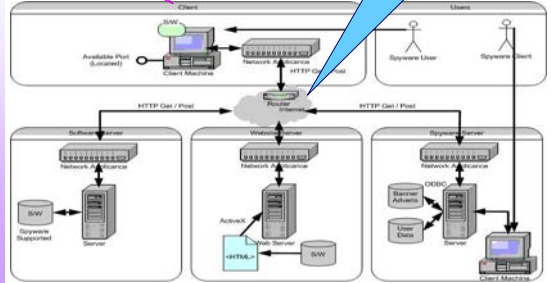
L'infrastruttura di rete dello spyware è:



7

Computer che contiene uno spyware

Dispositivo che permette il collegamento ad internet

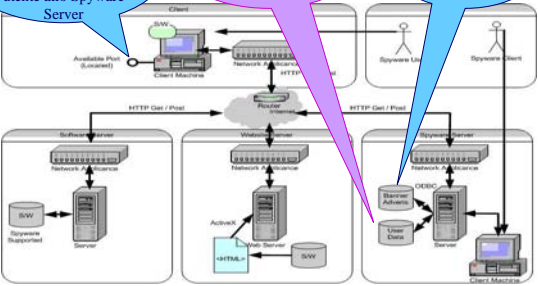


8

Porta disponibile tramite cui lo spyware invia le abitudini dell'utente allo Spyware Server

Contiene le informazioni sulle abitudini dell'utente ed è collegato al Server tramite ODBC

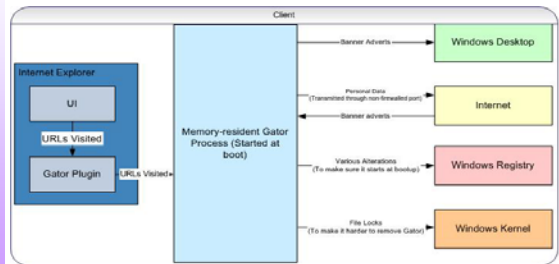
Contiene i banner pubblicitari spediti all'utente tramite internet in base alle sue preferenze



9

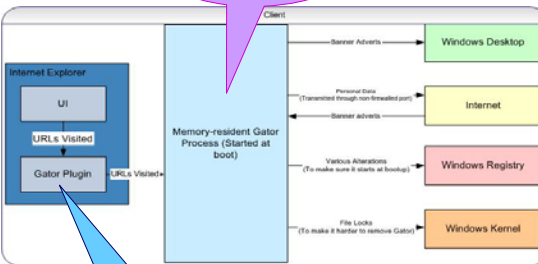
Funzionamento al lato client

Il funzionamento dello spyware al lato client si compone di due processi:



10

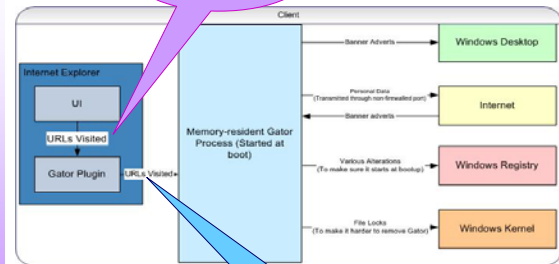
Applicazione residente in memoria creata al boot



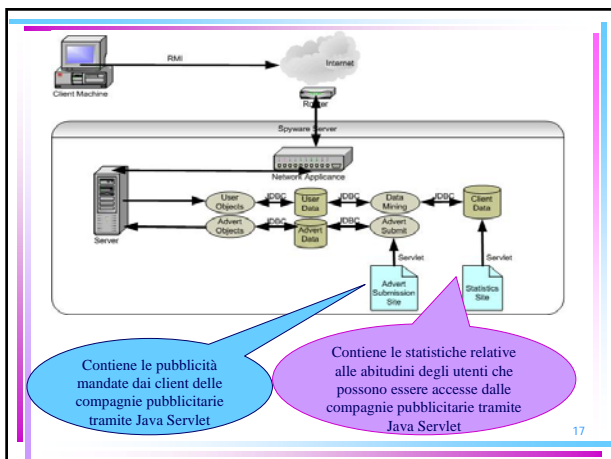
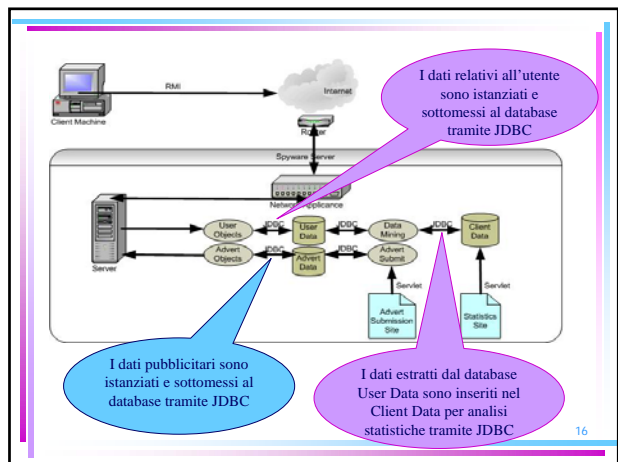
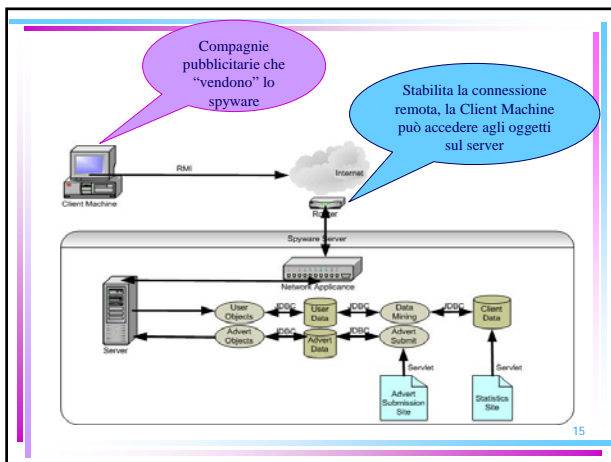
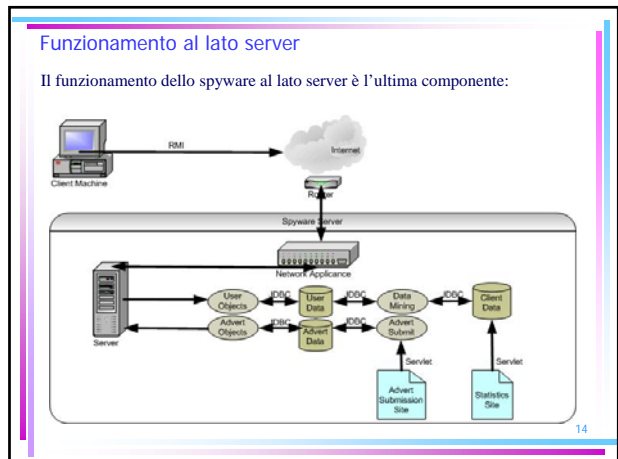
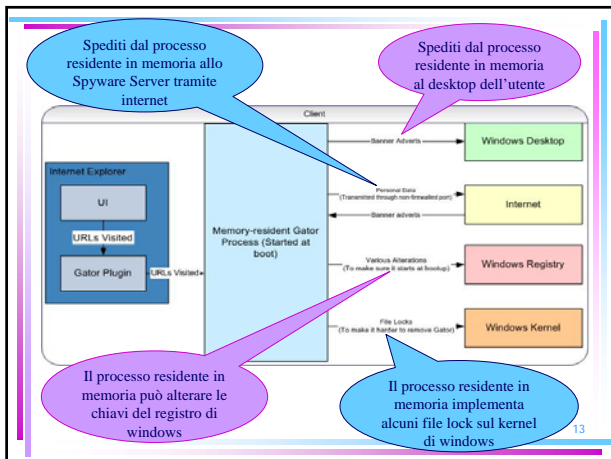
11

Inviati dall'interfaccia del browser al plugin

Inviati dal plugin al processo residente in memoria



12



- ### Indice:
- ✓ Adware e spyware
 - Come funzionano
 - Come si diffondono
 - Cosa causano
 - ✓ Strumenti di difesa
 - Programmi Anti-Spyware
 - Ad-Aware
 - Firewall

Adware e spyware: come si diffondono

Un PC viene infettato dagli spyware perlopiù tramite:

- il download di programmi freeware (del tutto gratuiti) o shareware (gratuiti solo per un determinato periodo)
- le utility di servizio che memorizzano e recuperano password, account, indirizzi e numeri di telefono
- la visita di pagine web create apposta per sfruttare eventuali vulnerabilità del browser

19

Indice:

- ✓ Adware e spyware
 - Come funzionano
 - Come si diffondono
 - Cosa causano 
- ✓ Strumenti di difesa
 - Programmi Anti-Spyware
 - Ad-Aware
 - Firewall

20

Adware e spyware: cosa causano

I danni più comuni causati dagli spyware alle macchine infette sono:

- riduzione della velocità della connessione ad Internet
- occupazione di cicli di CPU
- occupazione di spazio nella memoria RAM
- instabilità o blocco del sistema

I sintomi più evidenti di un'infezione da spyware sono:

- ✓ la difficoltà di connettersi ad internet
- ✓ la presenza di tentativi di connessione non richiesti dall'utente
- ✓ il passaggio del browser a nuovi siti web che non sono stati richiesti
- ✓ l'aggiunta di nuovi settaggi del browser non specificati

21

- Nessuno spyware ha lo scopo di danneggiare direttamente il sistema su cui è installato, dato che esso deve essere funzionante per consentire la raccolta e l'invio delle informazioni riguardanti l'utente, i quali sono spesso indotti a pensare che i malfunzionamenti derivano da difetti del sistema operativo o da virus.
- L'utente come soluzione pensa subito alla formattazione e reinstallazione del sistema operativo o al ricorso all'assistenza tecnica, con notevoli perdite di tempo e di denaro.

22

Indice:

- ✓ Adware e spyware
 - Come funzionano
 - Come si diffondono
 - Cosa causano
- ✓ Strumenti di difesa 
 - Programmi Anti-Spyware
 - Ad-Aware
 - Firewall

23

Strumenti di difesa

Disinstallare lo spyware è molto difficile in quanto è capace di:

- ✓ nascondersi agli antivirus
- ✓ continuare a funzionare nonostante il non funzionamento del programma in cui è inserito
- ✓ continuare a funzionare dopo la disinstallazione del programma in cui è inserito
- ✓ continuare a funzionare anche qualora l'utente decida di pagare il prezzo per la licenza d'uso del programma in cui è inserito

Per difendersi dagli spyware è bene:

- diffidare di qualsiasi programma offerto gratuitamente su Internet
- evitare di visitare siti "sospetti"
- astenersi dal seguire i link contenuti nei messaggi di posta elettronica indesiderata
- mantenere il sistema operativo aggiornato con le patch rilasciate dal produttore.

24

I modi più usati per difendersi dagli spyware sono:

- Programmi Anti-Spyware
- Ad-Aware
- Firewall

Ma per evitare lo spyware al 100% bisognerebbe installare **SOLO** programmi commerciali e programmi Open Source, **MAI** programmi freeware o shareware....ma si dubita che ciò sia per la maggior parte degli utenti proponibile.

25

Indice:

✓ Adware e spyware

- Come funzionano
- Come si diffondono
- Cosa causano

✓ Strumenti di difesa

- Programmi Anti-Spyware
- Ad-Aware
- Firewall

26

Strumenti di difesa: programmi anti-spyware

Il sito www.spyware.it contiene una lista dei programmi più utilizzati per rimuovere o prevenire l'installazione di software contenente spyware:

| Nome | SpyBot - S & D 1.2 | Anti-Keylogger 2.4 |
|----------------|--|--|
| Licenza d'uso | Freeware | Shareware |
| Compatibilità | Windows 98/ME/2000/XP | Windows 98/ME/2000/XP |
| Scaricabile da | www.safer-networking.org | www.anti-keyloggers.com |
| Descrizione | Rileva gli spyware installati nel nostro PC e rimuove determinati programmi che inviano dati tramite internet per tracciare dei profili statistici e individua quei programmi che catturano ciò che è digitato sulla tastiera. Possiede un'opzione per rimuovere le tracce di navigazione. | Offre una protezione completa contro quei programmi che catturano quello che è digitato sulla tastiera e che monitorano il sistema. Usa metodi per determinare se un programma cerca di catturare quello che viene digitato sulla tastiera e riesce in questo modo a trovarlo. |

27

| Nome | Spy Sweeper | PrivacyKeyboard 3.3 | SpywareBlaster 3.1 |
|----------------|---|--|---|
| Licenza d'uso | Shareware | Shareware | Freeware |
| Compatibilità | Windows 98/ME/2000/NT/XP | Windows NT/2000/XP | Windows 98/ME/2000/NT/XP |
| Scaricabile da | www.webroot.com/consumer/products/spysweeper | www.anti-keylogger.com | www.javacoolsoftware.com |
| Descrizione | Rileva e rimuove molte forme di spyware, tra cui i trojan, gli adware, i keylogger. Offre anche un'opzione per mettere in quarantena o disabilitare i programmi spyware presenti sul PC, consentendo di eseguirli ugualmente senza rischio. | Usato per proteggere dai keylogger che cercano di catturare quello che è digitato sulla tastiera del PC. Una volta installato è sempre attivo nella barra di sistema di windows ed offre una piccola tastiera virtuale che può essere utilizzata oltre a quella regolare ed in più è sicura. | Previene l'installazione di ogni tipo di spyware nel sistema e contiene una lista di programmi riconosciuti come spyware aggiornata tramite internet, ma non è in grado di rivelare se uno di essi è installato sul computer. |

28

| Nome | Ad-aware 6.181 | SpywareGuard 2.2 | PestPatrol 4.3.08 |
|----------------|--|---|---|
| Licenza d'uso | Freeware | Freeware | Shareware |
| Compatibilità | Windows 98/ME/2000/XP | Windows 98/ME/2000/XP | Windows 98/ME/2000/NT/XP |
| Scaricabile da | www.lavasoftusa.com | www.javacoolsoftware.com/spywareguard.html | www.pestpatrol.com |
| Descrizione | Rimuove gli spyware ed ha la capacità di eseguire una scansione completa della memoria, del registro di configurazione, delle unità fisse e rimovibili alla ricerca di tutti i componenti di raccolta dati e pubblicità aggressiva, offrendo agli utenti la sicurezza di navigare in Internet sapendo che la privacy non verrà lesa. | Previene l'installazione di spyware sul PC in quanto monitora il sistema in tempo reale. Se rileva uno spyware l'accesso al file infetto viene bloccato aspettando che l'utente scelga quale deve essere l'azione da compiere. Ha un'utilità per aggiornare la lista degli spyware. | Protegge la privacy eseguendo una scansione del sistema, che rileva ed elimina le minacce come adware, trojan ed altre forme di spyware. Rileva gli spyware che usano una connessione telefonica dal PC e i programmi che catturano quello che digitiamo sulla tastiera. Si aggiorna automaticamente. |

29


| Nome | Bazooka 1.13.01 | X-Cleaner Free 2.2 | Personal Antispy 1.2 |
|----------------|--|--|--|
| Licenza d'uso | Freeware | Freeware | Shareware |
| Compatibilità | Windows 98/ME/2000/XP | Windows 98/ME/2000/XP | Windows 2000/XP |
| Scaricabile da | www.kephyr.com | www.xblock.com/download-freeware.php | www.blazingtools.com |
| Descrizione | È un programma piccolo e veloce che effettua la scansione del sistema ricercando gli spyware installati. Il suo database contiene più di 460 forme di spyware, tra cui i keylogger, i trojan. Non rimuove i programmi rilevati ma informa della loro presenza e fornisce le istruzioni per rimuoverli. | Insieme di programmi che rileva e rimuove gli spyware installati nel PC automaticamente all'avvio e reimposta il registro di sistema di windows. La versione freeware non ha delle funzioni che sono disponibili solo nella versione completa del programma che è a pagamento. | Trova i trojan, che catturano quello che viene digitato sulla tastiera, e altri tipi di spyware installati nel PC. Analizza tutti i processi che sta eseguendo il PC dove è installato. Non effettua un controllo continuo del PC, infatti per una scansione del sistema è necessario farlo manualmente. |

30

| | | |
|-----------------------|---|---|
| Nome | XP-AntiSpy 3.72 | SpyRemover 1.60 |
| Licenza d'uso | Freeware | Shareware |
| Compatibilità | Windows XP | Windows 98/ME/2000/XP |
| Scaricabile da | www.xp-antispy.org. | www.itcompany.com |
| Descrizione | Applicazione che consente in modo rapido di riparare alcune vulnerabilità del sistema disabilitando alcune funzioni di aggiornamento e autenticazione contenute in Windows XP che potrebbero compromettere la sicurezza o la privacy. Grazie a XP-Antispy è possibile disabilitare manualmente tutti i servizi che destano sospetti attraverso un elenco dettagliato. | Scova e rimuove keylogger, trojan ed altri programmi pericolosi dal PC ed offre una visualizzazione categorizzata degli spyware trovati. Inoltre è possibile visualizzare e disabilitare le applicazioni che vengono eseguite all'avvio del PC. |

31

Indice:

- ✓ **Adware e spyware**
 - Come funzionano
 - Come si diffondono
 - Cosa causano
- ✓ **Strumenti di difesa**
 - Programmi Anti-Spyware
 - Ad-Aware 
 - Firewall

32

Strumenti di difesa: Ad-Aware

Il software Ad-Aware è:

- prodotto da Lavasoft
- completamente gratuito
- compatibile con windows 95/98/2000/ME/XP
- capace di rimuovere gli spyware e tutto ciò che compromette la sicurezza del computer permettendo agli utenti di navigare in internet senza che la privacy venga violata.

33


Ad-Aware permette di eseguire:

- una scansione completa della memoria
- una scansione del registro di configurazione
- una scansione delle unità fisse, rimovibili ed ottiche
- una ricerca di tutti gli spyware che riescono ad ottenere informazioni personali e che inviano pubblicità aggressiva pop-up.


Bisogna spesso aggiornarlo in quanto vengono creati sempre nuovi spyware ed i loro produttori fanno piccole modifiche ai software con lo scopo che lo spyware non venga più riconosciuto.

34

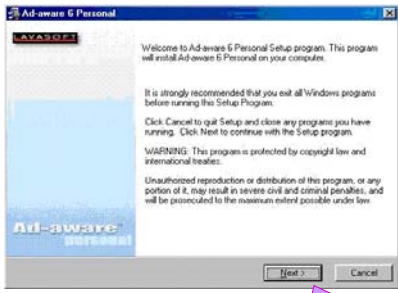
Per installarlo:

1. collegarsi al sito ufficiale di Ad-aware (www.lavasoft.com)
2. scaricare il programma nella sezione download (aaw6181.exe)
3. salvarlo su disco
4. mandarlo in esecuzione
5. fare un doppio click sull'icona 

Quello che appare è:




35

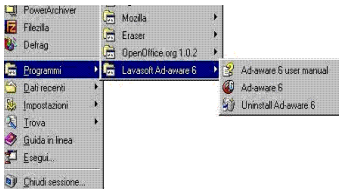


36

Dopo l'installazione appare l'icona:

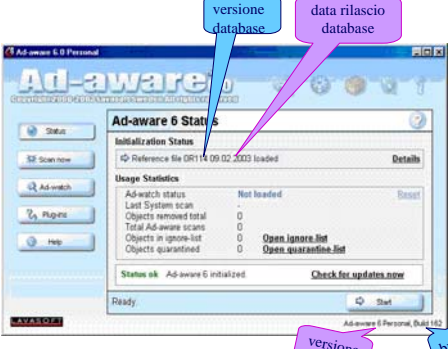


e una cartella nel menù Start → Programmi:

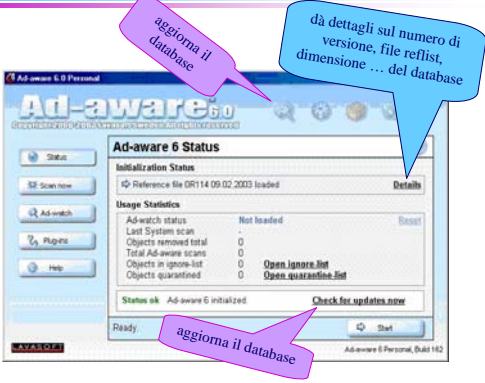


37

Cliccando sull'icona si apre il programma e appare:

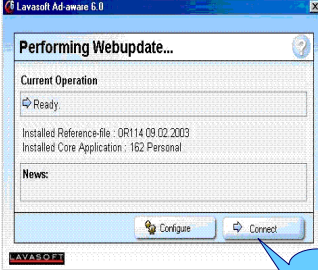


38



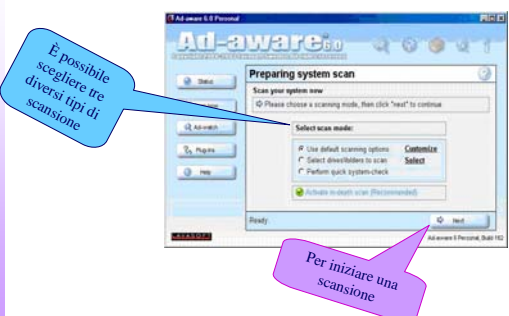
39

Cliccando su **Check for now Update** appare una finestra:



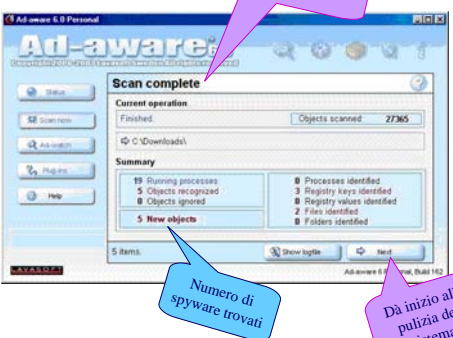
40

Cliccando su **Start** oppure **Scan Now**, appare:



41

A scansione terminata appare:



42

- Premendo Next appare:

Visualizza nel dettaglio i 5 componenti spyware trovati



43

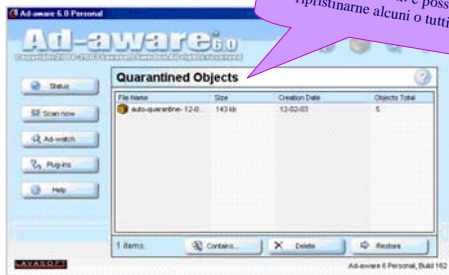
- Per rimuovere gli spyware trovati mettere il segno di spunta, premere Next, ed infine OK.



44

Poi appare:

Spyware quarantinati: è possibile ripristinarne alcuni o tutti



45

È buona cosa eseguire il programma subito dopo il riavvio del computer senza essere collegati a Internet e chiudendo quante più applicazioni possibile, così la scansione effettuata da Ad-Aware non viene intralciata dalle applicazioni in esecuzione.

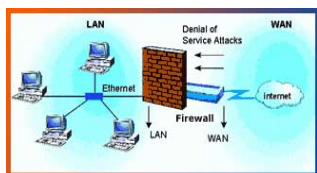
Indice:

- ✓ Adware e spyware
 - Come funzionano
 - Come si diffondono
 - Cosa causano
- ✓ Strumenti di difesa
 - Programmi Anti-Spyware
 - Ad-Aware
 - Firewall

46

Strumenti di difesa: firewall

- Sono un insieme di strumenti hardware e software che controlla e filtra il traffico in entrata e in uscita consentendo solo a determinate applicazioni autorizzate di accedere ad internet o al PC.
- Usati per concentrare la gestione della sicurezza della rete in pochi punti, poichè in grado di minimizzare l'interazione tra internet e le macchine della rete stessa.



47

I firewall:

- *bloccano* le porte non in uso del pc e se un programma lecito ha bisogno di una porta la aprono per il tempo strettamente necessario e poi la richiudono automaticamente
- *ci rendono* "Stealth" (invisibili) in modo che se qualcuno riesce ad avere il nostro IP e prova a "bussare" non ottiene risposta-eco e quindi non capisce nemmeno se siamo ancora connessi o meno
- *ci difendono* dall'installazione sul computer in remoto di alcuni spyware ad opera di pirati informatici

48

Attualmente sono disponibili tre tipi principali di firewall:

- *Firewall software* compatibili con Windows 98/ME/2000 e non necessari per Windows XP in quanto tale sistema operativo include un firewall incorporato.
- *Router hardware* rappresentano una scelta valida per le reti domestiche che verranno collegate a Internet.
- *Router senza fili* necessari se si utilizza una rete senza fili, poiché solo alcuni di esse sono dotate di un firewall incorporato.

49

Ecco una lista dei migliori firewall presenti sul mercato che tiene conto della loro semplicità di configurazione e del loro livello di protezione:

| | | |
|------------------------|--|---|
| Nome | Agnitum Outpost Firewall 1.0.1817 | Jetico Personal Firewall 1.0.1.61 |
| Scaricabile da | www.agnitum.com | www.jetico.com |
| Compatibile con | Windows 95/98/ME/2000/NT/XP | Windows 98/ME/2000/NT/XP |
| Dimensione | 2,8 Mb | 2,7 Mb |
| Licenza d'uso | Gratuito | Gratuito |
| Descrizione | Semplice da usare ed efficiente, protegge da tentativi estremi di accesso al PC come cookies, banner pubblicitari troppo invasivi, virus diffusi via e-mail e spyware. | Si basa su tre livelli di protezione sovrapposti, il primo filtra tutto quello che viaggia attraverso la Rete, il secondo monitora le connessioni ad Internet e il terzo segnala attività sospette. |

50

| | | |
|------------------------|---|--|
| Nome | Agnitum Outpost Firewall 3.0 | FirePanel XP v1. 5. 4. 0 |
| Scaricabile da | www.agnitum.com | www.router19.org |
| Compatibile con | Windows 98/ME/2000/XP/NT | Windows XP |
| Dimensione | 4.6 Mb | 50 Kb |
| Licenza d'uso | Non gratuito | Gratuito |
| Descrizione | Filtra gli allegati della posta elettronica e rileva i tentativi di scansione delle porte del PC, consente di aggiungere nuovi plug-in. Controlla in tempo reale l'attività del sistema operativo e blocca azioni sospette legate ai malware. | È capace di verificare le informazioni che viaggiano nei vari pacchetti IP e di mostrare il contenuto dei file di log e le connessioni attive sul sistema compresi i processi da cui esse dipendono. Restituisce informazioni sul consumo di banda, errori di protocollo, numeri di pacchetti in entrata/uscita. |

51

| | | |
|------------------------|---|---|
| Nome | Firestarter 0.9.1 | Kerio Personal Firewall 4.2.2 |
| Scaricabile da | http://firestarter.sourceforge.net/ | www.kerio.com |
| Compatibile con | Linux | Windows 98/ME/2000/NT/XP |
| Dimensione | 300 Kb | 7.2 Mb |
| Licenza d'uso | Gratuito | Gratuito |
| Descrizione | Semplice da usare ed è in grado di proteggere sia un singolo computer, sia una rete. Permette di creare regole in base alle necessità del momento e di aprire e chiudere le porte con pochi click del mouse. È in grado di mostrare costantemente tutti gli attacchi effettuati contro il sistema | Agisce come un filtro tra il computer e Internet, e controlla sia il traffico in entrata che quello in uscita, in modo che tutte le applicazioni che vogliono comunicare con Internet vengono riconosciute e i tentativi non autorizzati di scambiare dati vengono bloccati e segnalati all'utente. |

52

| | | |
|------------------------|--|---|
| Nome | VisualZone Report Utility 5.7 | Sygate Personal Firewall 5.6 |
| Scaricabile da | www.visualizesoftware.com | www.sygate.com |
| Compatibile con | Windows 95/98/ME/2000/NT/XP | Windows 95/98/ME/2000/NT/XP |
| Dimensione | 2.6 Mb | 8.8 Mb |
| Licenza d'uso | Gratuito | Gratuito |
| Descrizione | Fornisce informazioni dettagliate sui tentativi da parte di intrusi di accedere al PC ed è capace di analizzare questi dati ottenendo informazioni su chi ha sferrato l'attacco quindi preparare e-mail, in modo automatico, da inviare ai rispettivi provider comunicando in tal modo i tentativi di accesso illegale al proprio sistema. | Rende il PC "invisibile" agli altri utenti connessi ad internet. Con questo software tutti i tentativi di accesso da parte di intrusi vengono subito segnalati all'utente. Esiste una versione di questo firewall più avanzata ma non gratuita. |

53

| | | |
|------------------------|---|---|
| Nome | ZoneAlarm Free 6.0.632.002 | Tiny Personal Firewall 2.0.15 |
| Scaricabile da | www.zonealarm.com | www.tynisoftware.com |
| Compatibile con | Windows 95/98/ME/2000/NT/XP | Windows 95/98/ME/2000/NT |
| Dimensione | 8.9 Mb | 1.5 Mb |
| Licenza d'uso | Gratuito | Gratuito |
| Descrizione | Protegge il PC dagli attacchi sferrati via internet poiché riesce a controllare tutto il traffico entrante ed uscente. Controlla le richieste di accesso ad internet da parte di qualsiasi applicazione installata sul PC. Ciò previene l'accesso alla rete da parte di programmi indesiderati. | Protegge il PC da attacchi sferrati in Rete, è molto veloce ed occupa poca larghezza di banda. Si possono impostare regole personalizzate ed ha una semplice procedura di log anche se non molto dettagliata. Non dispone di filtri avanzati e non offre la possibilità di rimuovere delle porte dal controllo del programma. |

54

- I firewall devono essere configurati, ovvero bisogna creare delle *regole* di accesso alla rete privata dall'esterno e viceversa, mettendo in atto così politiche di sicurezza complesse.
- Definire una *regola* significa specificare quali applicazioni possono accedere alla rete, poichè ritenute sicure, e quali invece devono essere sottoposte a controlli maggiori.
- Prima di definire delle *regole* definitive è opportuno fare una scansione del pc con un antivirus aggiornato altrimenti si rischia di dare un "permesso" di uscita a qualche applicazione non sicura.