Introduzione

Panda Antivirus

Panda Antivirus è una soluzione completa ed efficace per proteggere il computer contro qualsiasi tipo di virus. Comprende versioni Windows 95, Windows NT Workstation, Windows 3.1x, DOS e OS/2, affinché la protezione sia effettiva indipendentemente dal sistema operativo utilizzato. Questa guida si riferisce a **Panda Antivirus** per Windows NT Workstation.

Strategie di protezione

Panda Antivirus comprende varie strategie di protezione contro i virus:

- **Protezione permanente:** la protezione permanente si occupa di proteggere il computer contro i virus costantemente e senza che l'utente debba intervenire. Il grande vantaggio di questa strategia di protezione sta nel fatto che permette di proteggere il computer in modo completamente automatico.
- **Analisi su richiesta:** l'analisi su richiesta permette di analizzare qualsiasi parte del computer su richiesta dell'utente. Una volta scelta l'area da analizzare comincerà la ricerca di virus all'interno dell'area selezionata.
- **Disinfezione:** una volta individuato un virus, esistono diverse possibilità di intervento. Una è la disinfezione, che consiste nell'eliminazione del virus dal file lasciando quest'ultimo com'era prima dell'infezione.
- **Analisi euristica:** l'analisi euristica è una tecnica di analisi alternativa a quelle viste in precedenza. Funziona a richiesta, l'utente, cioè, deve indicare quale area del computer desidera analizzare con questo metodo in un momento determinato. Questa tecnica di analisi è pensata per individuare virus sconosciuti.
- **Ricerca di catene:** Come l'analisi euristica, si tratta di una tecnica di analisi alternativa che funziona su richiesta dell'utente. La sua utilità consiste nella ricerca di nuovi virus sulla scorta dei dati offerti dal supporto tecnico di Panda Software.
- **Altre opzioni:** questa voce comprende alcune capacità dell'antivirus destinate a fornire informazione o ad agevolare la gestione dell'antivirus stesso. Per esempio, è disponibile un rapporto sui risultati in cui si possono vedere le diverse incidenze ed operazioni realizzate con l'antivirus.

Soluzioni antivirus Panda Software

Panda Software offre le seguenti soluzioni antivirus:

- **24h-365d® Assicurazione Antivirus® per PC Individuali**. *Licenze.*
- **24h-365d® Assicurazione Antivirus® per PC in rete** (distribuzione automatica da server).
- **24h-365d® Assicurazione Antivirus® per Server di rete** (Novell NetWare e Windows NT Server).
- **24h-365d® Assicurazione Antivirus® per Reti Locali**.
- **24h-365d® Assicurazione Antivirus® per clienti di e-mail e Groupware**.
- **24h-365d® Assicurazione Antivirus® per Server di e-mail e Groupware**.
- **24h-365d® Assicurazione Antivirus® per Server di Posta SMTP**.
- **24h-365d® Assicurazione Antivirus® per PC collegati a Internet**.
- **24h-365d® Assicurazione Antivirus® per Server di Internet (SMTP, FTP e HTTP)**.

- **24h-365d® Assicurazione Antivirus® per Proxy**.

Che cos'è 24h-365d Assicurazione Antivirus Panda Software?

24h-365d® Assicurazione Antivirus® Panda Software è un nuovo e rivoluzionario concetto di protezione antivirus che apporta una sicurezza ancora maggiore. **24h-365d® Assicurazione Antivirus® Panda Software** è una straordinaria combinazione di prodotti e servizi che offre i più alti livelli di protezione contro i virus. **24h-365d® Assicurazione Antivirus® Panda Software** si può contrattare con diverse scadenze di diritto ad aggiornamenti e con diversi periodi di aggiornamento.

Il prodotto è un apporto **Panda Antivirus**, un antivirus che ha ottenuto i certificati più ambiti in quanto a individuazione di virus:

- Il **Certificado ICSA:** concesso dalla prestigiosa organizzazione americana ICSA ai prodotti antivirus che individuano periodicamente il 100% dei virus *In the Wild* (i virus più diffusi in un momento determinato) e più di un 90% della *Zoo Collection* (collezione di migliaia di virus meno diffusi).
- Il **Certificado CheckMark:** concesso dalla rivista inglese specializzata in Sicurezza Informatica *Secure Computing*.

Se non si dispone di **24h-365d® Assicurazione Antivirus® Panda Software**, si può contrattarlo usando il tagliando d'ordine allegato alla scheda di registrazione. I servizi offerti da **24h-365d® Assicurazione Antivirus® Panda Software** sono i seguenti:

- **Hot-Line:** per UN anno risolveremo i problemi tecnici per telefono, fax, Internet o e-mail. Si può chiamare in qualsiasi momento, a qualsiasi ora del giorno o della notte. I nostri tecnici sono sempre a disposizione dall'altra parte del filo; sono persone altamente qualificate a disposizione 24 ore su 24, 365 giorni all'anno. È un servizio esclusivo di **Panda Software**.
- **S.O.S. Virus:** se si trova qualche virus che **Panda Antivirus** no individua o non elimina, manderemo un corriere a domicilio (o raccoglieremo il campione sospetto in qualche altro modo) e in meno di 24 ore creeremo una nuova versione capace di individuare ed eliminare il nuovo virus. Le manderemo questa nuova versione senza alcun costo aggiuntivo.
- **Servizio di Aggiornamenti con consegna a domicilio:** l'antivirus sarà totalmente aggiornato. L'utente riceverà a domicilio gli aggiornamenti mensili o trimestrali in CD o in floppy se ha contrattato la nostra soluzione **24h-365d® Assicurazione Antivirus® Panda Software**. Potrà anche aggiornare il prodotto attraverso il nostro WEB tutte le volte che vorrà per un anno; noi garantiamo come minimo un aggiornamento nuova ogni giorno.
- **Servizio WEB:** soluzione dei dubbi più frequenti ed informazione su virus.

Installazione

Requisiti

Per installare **Panda Antivirus** per Windows NT Workstation sono necessari i seguenti elementi:

- PC IBM compatibile con processore 486 o superiore.
- 16 Mb di RAM.
- 4 Mb di spazio su disco rigido.
- Sistema operativo Windows NT 3.51 o superiore.
- Lettore CD-Rom.
- Mouse.

Procedura di installazione

Esistono due versioni di **Panda Antivirus** per Windows NT Workstation. Una di queste corrisponde alla versione 3.51 del citato sistema operativo e l'altra alla versione 4.0. È necessario prestare attenzione e installare la versione corrispondente a ciascun sistema operativo.

Entrambe le versioni possono essere installate unicamente dal CD-Rom che accompagna il prodotto. Per installare una qualsiasi delle due versioni, è necessario eseguire il programma CDMENU.COM. Questo programma offre un semplice menù di opzioni. In primo luogo è necessario scegliere la lingua desiderata e quindi la versione che si desidera installare. In questo caso è necessario scegliere una delle due versioni di **Panda Antivirus** per Windows NT, la 3.51 o la 4.0 in base al sistema operativo che si è installato.

Per poter installare la versione di **Panda Antivirus** per Windows NT Workstation è necessario avere dei diritti di amministratore sul computer. Esiste questa necessità a causa dei diritti necessari per installare il driver che si occupa della protezione permanente.

La procedura di installazione si basa sui seguenti passaggi:

1. In primo luogo viene visualizzata una schermata di benvenuto.
2. Quindi vengono chiesti i dati dell'utente.
3. Si chiede la directory in cui si desidera installare l'applicazione.
4. Si chiede il gruppo di programmi in cui verranno create le icone di accesso all'antivirus.
5. Viene data l'opportunità di scegliere se si desidera installare la protezione permanente (driver **Sentinel**) o no.
6. Ha inizio la copiatura dei file su disco rigido.
7. Una volta terminata la copiatura dei file, si consiglia di riavviare il computer affinché la protezione permanente incominci a funzionare.

Aggiornamento dell'antivirus

Per aggiornare una versione con un aggiornamento ricevuto, è sufficiente installare la nuova versione su quella vecchia.

Disinstallazione

Se si tratta della versione per Windows NT 3.51, la disinstallazione di **Panda Antivirus** viene realizzata mediante il programma UNINST che si trova nel gruppo di programmi della applicazione.

Se si tratta della versione per Windows NT 4.0, la disinstallazione di **Panda Antivirus** viene realizzata mediante l'opzione *Aggiungi o elimina programmi* del *Pannello di Controllo*. È sufficiente scegliere **Panda Antivirus Windows NT W/S 4.0** dalla lista che appare in tale opzione e premere il pulsante *Aggiungi o Elimina*. Per completare la disinstallazione è necessario riavviare il computer.

Non bisogna cercare di disinstallare la versione cancellando la cartella in cui è stato installato l'antivirus. Disinstallare sempre seguendo la procedura descritta.

Che cos'è la protezione permanente?

La protezione permanente è un programma che, dal momento in cui viene avviato il computer, intercetta tutte le operazioni che implicano un pericolo di contagio e verifica che nessun virus entri nel sistema.

La protezione permanente funziona in modo totalmente automatico e senza che l'utente debba realizzare alcuna operazione. Nonostante la vigilanza sia costante, le prestazioni del sistema non ne risentono; l'installazione della protezione permanente è quindi consigliabile in ogni caso, dato che aumenta considerevolmente la protezione del computer.

Come si usa la protezione permanente

La protezione permanente è una delle opzioni dell'installazione. Se si è deciso di installare tale protezione, una volta avviato il computer, la protezione permanente (**Sentinel**) comincerà a funzionare.

Se il sistema operativo è Windows NT Workstation 3.51, **Sentinel** apparirà come un'icona minimizzata nel desktop di Windows. Se il sistema operativo è Windows NT Workstation 4.0, **Sentinel** apparirà come un'icona vicino all'orologio della barra delle applicazioni.

Il funzionamento della protezione permanente è totalmente automatico. Se in una certa operazione **Sentinel** rileva la presenza di un virus, ne dà immediato avviso ed esegue l'azione pertinente.

Come si configura la protezione permanente

La protezione permanente si può configurare ed adattare alle necessità di ogni singolo utente. Facendo doppio clic sull'icona di **Sentinel**, appare una finestra con varie schede. Ognuna di esse si riferisce alla configurazione dei diversi aspetti di **Sentinel**. Le opzioni di configurazione sono le seguenti:

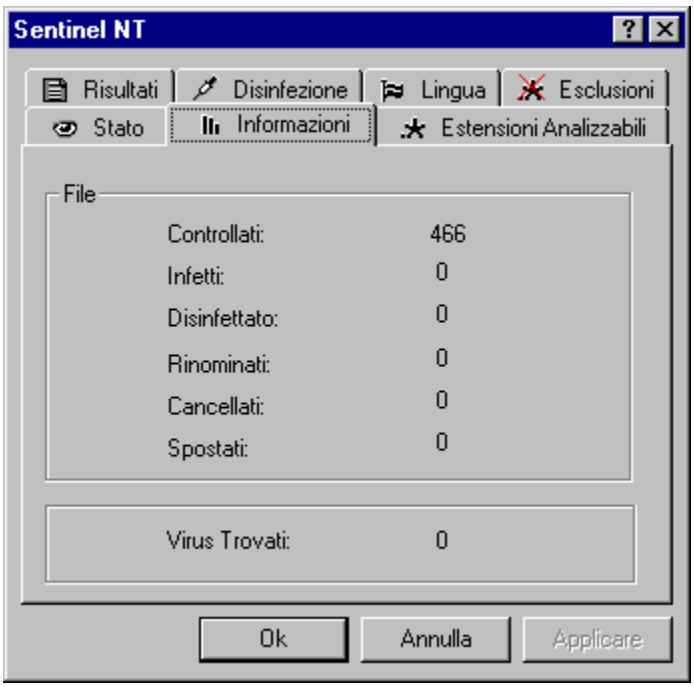
Stato

In questa scheda si definisce lo stato della protezione permanente.

- **Attivazione:** mediante questa opzione, si attiva o disattiva la protezione permanente. Va tenuto presente che se si disattiva la protezione permanente il computer resta privo di protezione contro i virus.
- **Arrivi:** se la protezione permanente è attivata, questa opzione indica che si devono analizzare tutti i file in arrivo al computer. Saranno analizzati anche i file creati e le modifiche apportate agli stessi.
- **Partenze:** se la protezione permanente è attivata, questa opzione indica che si devono analizzare tutti i file in partenza dal computer. Si analizzeranno anche tutte le aperture ed esecuzioni di file.
- **Rinominazione:** se la protezione permanente è attivata, questa opzione indica che si devono analizzare tutte le operazioni di rinominazione di file.
- **Rete Microsoft:** se la protezione permanente è attivata, questa opzione indica che si devono analizzare in modo remoto tutte le operazioni effettuate su un'unità di rete Microsoft.
- **Rete Novell:** se la protezione permanente è attivata, questa opzione indica che si devono analizzare in modo remoto tutte le operazioni effettuate su un'unità di rete Novell.

Informazione

In questa scheda si mostrano diverse informazioni relative all'attività della protezione permanente.



- **Revisioni:** indica il numero di file che la protezione permanente ha revisionato alla ricerca di virus dal momento dell'avvio del sistema.
- **Infetti:** questa informazione mostra il numero di file infetti trovati.
- **Disinfezioni:** indica il numero di file disinfettati dalla protezione permanente.
- **Rinominazioni:** mostra il numero di file che la protezione permanente ha rinominato.
- **Cancellazioni:** mostra il numero di file che la protezione permanente ha cancellato perché contaminati da virus.
- **Spostamenti:** mostra il numero di file che la protezione permanente ha spostato perché contaminati da virus.
- **Virus trovati:** indica quanti virus sono stati trovati.

Estensioni analizzabili

In questa scheda si configurano le estensioni che la protezione permanente deve analizzare.

- **Lista delle estensioni:** nella lista delle estensioni si possono selezionare tutte quelle estensioni che si desidera analizzare. La protezione permanente intercetta sempre tutti i file a cui si accede, ma analizzerà solo quelli che abbiano una delle estensioni selezionate. Indipendentemente dalla selezione fatta, i file EXE y COM si analizzeranno sempre.
- **Estensioni della lista:** questo dato informa sul numero di estensioni presenti nella lista.
- **Estensioni attive:** questo dato informa sulle estensioni che sono state selezionate nella lista affinché siano analizzate.
- **Aggiungi estensione:** per aggiungere un'estensione alla lista, si deve scrivere l'estensione nella casella apposita e premere il pulsante *Aggiungi*.
- **Elimina estensione:** per eliminare un'estensione dalla lista, si deve selezionare nella lista l'estensione da eliminare e premere il pulsante *Elimina*.
- **Tutti i file:** se si seleziona questa opzione, verranno analizzati tutti i file indipendentemente dalle estensioni selezionate.
- **Analizzare file compressi:** se si seleziona questa opzione, verranno analizzati i file compressi a cui si accede.

Lingue

In questa scheda si può consultare la lingua usata nella protezione permanente; si può scegliere un'altra lingua nella lista delle lingue disponibili.

- **Lingue disponibili:** mostra una lista delle diverse lingue disponibili per la protezione permanente. Per cambiare lingua basta selezionare la lingua prescelta e premere il pulsante *Accetta* o il pulsante *Applica*.
- **Lingua attuale:** si mostra la lingua che sta utilizzando in quel momento la protezione permanente.

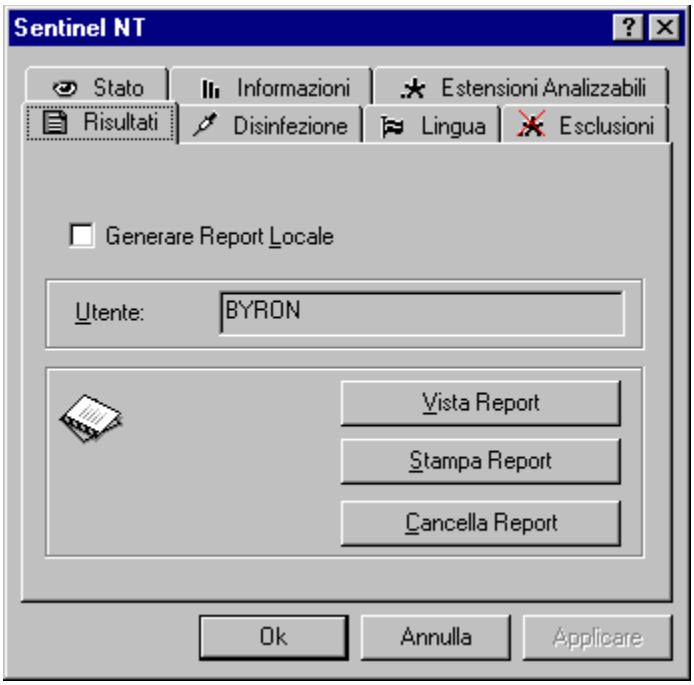
Esclusioni

In questa scheda si possono indicare le aree, file o estensioni che non si vogliono analizzare. Indipendentemente da quanto indicato in *Estensioni*, tutte le aree, file o estensioni selezionati qui, **non verranno analizzati**.

- **Attiva esclusioni:** se si seleziona questa opzione, si attiverà la funzione di esclusione in funzione dei dati di volta in volta indicati.
- **Directory:** in questa scheda si mostra una lista con tutte le directory che non si dovranno analizzare.
- **Aggiungi directory:** mediante questa opzione, si possono aggiungere directory alla lista delle directory che non si analizzeranno.
- **Elimina directory:** mediante questa opzione, si possono eliminare directory dalla lista di directory che non si analizzeranno.
- **File:** in questa scheda si mostra una lista dei file che non si devono analizzare.
- **Aggiungi file:** questa opzione permette di aggiungere un file alla lista di quelli che non si analizzano.
- **Elimina file:** questa opzione permette di eliminare un file dalla lista di file che non si analizzano.
- **Estensioni:** in questa scheda si mostra una lista delle estensioni che non si devono analizzare. Anche se alcune di queste estensioni figurano nella lista delle estensioni da analizzare, non si analizzeranno.
- **Aggiungere estensione:** grazie a questa opzione, è possibile aggiungere un'estensione alla lista di estensioni non analizzabili.
- **Eliminare estensione:** grazie a questa opzione, è possibile eliminare un'estensione dalla lista delle estensioni che non si analizzano.

Risultati

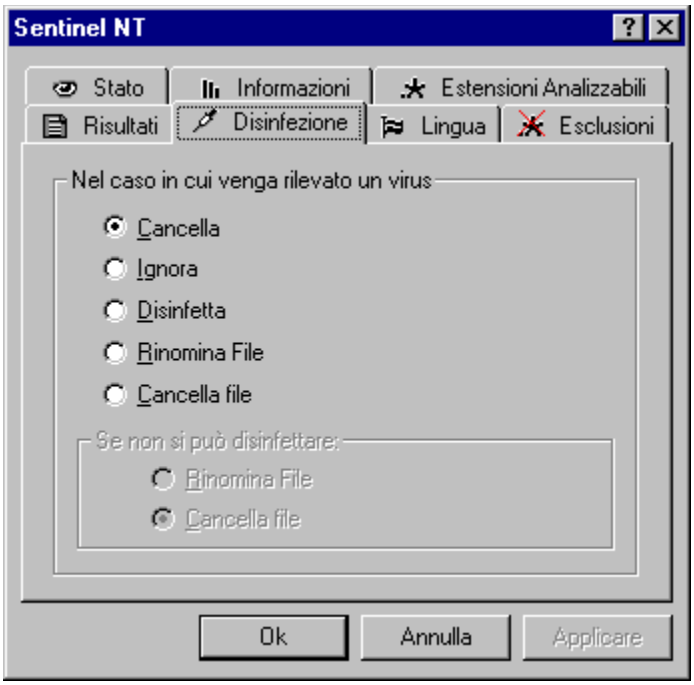
In questa scheda si configura il comportamento del sistema di rapporti sulle incidenze riscontrate dalla protezione permanente.



- **Crea rapporto locale:** se si attiva questa opzione, si creerà un rapporto con le diverse incidenze trovate dalla protezione permanente.
- **Utente:** mostra il nome dell'utente del computer.
- **Visualizza rapporto:** mostra il rapporto con le incidenze riscontrate fino a quel momento.
- **Stampa rapporto:** con questo pulsante si può stampare il rapporto sulle incidenze.
- **Cancella rapporto:** con questo pulsante si può cancellare il rapporto delle incidenze.

Disinfezione

In questa scheda si configura il comportamento della disinfezione di file contaminati da virus e individuati dalla protezione permanente.

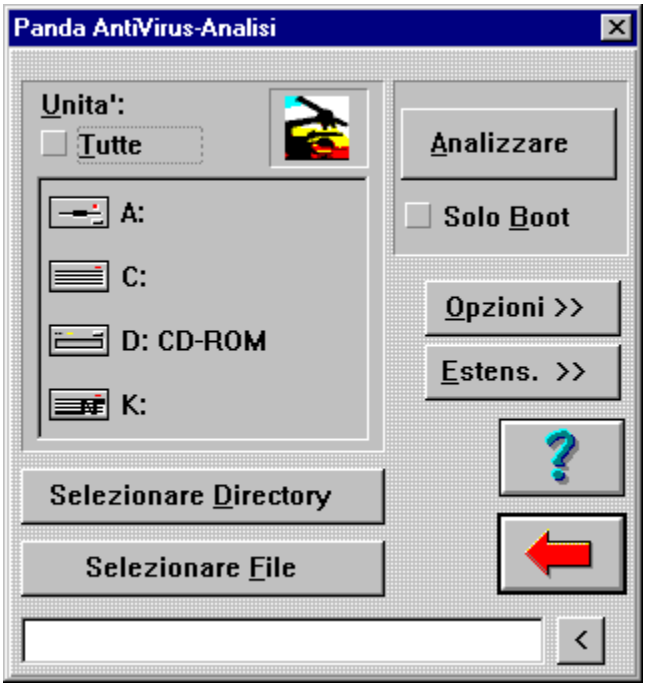


- **Annulla:** se si seleziona questa opzione, l'operazione in cui è stato individuato il virus verrà annullata. Se, per esempio, il virus è stato individuato in un file che si cercava di eseguire, verrà annullata la esecuzione del file in questione.
- **Ignora:** se questa opzione è selezionata, anche se viene trovato un virus il fatto viene ignorato.
- **Disinfetta:** se si seleziona questa opzione e la protezione permanente individua un virus, si procederà alla sua disinfezione lasciando il file in questione esattamente com'era prima di essere contaminato.
- **Rinomina file:** con questa opzione selezionata, se si individua un virus, **Sentinel** rinominerà il file con l'estensione VIR.
- **Cancella file:** se si seleziona questa opzione y **Sentinel** trova un virus in un file, si procederà a cancellare il file.
- **Se non si può disinfettare, rinomina file:** se questa opzione è attiva, quando **Sentinel** trova un virus e cerca invano di disinfettarlo, il file viene rinominato.
- **Se non si può disinfettare, cancella file:** se questa opzione è attiva, quando **Sentinel** trova un virus e cerca invano di disinfettarlo, il file viene cancellato.

Cos’è l’analisi su richiesta

L’analisi su richiesta permette di analizzare qualsiasi area del computer al momento desiderato. Ogni analisi realizzata può essere configurata grazie a una serie di semplici opzioni.

Come utilizzare l'analisi su richiesta



Per effettuare un'analisi su richiesta è necessario realizzare i seguenti passaggi:

1. **Eseguire l'antivirus:** per eseguire l'antivirus è necessario recarsi nel gruppo di programmi in cui sono state create le icone che permettono che venga eseguito. Fare doppio clic sull'icona *Panda Antivirus*.
2. **Recarsi alla sezione di analisi:** per entrare in tale sezione, premere il pulsante *Analizza* nella barra dei pulsanti dell'applicazione. Verrà visualizzata una finestra in cui bisognerà indicare cosa si vuole analizzare e le modalità di tale operazione.
3. **Scegliere l'area di analisi:** è necessario scegliere l'area che si desidera analizzare. In una lista vengono visualizzate le varie unità riconosciute dal sistema. È possibile inoltre specificare una directory o un file concreto mediante gli appositi pulsanti.
4. **Configurare le estensioni:** questo passaggio è facoltativo. Il programma salva la configurazione delle estensioni che si desidera analizzare. Pertanto, una volta configurate, non è necessario ripetere la configurazione ad ogni analisi.
5. **Configurare le opzioni di analisi:** anche questo passaggio è facoltativo. Il programma salva la configurazione delle opzioni di analisi. Pertanto, una volta configurate, non è necessario ripetere la configurazione ad ogni analisi. Tale configurazione dovrà essere modificata solo se si vorrà scegliere un insieme di opzioni diverse. In questo stesso documento, nella sezione dedicata alla configurazione, è presente una spiegazione più dettagliata delle opzioni di analisi.
6. **Specificare se si desidera analizzare solo il boot:** questo passaggio è facoltativo. Se si seleziona questa opzione verrà analizzato solo il boot e non i file delle unità specificate. Se non si seleziona questa opzione, verranno analizzati sia il boot che i file di tutte le unità specificate.
7. **Iniziare l'analisi:** il pulsante *Analizza* dà inizio all'analisi per individuare i virus nelle aree selezionate e con le opzioni prescelte.

Come si configura l'analisi su richiesta

Come si è precedentemente specificato, in un'analisi è necessario indicare:

- Che area si desidera analizzare.
- Quali estensioni vengono considerate nell'analisi.
- Come verrà effettuata l'analisi.

La configurazione di un'analisi implica la specificazione di quali estensioni verranno considerate e le opzioni di analisi.

Estensioni

Premendo il pulsante *Estensioni* viene visualizzata una finestra che permette di specificare quali estensioni si desidera analizzare.

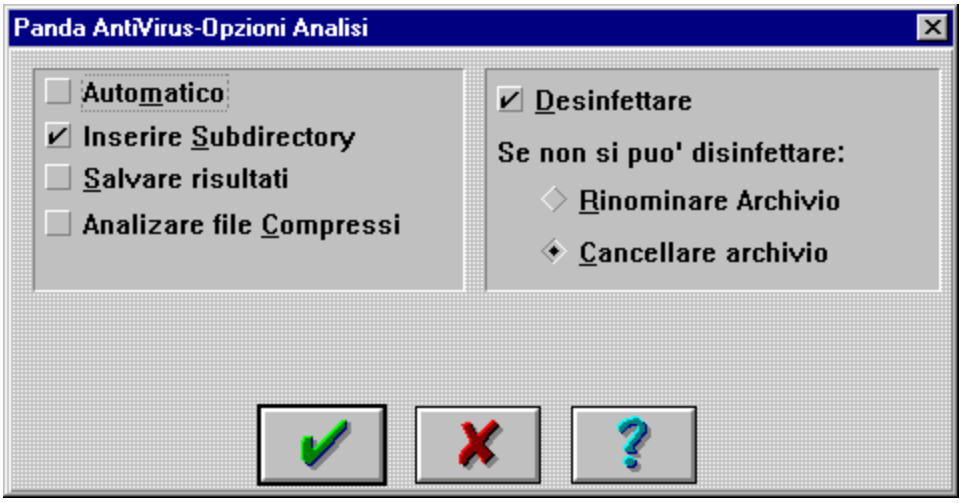
L'opzione *Tutte* nella lista delle estensioni sta a indicare che verranno analizzati tutti i file indipendentemente dalla loro estensione. Se questa opzione non è selezionata, verranno analizzati unicamente i file la cui estensione coincide con una di quelle della lista.

Due pulsanti permettono di aggiungere e eliminare estensioni nella lista. Secondo i parametri predefiniti, viene fornita una lista con le estensioni più comuni e una selezione delle estensioni in cui potrebbero risiedere dei virus.

Indipendentemente dalla selezione delle estensioni effettuata, i file EXE e COM verranno sempre analizzati.

Opzioni di analisi

Premendo il pulsante *Opzioni* appare una finestra che permette di scegliere le opzioni di analisi, che sono le seguenti:



- **Automatico:** se si seleziona questa opzione, il processo di analisi sarà completamente automatico. Se vengono individuati dei virus, il processo in corso ne darà informazione ma continuerà senza interruzione. Ciò è particolarmente utile quando il computer ha vari file infetti e sono in processo di disinfezione.
- **Entra nelle subdirectory:** se si seleziona questa opzione, verranno analizzate le subdirectory trovate nelle aree che vengono analizzate. Se non si seleziona tale opzione, non verranno analizzate le subdirectory trovate, per cui se si sceglie di analizzare un'unità ma non si seleziona questa opzione, verrà analizzata solamente la directory superiore alla stessa.
- **Registra i risultati:** se si seleziona questa opzione, i dati relativi all'analisi in questione verranno registrati nel file dei risultati.
- **Analizza compressi:** se si seleziona questa opzione, verranno analizzati i file compressi che vengono trovati.
- **Disinfetta:** se si seleziona questa opzione e si individua un virus, l'antivirus cercherà di disinfettarlo.
- **Se non è possibile disinfettare, rinomina:** se si seleziona questa opzione e si individua un virus che l'antivirus non può disinfettare, verrà rinominato il file in questione.
- **Se non è possibile disinfettare, cancella:** se si seleziona questa opzione e si individua un virus che l'antivirus non può disinfettare, verrà cancellato il file in questione.

Cos’é l’analisi euristica

L’analisi euristica è una tecnica di analisi aggiuntiva appositamente concepita per individuare virus sconosciuti.

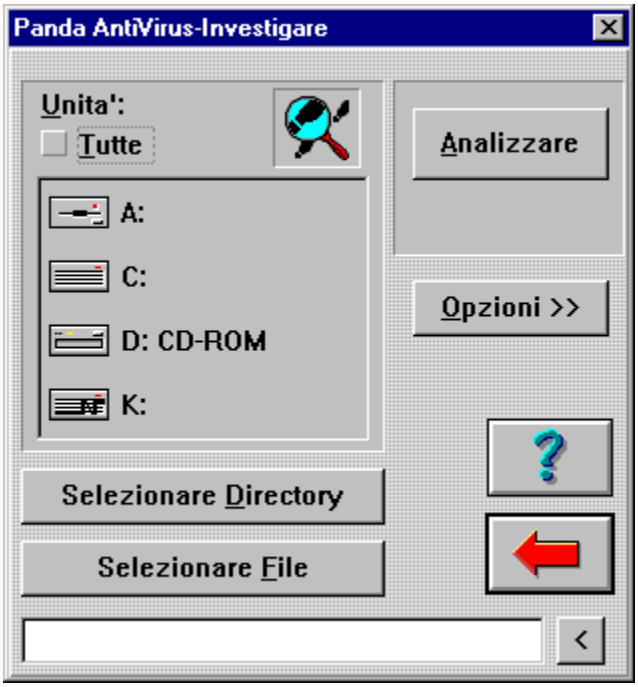
Allo stesso modo dell’analisi su richiesta, l’analisi euristica è immediata e su richiesta dell’utente. Il metodo di analisi su cui si basa l’analisi euristica è completamente diverso dal metodo di analisi su richiesta. Quest’ultimo si basa sul tentativo di trovare uno dei virus che l’antivirus conosce, mentre l’euristica cerca di stabilire se esiste un virus basandosi su caratteristiche generali comuni alla maggioranza dei virus.

Dal momento che l’analisi euristica può solo stabilire che un file è probabilmente infetto da un virus e che non si dispone di informazioni sufficienti relative al presunto virus, non è possibile eliminare tali presunti virus individuati dall’analisi euristica.

È importante tener presente che l’analisi euristica è una parte complementare dell’analisi su richiesta.

Il funzionamento dell’analisi euristica è simile a quella dell’analisi su richiesta.

Come si usa l'analisi euristica



Per effettuare un'analisi euristica è necessario realizzare i seguenti passaggi:

1. **Eseguire l'antivirus:** per eseguire l'antivirus, recarsi al gruppo di programmi in cui sono state create le icone che permettono tale operazione. Fare doppio clic sull'icona *Panda Antivirus*.
2. **Recarsi alla sezione dell'analisi euristica:** per recarsi in tale sezione, premere il pulsante *Ricerca* nelle barra dei pulsanti dell'applicazione. Apparirà una finestra in cui è possibile specificare cosa si deve analizzare con il metodo euristico e le modalità di tale operazione.
3. **Scegliere l'area di analisi:** è necessario scegliere l'area che si desidera analizzare. In una lista vengono visualizzate le varie unità riconosciute dal sistema. È possibile inoltre specificare una directory o un file concreti mediante gli appositi pulsanti.
4. **Configurare le opzioni dell'analisi euristica:** questo passaggio è facoltativo. Il programma salva la configurazione delle opzioni dell'analisi euristica. Pertanto, una volta configurata l'analisi euristica, non è necessario ripetere la configurazione ad ogni analisi di questo tipo. Tale configurazione dovrà essere modificata solo se si vorrà scegliere un insieme di opzioni diverse. In questo stesso documento, nella sezione dedicata alla configurazione, figura una spiegazione più dettagliata delle opzioni dell'analisi euristica.
5. **Iniziare l'analisi:** il pulsante *Analizza* dà inizio all'analisi euristica per individuare i virus nelle aree selezionate e con le opzioni prescelte.

Come configurare l'analisi euristica

Come precedentemente specificato, in un'analisi euristica è necessario indicare:

- Quale area si desidera analizzare mediante questo metodo.
- Come verrà realizzata tale analisi.

La configurazione di un'analisi euristica si basa sulle opzioni di tale tipo di analisi.

Opzioni di analisi

Premendo il pulsante *Opzioni* appare una finestra che permette di scegliere le opzioni di analisi euristica che sono le seguenti:

- **Sensibilità minima:** se si seleziona questa opzione, la sensibilità dell'analisi euristica sarà bassa e in questo modo si farà sì che vengano indicati come potenziali file infetti solo quelli in cui il sospetto circa la presenza di un virus è particolarmente elevato.
- **Sensibilità media:** se si seleziona questa opzione, l'analisi euristica verrà realizzata con una sensibilità media. In tal modo, verranno indicati come sospetti solo quei file che hanno una certa possibilità di essere infetti.
- **Sensibilità massima:** se si seleziona questa opzione, la sensibilità dell'analisi euristica sarà massima e indicherà come sospetti di infezione tutti quei file in cui si individui la benché minima possibilità di infezione. Ciononostante, la possibilità che un file non infetto venga considerato sospetto anche a questo livello è minima.
- **Informare circa data e ora inesatte:** se si seleziona questa opzione, apparirà un avviso ogni volta che viene individuato un file con una data o ora inesatta.
- **Informare circa file compressi:** se si seleziona questa opzione apparirà un avviso ogni volta che venga individuato un file compresso.
- **Informare circa file vaccinati:** se si seleziona questa opzione apparirà un avviso ogni volta che venga individuato un file vaccinato.

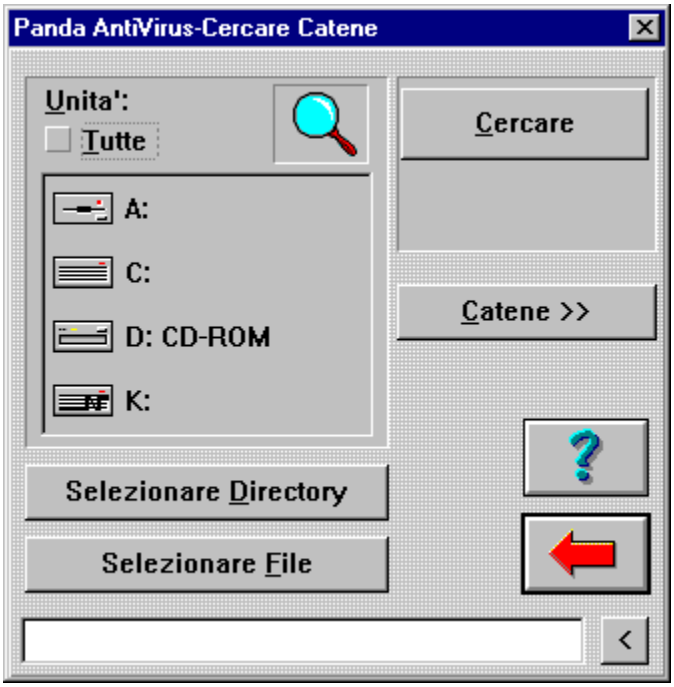
Cos'è la ricerca di catene

L'analisi su richiesta si basa sulla ricerca all'interno dei file di parti dei virus che l'antivirus conosce. Dal momento che ogni giorno sorgono nuovi virus, l'analisi su richiesta incomincia a diventare poco a poco obsoleta.

Nella ricerca di catene si usa lo stesso metodo dell'analisi su richiesta, ma è possibile indicare una catena (parte di un virus) affinché venga ricercata. In tal modo, il servizio di assistenza al cliente di **Panda Software** può indicare una catena corrispondente a un nuovo virus in modo che l'antivirus la individui nonostante sia privo di informazioni relative a tale virus nel suo interno.

Come nell'analisi su richiesta, la ricerca di catene è immediata e su richiesta dell'utente.

Come si usa la ricerca di catene



Per effettuare una ricerca di catene, è necessario realizzare i seguenti passaggi:

1. **Eseguire l'antivirus:** per eseguire l'antivirus, recarsi nel gruppo di programmi in cui sono state create le icone che permettono tale operazione. Fare doppio clic sull'icona *Panda Antivirus*.
2. **Recarsi alla sezione della ricerca di catene:** per recarsi in tale sezione, premere il pulsante *Ricerca* nelle barra dei pulsanti dell'applicazione. Apparirà una finestra in cui è possibile specificare cosa si deve analizzare con la ricerca di catene e le modalità di tale operazione.
3. **Scegliere l'area in cui verrà effettuata la ricerca:** è necessario scegliere l'area in cui si desidera effettuare la ricerca. In una lista vengono visualizzate le varie unità riconosciute dal sistema. È possibile inoltre specificare una directory o un file concreti mediante gli appositi pulsanti.
4. **Indicare le catene che si devono cercare:** è necessario scrivere le catene che l'antivirus deve cercare o scegliere catene già inserite da una lista. Dal momento che il programma salva le catene che sono state inserite in altre occasioni, se non si desidera aggiungere nessuna nuova catena non è necessario effettuare questo passaggio.
5. **Iniziare la ricerca:** il pulsante *Cerca* dà inizio alla ricerca delle catene indicate nelle aree selezionate.

Come si configura la ricerca di catene

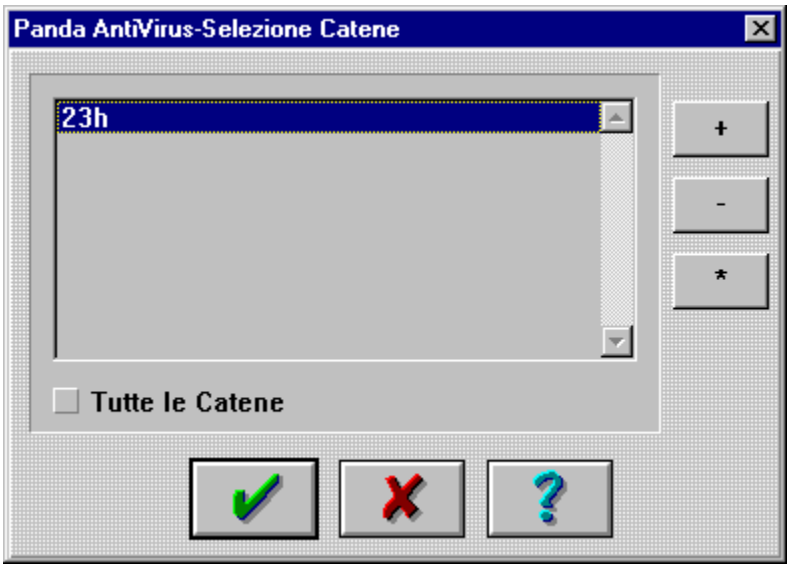
Come precedentemente specificato, in una ricerca di catene è necessario indicare:

- Quale area si desidera analizzare con questo metodo.
- Quali catene si desidera cercare.

La configurazione di una ricerca di catene si basa sulle catene che si devono cercare.

Catene

Premendo il pulsante *Catene* appare una finestra che permette di scegliere le catene che verranno cercate.



In tale finestra viene visualizzata una lista di catene inserite. Mediante uno degli appositi pulsanti è possibile aggiungere una catena in tale lista, modificare una delle catene inserite o eliminare una catena dalla lista.

Non verranno cercate tutte le catene indicate nella lista a meno che non venga selezionata l'opzione *Tutte le catene*. Se tale opzione non è selezionata, verranno cercate solo le catene selezionate nella lista.

Come disinfettare con Panda Antivirus

Non esiste una sezione specifica di disinfezione in **Panda Antivirus**. La disinfezione è associata all'analisi su richiesta o alla protezione permanente. Se l'analisi su richiesta o la protezione permanente trovano un virus, cercheranno di disinfettarlo (se così è indicato nella configurazione delle opzioni di queste due sezioni).

La configurazione della disinfezione permette di indicare che vengano cancellati o rinominati tutti quei file contaminati che non si possono disinfettare.

Un virus può risiedere nel boot di un disco o nei file. A seconda dei casi, è necessario procedere in modo leggermente diverso. Consultare le sezioni corrispondenti per ottenere una procedura di disinfezione dettagliata.

Disinfezione di un virus di boot

Divisione FAT

Per disinfettare un virus di boot dell'unità C, è necessario eseguire i seguenti passaggi:

1. Spegnere il computer. Inserire un disco di avvio privo di virus (se la disinfezione verrà effettuata mediante CD-Rom, il disco dovrà caricare i driver del CD) e riavviare il computer.
2. Una volta avviato, eseguire il nostro antivirus dalla riga di comando (PAVCL) attenendosi alle seguenti indicazioni:

   - Se si desidera eseguire **Pavcl** da un disco, inserire il disco 1 di **Panda Antivirus** per DOS/Windows 3.1x e scrivere quanto segue:

     ```
     PAVCL C: /CLV
     ```

   - Se si desidera eseguire **Pavcl** dal nostro CD-Rom, inserirlo nell'unità di lettura, collocarsi nella directory DOSWIN3X e nella lingua desiderata e scrivere quanto segue:

     ```
     PAVCL C: /CLV
     ```

     Se in una qualunque delle due situazioni appare un messaggio in cui si dice che l'unità selezionata non è valida, scrivere quanto segue:

     ```
     PAVCL /HD0 /CLV
     ```

Divisione NTFS

Per disinfettare un virus di boot basandosi su una divisione NTFS, è importante sapere se il virus ha attaccato il master boot, il boot o entrambi. Nel caso in cui il virus abbia attaccato solo il master boot, sarà valida la procedura indicata per divisioni FAT.

Se il virus ha attaccato il boot, si elimina il virus sostituendo il boot con un boot generico mediante uno qualsiasi degli strumenti che Windows NT fornisce a tale scopo.

Disinfezione di un virus presente in file

Se è stato individuato un virus nei file, è necessario realizzare la pulizia del sistema configurando l'antivirus nel seguente modo:

- In *Opzioni di analisi* attivare *Tutte le estensioni*, *Disinfetta* e *Analisi Automatica*.
- Recarsi alla sezione di analisi e scegliere l'opzione che corrisponde all'analisi di tutto il sistema (tutte le unità). Mano a mano che si realizza l'analisi verranno puliti i file infetti.

Disinfezione mediante la protezione permanente

Sentinel è in grado di disinfettare i virus che trova. Se **Sentinel** individua un virus ed è configurato per disinfettarlo, lo disinfetterà prima che venga realizzata l'operazione in corso e, una volta disinfettato, continuerà l'operazione in cui è stato trovato il virus. **Sentinel** visualizza sempre una finestra che indica l'individuazione del virus.

Analisi nella riga di comando

Panda Antivirus è dotato di un programma chiamato **Pavcl** che viene eseguito dalla riga di comando di MS-DOS. Il nostro programma di analisi dalla riga di comando individua e disinfetta gli stessi virus di qualsiasi altra versione di **Panda Antivirus**.

Pavcl è un programma di analisi rapida che occupa poca memoria, tuttavia per utilizzarlo è necessario avere una minima conoscenza dei parametri che accetta. **Pavcl** è disponibile nel disco numero 1 della versione DOS/Windows 3.1x o nella directory della lingua corrispondente all'interno della directory DOSWIN3X nel CD-Rom.

Parametri di Pavcl

Azioni

`/NOM` Non analizzare la memoria.

`/NOB` Non analizzare il sistema di avvio BOOT.

`/NOF` Non analizzare i file.

`/ALL` Analizzare tutte le unità del sistema.

`/INVx` Ricercare nell'unità "x" per individuare virus sconosciuti.
Esempio: `/INVA` ricerca nell'unità A:.

`/CLV` Eliminare i virus individuati.

`/LIS` Elencare i virus compresi in questa versione.

`/HEU` Attivare metodo di individuazione Euristico.

`/CMP` Analizzare compressi.

`/CDR` Mostra i codici di ritorno di **Pavcl**.

`/SAV` Salvare i parametri in un file. Le prossime volte che verrà eseguito aggiungerà questi parametri a quelli inseriti in ogni sessione.

`/IB+` Aggiungere vaccino Interno al BOOT.
`/IB-` Eliminare vaccino Interno al BOOT.
`/IB*` Verificare vaccino Interno del BOOT.

`/EB+` Aggiungere vaccino Esterno al BOOT.

/EB- Eliminare vaccino Esterno al BOOT.
/EB* Verificare vaccino Esterno del BOOT.

/IF+ Aggiungere vaccino Interno a un File.
/IF- Eliminare vaccino Interno a un File.
/IF* Verificare vaccino Interno di un File.

/EF+ Aggiungere vaccino Esterno a un File.
/EF- Eliminare vaccino Esterno a un File.
/EF* Verificare vaccino Esterno di un File.

/B+ Aggiungere vaccino Interno e Esterno al BOOT.
/B- Eliminare vaccino Interno e Esterno al BOOT.
/B* Verificare vaccino Interno e Esterno del BOOT.

/F+ Aggiungere vaccino Interno e Esterno a un File.
/F- Eliminare vaccino Interno e Esterno di un File.
/F* Verificare vaccino Interno e Esterno di un File.

Modificatori

/NSB Non analizzare le subdirectory di livello inferiore.

/PTH Analizzare le directory contenute nella variabile PATH del DOS.

/ISO Attivare il metodo di isolamento.

/NOS Disattivare il suono.

/AEX Analizzare tutti i File, indipendentemente dalla loro estensione.

/AUT Esplorazione senza l'intervento dell'utente.

/OVR Sovrascrivere prima di cancellare.

/NOR Non produrre File dei risultati.

/DEL Cancella i File infetti anche se si possono disinfettare.

/LOC Analizza tutte le unità locali.

/NBR Non permette di annullare il processo di analisi.

/ITW **Pavcl** effettuerà l'analisi solo per individuare i virus *In The Wild*. Questo parametro deve

essere utilizzato unicamente in condizioni particolari.

È dotato inoltre dello switch "/?" standardizzato nel DOS, per accedere a una lista degli switch disponibili. In questa vengono inclusi anche quelli corrispondenti alle lingue supportate dalla versione di **Pavcl**.

Le azioni predeterminate sono:

- Analizzare Memoria.
- Analizzare Boot.
- Analizzare File.

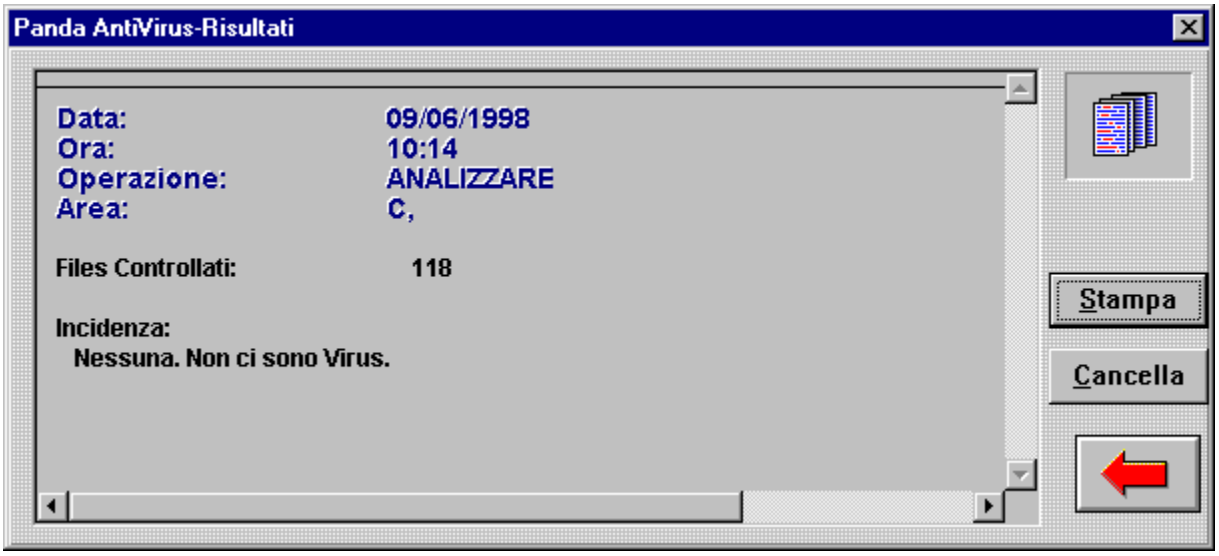
e i modificatori predeterminati sono:

- Analizzare subdirectory.
- Non disinfettare.
- Effetti sonori attivati.
- Analizzare solo le estensioni eseguibili.
- Produrre File dei risultati.

Le azioni /?, /LIS, /INVx sono esclusive, vale a dire, quando sono selezionate nessun'altra azione può essere eseguita. Una volta terminate si torna al DOS. Il percorso o percorsi che si desidera analizzare vengono indicati secondo la tipica modalità del DOS:

[Unità:][Percorso][NomeFile]

Rapporto risultati



Il rapporto risultati archivia le diverse operazioni realizzate con l'antivirus nonché le diverse incidenze che si verificano.

L'informazione contenuta nel rapporto risultati si archivia ad ogni sessione. È quindi utile per consultare, in qualsiasi momento, l'attività svolta dall'antivirus.

Per ogni operazione realizzata si archiviano i seguenti dati:

- Data e ora.
- Tipo di operazione.
- Area su cui l'operazione è stata realizzata.
- Numero di file revisionati.
- Tutte le incidenze verificatesi in relazione ai virus.

Per raccogliere i dati nel rapporto risultati è necessario attivare l'opzione *Registrare risultati* nella finestra *Opzioni di Analisi*.

Il contenuto del rapporto risultati si può stampare per agevolarne la consultazione. Si può anche cancellare il contenuto del rapporto risultati in qualsiasi momento per evitare che acquisisca dimensioni eccessive.

Lista dei virus

La lista dei virus presenta una lista con i virus che **Panda Antivirus** è capace di individuare. Nella lista dei virus si indicano i nomi e le dimensioni di ogni virus.

Assieme alla lista, si indica il numero di virus riconosciuti in quella versione di **Panda Antivirus**. Si indica anche la data del file di virus per sapere in che misura l'antivirus è aggiornato.

Si può indicare il nome di un virus nell'apposito spazio per trovare un virus in particolare con maggior facilità. Allo stesso scopo, la lista dei virus si presenta in ordine alfabetico.

Una volta scelto un virus, se si preme il pulsante *Info*, appare una finestra con una serie di dati di interesse:

- Nome.
- Origine.
- Dimensioni.
- Alias.
- data in cui è stato individuato per la prima volta.
- Possibilità o meno di disinfettarlo.
- Aree del computer che possono essere colpite dal virus.
- Caratteristiche di comportamento del virus.

Di seguito si dà una spiegazione sulle diverse caratteristiche che può presentare un virus:

- **Residente:** quando si esegue, il virus riserva una piccola parte della memoria e si installa in essa per propagarsi da lì.
- **Stealth:** è una tecnica che usano alcuni virus residenti. Consiste nel mimetizzare i cambiamenti che il virus effettua sui file che colpisce. Quando si cerca di verificare una delle caratteristiche del file che il virus ha modificato, il virus, che è residente in memoria, intercetta la consultazione ed offre i dati anteriori alla modifica.
- **Criptati:** i virus che possiedono questa caratteristica sono capaci di criptarsi in un modo differente ogniqualvolta infettano un file. Risulta così impossibile cercare il virus mediante una catena.
- **Sovrascrittura:** i virus di sovrascrittura, che possono essere residenti o no, sovrascrivono il file che infettano, che diventa perciò inservibile. Le dimensioni del file non variano, a meno che le dimensioni del virus siano maggiori di quelle del file. L'unica maniera di eliminare questi virus è quella di cancellare il file infetto e di sostituirlo con una copia non infetta.
- **Polimorfici:** i virus polimorfici sono delle versioni avanzate dei virus criptati. I polimorfici sono capaci di criptarsi in modo sempre diverso di generazione in generazione. In tal modo non c'è nessuna parte del virus che rimanga inalterata.

Funzionamento generale

Panda Antivirus per Windows NT offre una comoda interface di facile utilizzo. Nella finestra principale del programma, le opzioni più comuni sono disponibili mediante dei pulsanti di grandi dimensioni.

Premendo questi pulsanti si accede alle varie parti del programma. Fare riferimento alla sezione corrispondente per ottenere una spiegazione dettagliata sul funzionamento.