VirusScan per Windows 3.1*x*

Manuale dell'utente

Network Associates
Italy
Centro Direzionale Summit
Palazzo D/1
Via Brescia 38
20063 Cermusco sul Naviglio
Milano
Italy

COPYRIGHT

CONTRATTO DI LICENZA

A TUTTI GLI UTENTI: SI INVITANO GLI UTENTI A LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO LEGALE ("CONTRATTO"), CHE RIPORTA I TERMINI GENERALI DI LICENZA PER IL SOFTWARE NETWORK ASSOCIATES. PER I TERMINI SPECIFICI DELLA PROPRIA LICENZA, CONSULTARE IL DOCUMENTO README.1ST, LICENZA.TXT O ALTRA LICENZA CHE ACCOMPAGNA IL SOFTWARE COME FILE DI TESTO O COME PARTE DELLA CONFEZIONE DEL SOFTWARE STESSO. Qualora l'utente non accetti i termini del presente Contratto, NON DOVRÀ INSTALLARE IL SOFTWARE. (L'UTENTE POTRÀ EVENTUALMENTE RESTITUIRE IL PRODOTTO AL RIVENDITORE E OTTENERE IL RIMBORSO DEL PREZZO.)

1. **Concessione di licenza.** Previo pagamento delle quote di licenza richieste e nel rispetto delle condizioni e clausole del presente Contratto, Network Associates concede all'utente un diritto non esclusivo e non trasferibile all'uso di una copia della versione specificata del Software e della documentazione di accompagnamento (la "Documentazione"). La copia del Software può essere installata su computer, workstation, portatili, cercapersone, "telefoni intelligenti" o altri dispositivi elettronici per i quali il Software è stato progettato (le "periferiche client"). Se il Software è concesso in licenza all'interno di un insieme di prodotti o unitamente a più di un prodotto Software, la presente licenza si applica a tutti i prodotti Software soggetti ai vincoli o ai termini di utilizzo specificati per ogni singolo Software nella fattura o sulla confezione del prodotto.

   a. **Utilizzo.** Il Software è concesso in licenza come singolo prodotto; non può essere usato su più periferiche client o da più utenti contemporaneamente, fatta eccezione per quanto riportato nella presente Sezione 1. Il Software si intende "in uso" su di un computer quando esso è caricato sulla memoria temporanea (ossia RAM) o installato sulla memoria permanente (ad esempio su disco rigido, CD-ROM o altro dispositivo di memorizzazione) di quella periferica client. La presente licenza autorizza l'utente a produrre una copia del Software esclusivamente come copia di riserva e per scopi d'archivio, purché tale copia contenga tutte le informazioni relative al proprietario.

   b. **Utilizzo del server.**Conformemente a quanto specificato nella fattura o nella confezione del prodotto, è consentito installare e utilizzare il Software su una periferica client o su un server ("Server") all'interno di un ambiente per più utenti o di una rete ("Utilizzo del server") per (i) la connessione, diretta o indiretta, ad un numero di periferiche client o "postazioni" specificate che non superi il massimo consentito; oppure per (ii) la distribuzione di un numero di agenti (poller) che non superi il massimo specificato per la distribuzione. Se la fattura o la confezione del prodotto non specificano un massimo numero di periferiche client o poller, la presente licenza fornisce il permesso per l'uso di un singolo prodotto, conformemente a quanto previsto dalla precedente sottosezione (a). Un'apposita licenza è richiesta per ciascuna periferica client o postazione che può connettersi al Software in qualsiasi momento, indipendentemente dal fatto che le suddette periferiche client o postazioni dotate di licenza siano connesse al Software contemporaneamente o usino effettivamente il Software in ogni momento.

L’uso da parte dell’acquirente di software o hardware che riducono il numero di periferiche client o postazioni che si connettono al Software e lo utilizzano simultaneamente (ad esempio hardware e software "multiplexing" o "pooling") non riduce il numero totale di licenze che è necessario possedere. In particolare è necessario possedere un numero di licenze pari al numero di distinti input dati al software o all'hardware multiplexing o pooling "front end". Se il numero di periferiche client o postazioni che possono connettersi al Software può eccedere il numero di licenze acquistate, è necessario predisporre un valido meccanismo in grado di assicurare che l'uso del Software non ecceda i limiti di utilizzo specificati nella fattura o sulla confezione del prodotto. La presente licenza autorizza l'utente a creare o scaricare una copia della Documentazione per ogni periferica client o postazione dotata di licenza, purché ogni copia contenga tutte le informazioni relative al proprietario per la Documentazione.

c. **Utilizzo del volume.** Se il Software è concesso in licenza in base ai termini di utilizzo del volume specificati nella fattura o sulla confezione, è consentito produrre, utilizzare e installare tutte le copie addizionali del Software necessarie per le periferiche client specificate nei termini di utilizzo del volume. La presente licenza autorizza l'utente a produrre o scaricare una copia della Documentazione per ognuna delle copie del Software consentite dai termini di utilizzo del volume, purché ciascuna di esse contenga tutte le informazioni relative al proprietario per la Documentazione. è obbligatorio predisporre un valido meccanismo in grado di assicurare che il numero di periferiche client su cui il Software è installato non ecceda il numero di licenze acquistate.

2. **Risoluzione.** La presente licenza è valida per il periodo di tempo specificato nella fattura o sulla confezione del prodotto, oppure nel file README.1ST, LICENZA.TXT, o in altri file di testo che accompagnano il Software e hanno lo scopo di definire i termini del contratto di licenza. Dove le disposizioni del Contratto qui indicate entrano in conflitto con le disposizioni riportate nella fattura o sulla confezione del prodotto, il documento README.1ST, il documento LICENZA.TXT, la fattura, la confezione del prodotto o altri documenti di testo costituiranno i termini della licenza d'uso del Software. Sia l'utente, sia Network Associates possono sospendere la licenza prima del termine specificato nell'apposito documento e secondo i termini in esso indicati. Il presente Contratto e la licenza si ritengono automaticamente decaduti qualora l'utente non rispettasse uno qualsiasi dei limiti o delle altre richieste in esso descritte. Alla risoluzione del presente contratto, l'utente è tenuto a distruggere tutte le copie del Software e della Documentazione in suo possesso. L'utente può risolvere il presente Contratto in qualsiasi momento distruggendo il Software e la Documentazione, oltre a tutte le copie in suo possesso.

3. **Aggiornamenti.** Durante il periodo di validità della licenza, l'utente ha il diritto di scaricare revisioni, perfezionamenti e aggiornamenti del Software, quando Network Associates li pubblica sui propri servizi elettronici, siti Web o altri servizi in linea.

4. **Diritti di proprietà.** Il Software e la Documentazione sono protetti dalle leggi degli Stati Uniti e dagli accordi internazionali sul copyright. Network Associates possiede e mantiene pienamente qualsivoglia diritto, titolo e interesse relativamente al Software, inclusi tutti i diritti di copyright, brevetti, diritti al segreto commerciale, marchi commerciali e altri diritti di proprietà intellettuale connessi. L'utente riconosce che il possesso, l'installazione e l'uso del Software non trasferiscono alla sua persona la proprietà intellettuale del Software e che egli non acquisirà alcun diritto al Software, fatta eccezione per quanto espressamente stabilito dal presente Contratto. L'utente accetta che ogni copia del Software e della Documentazione conterrà le stesse informazioni relative al proprietario che appaiono nel Software e nella Documentazione.

5. **Restrizioni.** Non è consentito affittare, noleggiare, prestare o rivendere il Software e neppure consentire a terze parti il beneficio dell'uso o delle funzionalità del Software condividendolo o consentendone l'uso attraverso servizi di alcun tipo o altri accordi. Non è consentito trasferire nessuno dei diritti che il presente contratto attribuisce all'utente. Non è consentito copiare la Documentazione del Software. Non è consentito elaborare, decompilare o disassemblare il Software, fatta eccezione per quanto consentito dalla legge in vigore. Non è consentito modificare o creare lavori derivati, basati sul Software integralmente o in parte. Non è consentito copiare il Software, fatta eccezione per i casi espressamente consentiti dalla Sezione 1 di cui sopra. Non è consentito rimuovere etichette o altre indicazioni relative al proprietario presenti sul Software. Tutti i diritti non espressamente elencati qui di seguito devono essere accordati da Network Associates. Network Associates si riserva il diritto di condurre controlli periodici, previo preavviso scritto, per verificare che vengano rispettati i termini del contratto di licenza.

6. **Garanzia ed esclusione di garanzia**

   a. **Garanzia limitata.** Network Associates garantisce che, per trenta (30) giorni dalla data dell'acquisto o della distribuzione originale, il supporto (ad esempio i dischetti) su cui il Software è registrato sarà privo di difetti di materiale e di fabbricazione.

   b. **Tutela del cliente.** La responsabilità di Network Associates e dei suoi fornitori, e unica forma di tutela per i clienti, sarà limitata, a discrezione di Network Associates, (i) alla restituzione dell'eventuale prezzo di acquisto pagato per la licenza oppure (ii) alla sostituzione del supporto difettoso su cui il Software è registrato con una copia non difettosa. Il supporto difettoso dovrà essere restituito a Network Associates dall'acquirente a proprie spese, unitamente a una copia della ricevuta d'acquisto. La presente garanzia limitata è nulla se il difetto è dovuto a incidente, abuso o uso erroneo. Qualsiasi supporto sostitutivo è garantito fino al completamento del periodo di garanzia iniziato con il precedente Software. Fuori dal territorio degli Stati Uniti il presente diritto non è garantito, date le restrizioni cui Network Associates è soggetta in materia di esportazione.

   Esclusione di garanzia. Conformemente a quanto consentito dalle leggi vigenti e fatta eccezione per la garanzia limitata di cui sopra, IL SOFTWARE è FORNITO TALE E QUAL è, SENZA ALCUNA GARANZIA ESPRESSA O IMPLICITA. SENZA ALCUN LIMITE ALLE SUDDETTE DISPOSIZIONI, L'ACQUIRENTE ASSUME LA PIENA RESPONSABILITà PER LA SCELTA DEL SOFTWARE AL FINE DI SVOLGERE DETERMINATE ATTIVITà E PER L'INSTALLAZIONE, L'USO E I RISULTATI OTTENUTI DAL SOFTWARE STESSO. SENZA ALCUN LIMITE ALLE SUDDETTE DISPOSIZIONI, NETWORK ASSOCIATES NON GARANTISCE IN ALCUN MODO CHE IL SOFTWARE SIA PRIVO DI ERRORI, INTERRUZIONI O ALTRI DIFETTI O CHE IL SOFTWARE SODDISFI LE ESIGENZE DELL'ACQUIRENTE. SECONDO QUANTO CONSENTITO DALLA LEGGE, NETWORK ASSOCIATES non riconosce alcuna altra garanzia, espressa o implicita, comprese, in via esemplificativa, la garanzia di commerciabilità ed idoneità per un fine particolare, relativamente al software e alLA DOCUMENTAZIONE di accompagnamento. L'apposizione di limiti alla garanzia implicita non è consentita in alcuni Stati o giurisdizioni; pertanto la limitazione di cui sopra potrebbe non essere applicabile. I suddetti termini saranno applicabili conformemente a quanto consentito dalle leggi vigenti.

L’acquisto o il pagamento del Software potrebbero dare all’acquirente il diritto a ulteriori garanzie che Network Associates specificherà nella fattura o sulla confezione del prodotto ricevuto con l'acquisto o nei file README.1ST, LICENZA.TXT o altri file di testo che accompagnano il Software e hanno lo scopo di stabilire i termini del contratto di licenza. Dove le disposizioni del presente Contratto entrano in conflitto con le disposizioni riportate nella fattura o sulla confezione del prodotto, nel file README.1ST, LICENZA.TXT o in simili documenti, la fattura, la confezione o il file di testo faranno fede per i termini relativi al diritto di garanzia dell'acquirente in merito al Software.

7. **Limitazione di responsabilità.** IN NESSUN CASO E CONFORMEMENTE A NESSUNA TEORIA LEGALE, ANCHE SE IN CASO DI ILLECITO CIVILE, CONTRATTO, O IN ALTRO MODO, NETWORK ASSOCIATES O I SUOI FORNITORI SARANNO RESPONSABILI VERSO L’ACQUIRENTE O QUALSIASI ALTRA PERSONA PER QUALSIVOGLIA DANNO INDIRETTO, SPECIALE, INCIDENTALE O CONSEQUENZIALE DI OGNI SORTA, INCLUSI, SENZA ALCUNA LIMITAZIONE, DANNI PER LA MANCANZA DI BUONA VOLONTÀ, SOSPESO FUNZIONAMENTO, BLOCCO DEL COMPUTER O MALFUNZIONAMENTO, E PER QUALSIASI ALTRO POSSIBILE DANNO O PERDITA. IN NESSUN CASO NETWORK ASSOCIATES POTRà ESSERE RITENUTA RESPONSABILE PER DANNI CHE SUPERINO IL PREZZO DI LISTINO APPLICATO DA NETWORK ASSOCIATES PER LA LICENZA D'USO DEL SOFTWARE, ANCHE NEL CASO IN CUI NETWORK ASSOCIATES SIA STATA AVVERTITA DELLA POSSIBILITà DI TALI DANNI. QUESTA LIMITAZIONE DI RESPONSABILITà NON SI APPLICA ALLA RESPONSABILITà PER MORTE O INFORTUNIO ALLA PERSONA, CONFORMEMENTE AL DIVIETO DI TALI LIMITAZIONI IMPOSTO DALLE LEGGI VIGENTI. INOLTRE, DATO CHE ALCUNI STATI E GIURISDIZIONI NON CONSENTONO L'ESCLUSIONE O LIMITAZIONE DEI DANNI INCIDENTALI O CONSEQUENZIALI, TALE LIMITAZIONE O ESCLUSIONE POTREBBE NON APPLICARSI A TUTTI GLI UTENTI. I suddetti termini saranno applicabili conformemente a quanto consentito dalle leggi vigenti.

8. **Governo degli Stati Uniti.** Il Software e la Documentazione di accompagnamento sono considerati rispettivamente "software commerciale per computer" e "documentazione di software commerciale per computer", conformemente al DFAR Section 227.7202 e FAR Section 12.212, quando applicabili. Qualsiasi uso, modifica, riproduzione, dimostrazione, rappresentazione o presentazione del Software e della Documentazione di accompagnamento da parte del Governo degli Stati Uniti sarà regolamentata esclusivamente dai termini del presente Contratto e sarà vietata in tutti i casi, fatta eccezione per quanto espressamente consentito dai termini del presente Contratto.

9. **Controlli di esportazione.** Né il Software né la relativa Documentazione e le informazioni o tecnologie che vi stanno alla base possono essere scaricate o esportate in altro modo o riesportate (i) negli stati di (o a cittadini o residenti degli stati di) Cuba, Iran, Iraq, Libia, Corea del Nord, Sudan, Siria o qualsiasi altro paese a cui gli Stati Uniti abbiano imposto l'embargo dei beni; o (ii) agli stati che compaiono nell'elenco Specially Designated Nations del Ministero del Tesoro degli Stati Uniti o nella Table of Denial Orders del Ministero del Commercio degli Stati Uniti. Coloro che scaricano o usano il Software aderiscono automaticamente alle suddette disposizioni e garantiscono di non essere domiciliati in nessuno di tali paesi o di trovarsi sotto il loro controllo o di non essere cittadini o residenti di nessuno di tali paesi e di non essere contemplati in nessuna delle suddette liste.

VINCOLI ALL'ESPORTAZIONE E RIESPORTAZIONE DI DETERMINATI PRODOTTI E DATI TECNICI. SE L'ESPORTAZIONE DEL SOFTWARE È CONTROLLATA DA QUESTE NORME E REGOLAMENTAZIONI, IL SOFTWARE NON VERRÀ ESPORTATO O RIESPORTATO, DIRETTAMENTE O INDIRETTAMENTE, (A) SENZA TUTTE LE LICENZE DI ESPORTAZIONE E RIESPORTAZIONE E LE APPROVAZIONI RICHIESTE DAGLI STATI UNITI O DA ALTRI GOVERNI CONFORMEMENTE ALLE LEGGI VIGENTI, O (B) IN VIOLAZIONE DI QUALSIASI DIVIETO APPLICABILE CONTRO L'ESPORTAZIONE O RIESPORTAZIONE DI QUALSIASI PARTE DEL SOFTWARE. ALCUNI PAESI IMPONGONO RESTRIZIONI ALL'USO DELLA CODIFICA ENTRO I LORO CONFINI O ALLA SUA IMPORTAZIONE O ESPORTAZIONE, ANCHE SE ESCLUSIVAMENTE PER USO TEMPORANEO E PER SCOPI PERSONALI O LAVORATIVI. L'UTENTE è CONSAPEVOLE CHE L'APPLICAZIONE DELLE SUDDETTE LEGGI NON è LA MEDESIMA IN TUTTI I PAESI. SEBBENE L'ELENCO DI PAESI CHE SEGUE NON SIA ESAURIENTE, POTREBBERO ESSERE IMPOSTI VINCOLI ALL'ESPORTAZIONE DELLA TECNOLOGIA DI CODIFICA VERSO, O ALL'IMPORTAZIONE DA: BELGIO, CINA (INCLUSA HONG KONG), FRANCIA, INDIA, INDONESIA, ISRAELE, RUSSIA, ARABIA SAUDITA, SINGAPORE E COREA DEL SUD. L'UTENTE è CONSAPEVOLE CHE è SUA RESPONSABILITà IL RISPETTO DI QUALSIASI LEGGE GOVERNATIVA DI ESPORTAZIONE E DELLE ALTRE LEGGI VIGENTI E CHE NETWORK ASSOCIATES NON È SOGGETTA A ULTERIORI RESPONSABILITà DOPO LA VENDITA INIZIALE ENTRO I CONFINI DEL PAESE DI ORIGINE.

10. **Attività ad alto rischio.** Il Software non possiede caratteristiche di fault tolerance e non è progettato o destinato all'uso in ambienti pericolosi, che richiedono prestazioni infallibili inclusi, senza limitazioni, il controllo di impianti nucleari, il pilotaggio di aeromobili o il controllo dei relativi sistemi di comunicazione, il controllo del traffico aereo, il controllo di sistemi di offesa, il controllo di macchine di ausilio alla vita o qualsiasi altra applicazione in cui errori del Software potrebbero causare direttamente la morte, l'infortunio o gravi danni fisici alla persona o alla proprietà (in generale "attività ad alto rischio"). Network Associates rifiuta espressamente di rilasciare qualsiasi garanzia espressa o implicita di attitudine del Software per attività ad alto rischio.

11. **Varie.** Il presente Contratto è regolato dalle leggi degli Stati Uniti e dello stato della California, senza riferimenti ai conflitti dei principi di legge. L'applicazione della United Nations Convention of Contracts for the International Sale of Goods è espressamente esclusa. Il Contratto qui riportato è di natura consultiva e non sostituisce le disposizioni di Contratto eventualmente riportate nei file README.1ST, LICENZA.TXT o altri file di testo che accompagnano il Software e hanno lo scopo di stabilire i termini del contratto di licenza dell'utente. Dove i termini previsti dal presente Contratto entrano in conflitto con quanto riportato nei documenti README.1ST o LICENZA.TXT, il documento di testo fa fede per i termini di concessione della licenza d'uso del Software. Il presente Contratto non può essere modificato se non per mezzo di un addendum scritto pubblicato da un rappresentante autorizzato di Network Associates. Nessun provvedimento qui riportato dovrebbe essere ritenuto privo di validità, a meno che il documento che ne fa decadere la validità non sia in forma scritta e non porti la firma di Network Associates o di un rappresentante autorizzato di Network Associates. Se uno qualsiasi dei termini previsti dal presente Contratto viene dichiarato non valido, la parte rimanente del Contratto rimarrà pienamente vincolante ed efficace. Le parti confermano che, secondo il loro desiderio, il presente Contratto è stato scritto solo in lingua inglese.

12. **Servizio clienti Network Associates.** Per qualsiasi quesito riguardante i termini e le condizioni qui riportate o per contattare Network Associates per qualunque altra ragione, chiamare il numero (408) 988-3832, fax (408) 970-9727, scrivere a Network Associates, Inc., 3965 Freedom Circle, Santa Clara, California 95054 oppure visitare il sito Web di Network Associates all'indirizzo http://www.nai.com.

Prefazione

Cos'è successo?

Coloro che hanno già avuto modo di sperimentare la perdita di importanti dati memorizzati sul disco rigido o di osservare impotenti l'arresto del computer mentre sul monitor compariva un messaggio di saluto o ancora di doversi scusare per l'invio di messaggi di posta elettronica indesiderati che in realtà non avevano mai inviato, conoscono già gli effetti e il potenziale distruttivo dei virus informatici e di altri programmi dannosi. Solo poche fortunate persone possono affermare di non essersi ancora imbattute in una "infezione" da virus. Oggi, tuttavia, con gli oltre 16.000 virus conosciuti in circolazione in grado di attaccare i sistemi basati su Windows e su DOS, il contagio da virus è diventato sempre più probabile.

Fortunatamente solo alcuni di essi sono in grado di arrecare danni gravi ai dati. Il termine "virus informatico", infatti, comprende un'ampia gamma di programmi con un'unica caratteristica in comune: si "autoreplicano" automaticamente infettando un programma ospite o alcuni settori del disco del computer evitando di essere rilevati. La maggior parte dei virus causa problemi di natura relativamente innocua, con effetti semplicemente fastidiosi o talvolta addirittura insignificanti. Spesso, la conseguenza principale di un'infezione da virus è da ricercarsi nei costi derivanti dall'investimento di tempo o risorse nella ricerca dell'origine dell'infezione e nell'eliminazione di ogni traccia.

Perché preoccuparsi?

Ci si chiederà dunque perché preoccuparsi delle infezioni da virus se causano problemi così banali. Il problema non può risolversi così semplicemente: innanzitutto, sebbene siano relativamente pochi i virus con effetti distruttivi, non si conosce la reale diffusione di quelli dannosi. In molti casi i virus con gli effetti più devastanti sono i più difficili da scoprire, in quanto frutto di uno sviluppo doloso e corredati di tutte le misure necessarie per evitarne il rilevamento. In secondo luogo, anche i virus relativamente "benigni" possono interferire con le normali attività del computer e causare un comportamento imprevedibile in altri programmi. Alcuni virus contengono dei bug, del codice scritto male oppure degli altri programmi in grado di causare l'arresto del sistema nel momento in cui vengono eseguiti. In altri casi, si verificano problemi nell'esecuzione di programmi legittimi quando un virus, intenzionalmente o casualmente, altera i parametri del sistema o altri aspetti dell'ambiente di elaborazione. Individuare l'origine dei blocchi e degli errori del sistema può essere un'operazione dispendiosa in termini di tempo e denaro che va a discapito di attività più produttive.

Al di là di queste difficoltà, esiste un problema di prospettiva: i computer infetti possono essere portatori dell'infezione ad altri computer. Se si scambiano regolarmente dati con colleghi o clienti, è possibile diventare la causa di un involontario contagio e provocare più danni alla propria reputazione o al proprio volume d'affari di quanti non ne subisca fisicamente il computer.

La minaccia dei virus e di altri programmi dannosi è reale ed è in continuo aumento. Secondo una stima dell'International Computer Security Association, i costi derivanti solo dal rilevamento e dall'eliminazione delle infezioni da virus, in termini di tempo e mancata produttività, ammontano a 1 miliardo di dollari all'anno, cifra da cui sono esclusi i costi della perdita e del ripristino dei dati nelle prime fasi dell'attacco del virus.

Da dove vengono i virus?

Molte persone, dopo aver subito l'attacco di un virus o aver sentito parlare della comparsa di nuovi programmi insidiosi all'interno dei programmi di uso comune, si saranno posti molte domande riguardo l'origine dei virus. Da dove vengono i virus e gli altri programmi dannosi? Chi li scrive? Per quale motivo tali sviluppatori tentano di interrompere le attività lavorative, distruggere i dati o causare costose perdite di tempo e denaro? In che modo è possibile fermarli?

Perché è successo a me?

Probabilmente non consolerà affatto sapere che chi ha scritto il virus che ha cancellato la tabella di allocazione dei file del disco rigido non aveva intenzione di colpire un'azienda in particolare. E neanche rallegrerà sapere che il problema dei virus probabilmente non sarà mai eliminato del tutto. Tuttavia può essere utile avere alcune nozioni sulla provenienza dei virus e sulle loro modalità di funzionamento per proteggersi in modo più efficace.

Preistoria dei virus

Gli storici dei virus hanno identificato numerosi programmi che rappresentano i precursori degli odierni virus o che disponevano di caratteristiche che oggi sono associate ai virus. Robert M. Slade, ricercatore e insegnante canadese, fa risalire l'origine dei virus a particolari programmi di utility creati per ottimizzare l'uso dello spazio dei file e per eseguire altre utili attività al tempo delle prime reti di computer. Slade ricorda che gli scienziati di un laboratorio di ricerca della Xerox Corporation avevano definito questi programmi come "worm" (vermi), un termine coniato quando tali scienziati avevano iniziato a notare la presenza di "buchi" negli stampati delle mappe della memoria dei computer che parevano frutto dell'azione di vermi.

Questo termine è utilizzato ancora oggi per descrivere i programmi che si autoreplicano senza alterare il programma ospite.

Tra gli studenti universitari sopravvive una forte tradizione di scherzi informatici che probabilmente ha contribuito a sviluppare l'utilizzo delle tecniche di programmazione alla base dei programmi "worm" nella direzione di insidiose minacce piuttosto che in quella dei programmi di utility. Per mettere alla prova la propria abilità, gli studenti di informatica costruivano spesso programmi "worm" e li rilasciavano affinché "lottassero" gli uni contro gli altri in una sorta di competizione che aveva lo scopo finale di valutare quale di essi era in grado di "sopravvivere" e di sterminare i rivali. Quegli stessi studenti utilizzavano anche i programmi "worm" per fare degli scherzi a ignari colleghi.

Alcuni di questi studenti scoprirono presto che alcune funzioni del sistema operativo ospite potevano essere utilizzate per ottenere accesso non autorizzato alle risorse del computer. Altri, approfittando della relativa incompetenza di alcuni utenti, sostituivano alcuni programmi di utility di uso comune con programmi di loro creazione. Gli ignari utenti, eseguendo quelli che credevano essere i programmi utilizzati in precedenza, constatavano che i propri file non esistevano più, che le proprie password di account erano state rubate o incorrevano in altri spiacevoli incidenti. Questi programmi, denominati "cavalli di Troia" per la somiglianza metaforica con l'antico dono dei Greci alla città di Troia, costituiscono ancora oggi una seria minaccia per gli utenti di computer.

I virus e la rivoluzione dei PC

Ciò che oggi è considerato un vero virus informatico è comparso per la prima volta, secondo Robert Slade, subito dopo la diffusione dei personal computer nel mercato di massa nei primi anni '80. Altri ricercatori fanno risalire l'avvento dei programmi virus al 1986, in corrispondenza della comparsa del virus "Brain". Qualunque sia la data precisa, il collegamento tra la minaccia dei virus e i personal computer non è casuale.

La diffusione dei computer su vasta scala ha reso possibile il dilagare dei virus in molti sistemi, mentre in precedenza il mondo dell'informatica era stato appannaggio esclusivo di poche grandi corporazioni e università che disponevano di grandi mainframe sottoposti a stretta sorveglianza. Non aveva senso impiegare nei PC le sofisticate misure di sicurezza utilizzate per proteggere i dati importanti in tali ambienti. Anzi, gli scrittori di virus vi trovarono un terreno particolarmente fertile servendosi proprio delle tecnologie PC per i propri scopi.

Infezione del settore di boot

Con i primi PC, ad esempio, il sistema operativo veniva caricato ("boot") con i dischi floppy. Gli autori del virus Brain scoprirono presto che potevano inserire il proprio programma al posto del codice eseguibile presente nel settore di boot di tutti i floppy disk formattati con MS-DOS, anche se non comprendente i file di sistema. In questo modo, gli utenti caricavano il virus nella memoria ogni volta che avviavano il computer inserendo un disco floppy formattato nell'unità floppy. Una volta caricati nella memoria, i virus sono in grado di autoreplicarsi nei settori di boot di altri floppy o dischi rigidi.
Gli ignari utenti che caricavano il virus Brain da un disco floppy infetto vedevano comparire la "pubblicità" di una società di consulenza informatica pakistana.

Con tale annuncio pubblicitario, il virus Brain è stato il precursore di un'altra caratteristica dei virus moderni: il carico utile. Per carico utile si intendono gli scherzi o i comportamenti dolosi i cui effetti possono spaziare dalla visualizzazione di messaggi indesiderati fino alla distruzione dei dati. È la caratteristica dei virus che suscita maggiore interesse - molti autori di virus scrivono oggi i propri virus con il chiaro intento di distribuire il carico utile nel maggior numero di computer possibile.

Per un certo periodo, i sofisticati discendenti del primo virus del settore di boot hanno rappresentato la minaccia più seria per gli utenti di computer. Esistono anche varianti dei virus del settore di boot che infettano il record MBR (Master Boot Record), nel quale vengono memorizzate le informazioni sulla partizione che sono necessarie affinché il computer riesca a trovare tutte le partizioni del disco rigido e lo stesso settore di boot.

Realisticamente parlando, tutte le fasi del processo di boot, dalla lettura del record MBR al caricamento del sistema operativo, sono vulnerabili nei confronti dei sabotaggi virali. Tra i diversi effetti dei virus più tenaci e devastanti ancora oggi è compresa la capacità di infettare il settore di boot o il record MBR del computer. Entrando in azione al momento dell'avvio, il virus dispone di molti vantaggi, fra cui la possibilità di infettare il sistema ancora prima che venga eseguito il codice di protezione antivirus in grado di rilevarlo.

I virus del settore di boot e del record MBR hanno tuttavia un limite sostanziale: devono diffondersi per mezzo dei dischi floppy o di altri supporti rimovibili rimanendo confinati nella prima traccia del disco. Di pari passo con il sempre minore utilizzo dei dischi floppy e con la distribuzione del software tramite altri supporti, quali i CD-ROM, altri tipi di virus hanno preso il posto di quelli che costituivano una minaccia per il settore di boot. La diffusione di dischi floppy ad alta capacità, come i dischi Iomega Zip e prodotti simili di Syquest e altri ancora, potrebbe tuttavia dare luogo a un nuovo focolaio di infezione.

Virus che infettano i file

Nello stesso periodo in cui gli autori del virus Brain scoprirono la vulnerabilità del settore di boot del DOS, altri autori scoprirono come utilizzare il software esistente per consentire la replicazione delle proprie creazioni. Uno dei primi esempi di questo tipo di virus è comparso nei computer della Lehigh University in Pennsylvania. Questo virus ha infettato l'interprete dei comandi DOS COMMAND.COM utilizzandolo per caricarsi nella memoria. Una volta entrato nel sistema, si diffondeva in altri file COMMAND.COM non infetti ogni volta che un utente immetteva un qualunque comando DOS standard che invocava l'accesso al disco. La diffusione di questo virus si è limitata ai dischi floppy che contenevano, solitamente, un intero sistema operativo.

I virus della successiva generazione hanno presto superato questo limite grazie anche a sofisticate tecniche di programmazione. I virus di questo tipo, ad esempio, aggiungono il proprio codice all'inizio di un file eseguibile in modo che tale codice venga eseguito immediatamente all'avvio del programma e restituiscono il controllo al programma legittimo, il quale continua le proprie operazioni come se non fosse successo niente di insolito. Una volta attivato, il virus "blocca" o "intrappola" le richieste che il programma legittimo invia al sistema operativo e inserisce le proprie risposte. Alcuni virus particolarmente astuti sono perfino in grado di sovvertire i tentativi di eliminarli dalla memoria intrappolando la sequenza di input per il riavvio a freddo CTRL+ALT+CANC e di fingere un riavvio. A volte l'unico segnale che indica la presenza del virus - ovviamente prima che esploda il carico utile - è una piccola variazione nella dimensione del file del programma contaminato.

Virus invisibili, mutanti, cifrati e polimorfi

Sebbene si tratti di segnali minimi, il cambiamento della dimensione del file e altri fattori di questo tipo sono indizi sufficienti per la maggior parte dei prodotti antivirus per individuare e rimuovere il codice responsabile dell'infezione. Per questo motivo, una delle principali preoccupazioni degli scrittori di virus è rappresentata dai metodi possibili per nascondere il proprio artefatto. Inizialmente venivano utilizzate tecniche che costituivano un insieme di programmazione innovativa ed espedienti ovvii. Il virus Brain, ad esempio, reinstradava le richieste in modo da spostare un settore di boot di un dischetto dalla posizione attuale alla nuova posizione dei file di boot, che il virus aveva rimosso. Questa capacità di "invisibilità" gli consentiva, così come ad altri virus, di non essere rilevato con le tradizionali tecniche di ricerca.

Poiché i virus dovevano continuamente evitare di infettare i sistemi già contaminati - per evitare che le dimensioni dei file o l'utilizzo della memoria giungessero a punti tali da rendere facilmente rilevabile la presenza del virus - gli autori dovevano anche fornire l'istruzione di non toccare determinati file. Per risolvere questo problema, facevano in modo che il virus scrivesse una "firma" in codice per contrassegnare i file contaminati che non dovevano più essere infettati. Questo espediente riuscì a impedire che il virus venisse rilevato immediatamente ma aprì anche la strada per la nascita del software antivirus che sfrutta proprio quelle firme codificate per rintracciare il virus.

Di conseguenza, gli scrittori di virus escogitarono diversi metodi per nascondere le firme codificate. Alcuni virus "mutano" o cambiano la firma ogni volta che infettano un file. Altri cifrano la firma in codice o il virus stesso, lasciando solo un paio di byte da utilizzare come chiave per decifrarli. I nuovi virus più sofisticati, utilizzando l'invisibilità, la mutazione e la codifica, appaiono sempre più diversificati e difficili da rilevare. La ricerca di questi virus "polimorfi" ha visto impegnati gli ingegneri informatici nello sviluppo di elaborate tecniche di programmazione nell'ambito del software antivirus.

Virus macro

Intorno al 1995, la lotta contro i virus è giunta a una svolta. Nascevano continuamente nuovi virus, in parte favoriti dalla disponibilità di "kit" virali preconfezionati che consentivano anche ad utenti non programmatori di creare un nuovo virus in brevissimo tempo. Molti dei prodotti antivirus in commercio, tuttavia, potevano essere aggiornati semplicemente per rilevare ed eliminare le nuove varianti virali, che consistevano principalmente in errori di lieve entità in modelli noti.

Tuttavia, il 1995 è stato anche l'anno della comparsa del virus Concept, che ha scritto una nuova sorprendente pagina nella storia dei virus. Prima di Concept, i file di dati, quali documenti, fogli di lavoro e oggetti di grafica creati con i più diffusi prodotti software, erano considerati immuni alle infezioni. I virus, dopo tutto, non sono altro che programmi e, come tali, dovevano essere eseguiti analogamente ai programmi eseguibili per poter evidenziare i propri effetti dannosi. I file di dati, invece, memorizzavano solo le informazioni immesse tramite il software durante la lavorazione.

Questa distinzione venne meno nel momento in cui la Microsoft aggiunse per la prima volta funzioni macro in Microsoft Word e Microsoft Excel, le applicazioni di punta della suite di Office. Utilizzando la versione semplificata del linguaggio Visual BASIC incluso nella suite, gli utenti potevano creare modelli di documenti che avrebbero formattato e aggiunto automaticamente alcune funzioni nei documenti creati con Microsoft Word e Microsoft Excel. Per gli scrittori di virus, si trattò di un'opportunità per nascondere e diffondere i virus nei documenti creati dall'utente stesso.

Con la crescente diffusione di Internet e di prodotti di posta elettronica che consentono di allegare file ai messaggi, si è creata la condizione ideale per una rapida e capillare diffusione dei virus macro. In meno di un anno, i virus macro sono diventati la minaccia più insidiosa dall'avvento dei virus.

Nuovi sviluppi

Il software dannoso ha iniziato a insinuarsi anche in ambiti che prima erano considerati inattaccabili. Gli utenti del client mIRC (Internet Relay Chat), ad esempio, hanno avuto esperienza di virus costruiti con il linguaggio procedurale mIRC. I virus procedurali vengono inviati in testo normale, una caratteristica che li escluderebbe generalmente dall'infezione da virus, ma le versioni precedenti del software client mIRC interpretavano le istruzioni codificate, causando l'esecuzione degli effetti dannosi sul computer del destinatario. Nelle versioni aggiornate del prodotto è stata disabilitata questa capacità, ma il problema del mIRC è utile per confermare la regola generale che vede sempre qualcuno pronto ad approfittare dei punti non protetti all'interno del software.

I virus vengono sviluppati per ragioni molto diverse, dal puro divertimento al desiderio di notorietà nel gruppo dei pari o ancora per vendetta nei confronti di colleghi di lavoro o di persone che si ritengono ostili. Indipendentemente dalle singole motivazioni, gli scrittori continuano a sviluppare nuovi modi per arrecare danni al prossimo.

Come proteggersi

Il software antivirus Network Associates è uno strumento efficace per la prevenzione contro le infezioni e il danneggiamento dei dati. Tuttavia, è molto più efficace se utilizzato in combinazione con un programma di sicurezza completo comprendente una varietà di misure di sicurezza per la protezione dei dati. La maggior parte di queste misure sono dettate dal senso comune: è sempre consigliabile eseguire un controllo dei dischi che si ricevono da fonti sconosciute o di cui si dubita tramite un software antivirus o un'utility di verifica. I programmatori più subdoli utilizzano oggi programmi il cui aspetto ricorda quello dei programmi utilizzati per garantire la protezione dei computer, celando uno scopo disdicevole dietro un aspetto familiare. Insieme ai propri prodotti, la Network Associates fornisce VALIDATE.EXE, un programma di utility di verifica che consente di prevenire questo tipo di manipolazione, ma né questo né altri prodotti antivirus sono in grado di rilevare la sostituzione dei programmi shareware o delle utility di uso comune con i cosiddetti "cavalli di Troia" o altri programmi dannosi.

L'accesso al World Wide Web e ad Internet pone altri rischi. Disporre di un firewall completo per proteggere la rete e implementare altre misure di sicurezza rappresenta una necessità quando la rete è vulnerabile agli attacchi di avventori senza scrupoli che possono penetrare da qualunque parte del mondo per appropriarsi di dati sensibili o per insediare un codice dannoso. È necessario anche assicurarsi che la rete non sia accessibile da parte di utenti non autorizzati e disporre di adeguati programmi di formazione per insegnare e mettere in atto le misure di sicurezza standard.

Per informazioni sull'origine, il comportamento e altre caratteristiche di particolari virus, consultare la Virus Information Library disponibile presso il sito Web di Network Associates. Alcuni prodotti Network Associates sono corredati di un Elenco virus che riepiloga tutti i virus che il programma è in grado di rilevare e contiene informazioni sulle dimensioni dei virus, le infezioni che provocano e sulla possibilità di rimuoverli dai file.

Altri prodotti di Network Associates sono compresi nella suite Total Virus Defense (TVD), la soluzione antivirus più completa attualmente disponibile, e in Total Network Security (TNS), la più avanzata suite di sicurezza antivirus di rete oggi sul mercato. Per entrambi Network Associates offre un eccellente servizio di assistenza tecnica, addestramento e una rete mondiale di ricercatori e sviluppatori. Per informazioni sulle capacità di Total Virus Defense, rivolgersi al rappresentante Network Associates locale oppure visitare il sito World Wide Web della Network Associates all'indirizzo **http://www.nai.com**.

Come contattare il servizio clienti

Servizio clienti

Per ordinare i prodotti o avere informazioni su di essi, contattare il reparto Assistenza clienti di Network Associates al numero 39 (0)2 9214 1555 o scrivere al seguente indirizzo:

Network Associates Srl.
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
ITALIA

Supporto tecnico

Network Associates è nota per il suo grande impegno nel cercare di soddisfare i propri clienti. Per continuare questa tradizione, abbiamo trasformato il nostro sito World Wide Web in una valida fonte informativa in materia di supporto tecnico. Consigliamo a tutti gli utenti di visitare il nostro sito Web per leggere le risposte alle domande frequenti, scaricare gli aggiornamenti ai software Network Associates e ottenere le notizie e le informazioni più aggiornate sui virus pubblicate da Network Associates.

World Wide Web	http://support.nai.com

Agli utenti che non dispongono dell'accesso al Web e a coloro che non trovano sul nostro sito ciò che desiderano, si consiglia l'utilizzo dei servizi automatici.

Automated Voice and Fax Response System	(408) 988-3034
Internet	support@nai.com
CompuServe	GO NAI
America Online	parola chiave NAI

Quando nessuno dei servizi automatici dispone delle risposte desiderate, si consiglia di contattare Network Associates a uno dei seguenti numeri, dal lunedì al venerdì, dalle ore 6:00 alle ore 18:00. , ora locale della costa del Pacifico.

Per i clienti dotati di licenza aziendale:

Tel.	(408) 988-3832
Fax	(408) 970-9727

Per i clienti dotati di licenza personale:

Tel.	(972) 278-6100
Fax	(408) 970-9727

Per fornire le risposte agli utenti in modo rapido ed efficiente, il personale del supporto tecnico di Network Associates necessita di alcune informazioni sul computer e sul software in uso. Saranno necessarie le seguenti informazioni:

- Nome del prodotto e numero della versione in uso
- Marca e modello del computer in uso
- Eventuali hardware o periferiche aggiuntive collegate al computer
- Tipo di sistema operativo e numero della versione in uso

- Tipo e versione della rete, se il computer in uso è collegato a una rete
- Contenuto di AUTOEXEC.BAT, CONFIG.SYS, dello script di LOGIN al sistema e di NOTES.INI
- Precisi passaggi da svolgere perché si verifichi il problema

Addestramento Network Associates

Per informazioni sui programmi di addestramento in loco per i prodotti Network Associates, chiamare il numero (800) 338-8754.

Informazioni relative ai contatti internazionali

Per contattare Network Associates fuori degli Stati Uniti, usare gli indirizzi e i numeri di telefono elencati sotto.

Network Associates Australia
Level 1, 500 Pacific Highway
St. Leonards, NSW 2065
Australia
Tel.: 61-2-9437-5866
Fax: 61-2-9439-5166

Network Associates Canada
139 Main Street, Suite 201
Unionville, Ontario
Canada L3R 2G6
Tel.: (905) 479-4189
Fax: (905) 479-4540

Network Associates Deutschland GmbH
Industriestrasse 1
D-82110 Germering
Germania
Tel.: 49 8989 43 5600
Fax: 49 8989 43 5699

Network Associates International B.V.
Gatwickstraat 25
1043 GL Amsterdam
Paesi Bassi
Tel.: 31 20 586 6100
Fax: 31 20 586 6101

NA Network Associates Oy
Kielotie 14B
01300 Vantaa
Finlandia
Tel.: 358 9 836 2620
Fax: 358 9 836 26222

Network Associates France S.A.
50 rue de Londres
75008 Parigi
Francia
Tel.: 33 1 44 908 737
Fax: 33 1 45 227 554

Network Associates Hong Kong

19/F, Matheson Centre
3 Matheson Street
Causeway Bay
Hong Kong
Tel.: 852-2832-9525
Fax: 852-2832-9530

Network Associates Japan, Inc.

Toranomon 33 Mori Bldg.
3-8-21 Toranomon
Minato-Ku, Tokyo 105-0001
Giappone
Tel.: 81 3 5408 0700
Fax: 81 3 5408 0780

Network Associates Korea

135-090, 18th Floor, Kyoung Am Bldg.
157-27 Samsung-Dong, Kangnam-Ku
Seul, Korea
Tel.: 82-2-555-6818
Fax: 82-2-555-5779

Network Associates Sweden

Datavägen 3A, box 59678
S-175 26 Järfälla
Svezia
Tel.: 46 8 580 100 02
Fax: 46 8 580 100 05

Network Associates South East Asia

78 Shenton Way
#29-02
Singapore 079120
Tel.: 65-222-7555
Fax: 65-220-7255

Network Associates International Ltd.

Minton Place, Victoria Street
Windsor, Berkshire
SL4 1EG
Regno Unito
Tel.: 44 (0)1753 827500
Fax: 44 (0)1753 827520

Network Associates Srl

Centro Direzionale Summit
Palazzo D/1
Via Brescia, 28
20063 - Cernusco sul Naviglio (MI)
Italia
Tel.: 39 (0)2 9214 1555
Fax: 39 (0)2 9214 1644

Network Associates Latin America

150 S. Pine Island Road, Suite 205
Plantation, Florida 33324
USA
Tel.: (954) 452-1731
Fax: (954) 236-8031

Network Associates Switzerland

Baeulerwisenstrasse 3
8152 Glattbrugg
Svizzera
Teléfono:41 1 808 99 66
Fax: 41 1 808 99 77

Network Associates Spain

Orense, 36. 3a planta
28020 Madrid
Spagna
Tel.: 34 902 40 90 40
Fax: 34 902 40 10 10

Sommario

Introduzione a VirusScan 1

McAfee VirusScan per Windows 3.1*x* è la potente soluzione desktop antivirus di Network Associates. La strategia di protezione di VirusScan si compone di tre elementi: scansione all'accesso, scansione su richiesta e scansione pianificata.

VirusScan controlla costantemente il sistema per rilevare eventuali presenze di virus tramite VShield, il componente di scansione all'accesso. Se viene rilevato un virus, è possibile scegliere un'operazione automatica di eliminazione del virus, di spostamento dei file infetti in un'altra posizione o di eliminazione dei file infetti.

VirusScan può inoltre essere avviato dall'utente affinché esegua la scansione di un file, di una cartella, di un disco o di un volume. È questo il componente di scansione su richiesta della strategia di protezione offerta da VirusScan.

La scansione pianificata consente di configurare VirusScan in modo da eseguire scansioni specifiche ad orari o intervalli prestabiliti. In tal modo è possibile sottoporre a scansioni frequenti le aree del sistema particolarmente vulnerabili, o eseguire una scansione accurata dell'intero sistema mentre non è in uso.

VirusScan è un importante elemento di un programma di sicurezza globale comprendente una serie di misure di sicurezza tra cui backup regolari, un sistema di protezione tramite password significative, addestramento e nozioni di approfondimento. Si consiglia di adottare al più presto questo programma di sicurezza come misura preventiva contro future infezioni. Per suggerimenti sulla creazione di un ambiente sicuro, consultare l'Appendice B, "Prevenzione delle infezioni".

Caratteristiche principali

- Lo scanner certificato NCSA assicura un rilevamento del 100% dei virus in circolazione. Per informazioni sulle certificazioni, visitare il sito Web della National Computer Security Association all'indirizzo **http://www.NCSA.com**.
- VShield, lo scanner all'accesso di VirusScan, fornisce un'identificazione in tempo reale dei virus sia conosciuti che sconosciuti nello stesso momento in cui si accede, si crea, si copia, si rinomina o si esegue un file, si accede ad un disco oppure si avvia o si arresta il sistema.

- La scansione su richiesta consente di avviare il rilevamento di virus conosciuti (siano essi di boot, di file, di tipo multipartito, camuffati, cifrati e polimorfi) presenti nei file, nelle unità e nei dischetti.
- I tipi di scansione Code Trace™, Code Poly™ e Code Matrix™ utilizzano le tecnologie Network Associates per ottenere la massima accuratezza nell'identificazione dei virus.
- VirusScan può essere configurato affinché risponda automaticamente al rilevamento dei virus tramite avviso, registrazione, eliminazione, isolamento o pulizia. VirusScan può anche essere configurato in modo che invii avvisi e rapporti a un server centralizzato.
- VirusScan include un pianificatore che consente di impostare scansioni giornaliere, settimanali o mensili.
- Quando si acquista una licenza di abbonamento Network Associates si ricevono aggiornamenti mensili delle firme dei virus e aggiornamenti del prodotto che garantiscono le più elevate percentuali di rilevamento e rimozione dei virus.

Modalità di funzionamento del rilevamento dei virus

VirusScan controlla il computer e ricerca le caratteristiche (sequenze di codice) uniche di ogni virus conosciuto. Quando rileva un virus, VirusScan esegue le operazioni preconfigurate. Nel caso di virus cifrati o mutati, VirusScan utilizza degli algoritmi basati su analisi statistiche, euristica e disassemblaggio del codice.

Quando eseguire le scansioni

Lo scanner all'accesso di VirusScan esegue la scansione del sistema ogni volta che si accede, si crea, si copia, si rinomina o si esegue un file oppure si avvia il sistema. Inoltre, protegge il sistema dai virus quando si carica o scarica dalle reti.

Per la massima protezione, utilizzare la funzione di scansione su richiesta di VirusScan per rilevare i virus quando si aggiungono file al sistema, ad esempio file copiati da un dischetto o file scaricati da un servizio in linea.

Scansione di dischetti sconosciuti

Prima di eseguire, installare o copiare file da un dischetto sconosciuto, eseguire VirusScan per controllare i file contenuti nel dischetto.

Scansione di nuovi file scaricati o installati

Quando si installa del nuovo software o si scaricano file eseguibili da un servizio in linea, è consigliabile eseguire VirusScan per controllare i file prima di utilizzarli.

Scansioni regolari

Eseguire scansioni su richiesta del sistema con frequenza regolare da un massimo di una volta al giorno a un minimo di una volta al mese, in base alla suscettibilità del sistema alle infezioni da virus. Pianificare la scansione delle aree più vulnerabili del sistema per ottenere la massima sicurezza.

Installazione di VirusScan 2

Prima di iniziare

Prima di installare VirusScan per Windows 3.1*x*, procedere come riportato di seguito. In questo modo si ridurrà al minimo il rischio di diffondere eventuali virus che potrebbero essere presenti nel sistema.

1. Esaminare i requisiti di sistema di VirusScan.
2. Verificare che il sistema sia esente da virus. Se si sospetta che il sistema sia già infetto, consultare la sezione "Se si sospetta la presenza di un virus" a pagina 63 prima di iniziare la procedura di installazione.

Requisiti di sistema

- Personal computer IBM compatibile 386 o superiore, con sistema operativo Windows 3.1*x*
- 5MB di spazio libero su disco rigido
- 4MB di memoria (consigliati 8 MB).

Procedura di installazione

In questa sezione viene descritta la procedura di installazione di base. Per informazioni sulle installazioni condivise vedere l'Appendice C, "Installazioni condivise".

NOTA: Se si sospetta che il sistema sia già infetto, consultare la sezione "Se si sospetta la presenza di un virus" a pagina 63 prima di installare VirusScan.

Per installare VirusScan sul sistema procedere come riportato di seguito:

1. Avviare Windows.
2. Utilizzare uno dei metodi riportati di seguito:
   - Se si esegue l'installazione da dischetto o da CD, inserire il dischetto o il CD di installazione di VirusScan.

- Se si esegue l'installazione da file scaricati da una BBS o dal sito Web Network Associates, decomprimere i file zip in una directory sulla rete o sull'unità locale.

3. Scegliere **Esegui** dal menu File.
   - Se si esegue l'installazione da dischetto, digitare:

     ```
     x:\setup.exe
     ```

     dove *x* è l'unità contenente il dischetto. Fare clic su **OK**.
   - Se si esegue l'installazione da CD, digitare:

     ```
     x:\win\setup.exe
     ```

     dove *x* è l'unità contenente il CD. Fare clic su **OK**.
   - Se si esegue l'installazione da file scaricati, digitare:

     ```
     x:\percorso\setup.exe
     ```

     dove **x:\percorso** è la posizione dei file. Fare clic su **OK**.
4. Viene visualizzato il contratto di licenza di VirusScan. Leggere le informazioni visualizzate, quindi fare clic su **Sì** per continuare.
5. Quando viene visualizzata la schermata introduttiva, leggere le relative informazioni, quindi fare clic su **Avanti** per continuare.
6. Selezionare il tipo di installazione:
   - L'installazione **Standard** consente di eseguire un'installazione completa di VirusScan con le opzioni più comuni.
   - L'installazione **Minima** consente di installare VirusScan con il minimo delle opzioni necessarie.
   - L'installazione **Personalizzata** consente di installare VirusScan con i componenti desiderati.
7. Selezionare una directory di destinazione per i file di VirusScan.
   - Specificare il nome della directory nella casella specificata, quindi fare clic su **Avanti**.
   - Scegliere **Sfoglia** per accedere ad una directory specifica, quindi scegliere **Avanti**.
8. Quando il sistema lo richiede, rivedere le impostazioni e fare clic su **Avanti** per continuare. I file di VirusScan vengono copiati sull'unità disco rigido.

9. Viene richiesto di inserire un dischetto vuoto nell'unità A:.. Seguire le istruzioni visualizzate per creare un disco di emergenza per il ripristino del sistema nel caso di un'infezione del settore di boot.

NOTA: Se non si desidera creare un disco di emergenza ora, fare clic su **Annulla**. Sarà possibile creare un disco di emergenza in un secondo momento, facendo doppio clic sull'icona del disco di emergenza nel gruppo di programmi VirusScan.

---

10. Fare clic su **Sì** per leggere il file di testo What's New contenente le informazioni sulle nuove caratteristiche di VirusScan.
11. Rivedere le modifiche apportate ai file di sistema e fare clic su **Avanti**.
12. Scegliere **Sì** per riavviare il computer, quindi fare clic su **Fine**. Il sistema viene riavviato. Tutte le modifiche sono attive. VirusScan è ora in esecuzione.

NOTA: Se al passaggio 8 la creazione del disco di emergenza era stata annullata, si consiglia di creare subito tale disco. Vedere "Creazione di un disco di emergenza" a pagina 76 per ulteriori informazioni.

Verifica dell'installazione

L'Eicar Standard AntiVirus Test File è il risultato di uno sforzo combinato dei produttori di programmi antivirus diretto ad elaborare uno standard per i clienti affinché possano verificare le loro installazioni antivirus.

Per verificare l'installazione, copiare la seguente riga nel proprio file e denominarlo EICAR.COM.

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

NOTA: Questa stringa di caratteri deve comparire su un'unica riga nel file.

Al termine dell'operazione si avrà un file di 69 o 70 byte. Quando questo file viene sottoposto a scansione, VirusScan segnala la presenza del virus EICAR-STANDARD-AV-TEST-FILE. Malgrado quanto riportato, VirusScan non ha rilevato un virus, ma soltanto un file progettato per verificarne la capacità di rilevamento dei virus.

Eliminare il file EICAR.COM al termine della verifica dell'installazione in modo da non allarmare inutilmente gli altri utenti.

Scansione all’accesso 3

Definizione della scansione all’accesso

La scansione all'accesso è uno dei tre componenti della strategia di protezione utilizzata da VirusScan per Windows 3.1*x*. Gli altri componenti sono la scansione su richiesta e la scansione pianificata.

La scansione all'accesso viene eseguita tramite un programma residente in memoria, VShield, che utilizza una serie di moduli VxD (driver di dispositivo virtuale caricato in modo dinamico) per fornire una protezione in tempo reale del sistema. La scansione all'accesso previene le infezioni da virus controllando automaticamente elementi quali file, directory, unità e qualsiasi altro supporto nel momento in cui vi si accede.

In questo capitolo verranno illustrate le procedure necessarie per avviare e configurare VShield, il componente per la scansione all'accesso di VirusScan.

Avvio di VShield

VShield, lo scanner all'accesso di VirusScan, è un driver di dispositivo virtuale. In base all'impostazione predefinita, VShield viene attivato automaticamente ogni volta che si avvia Windows e rimane attivo in background durante ciascuna sessione di Windows.

VShield può essere attivato in uno dei seguenti modi:

- Fare doppio clic sull'icona VShield presente sul desktop. Se il pulsante all'estrema sinistra nella finestra di dialogo visualizzata riporta "Disattiva", VShield è attivato. Se viene visualizzato "Attiva", per attivare VShield è necessario selezionare il pulsante.
- Eseguire VSHWIN.EXE, contenuto nella directory di installazione.

Se per qualche ragione VShield non è attivo all'avvio di Windows, sarà necessario riconfigurarlo in modo che si carichi all'avvio. Per informazioni su questa procedura, consultare la sezione "Configurazione della scansione all'accesso" a pagina 11.

Utilizzo della finestra di stato VShield

Quando VShield è attivato, è possibile utilizzare la finestra di stato VShield (Figura 3-1) per configurare le opzioni di scansione o per visualizzare lo stato dei file sottoposti a scansione. Per visualizzare tale finestra, fare doppio clic sull'icona VShield sul desktop.

NOTA: Se l'icona VShield non è visibile, eseguire il Configuration Manager di VShield (VSHCFG16.EXE) e selezionare **Visualizza icona sul desktop**.

Figura 3-1.. Finestra di stato VShield

La finestra di stato VShield riporta il nome dell'ultimo file sottoposto a scansione, il numero di file sottoposti a scansione, il numero di file infetti e il numero di file puliti, eliminati o spostati.

Inoltre, sono disponibili le seguenti opzioni:

- **Disattiva/Attiva** consente di attivare o disattivare la scansione all'accesso nella sessione corrente di Windows.
- **Proprietà** consente di configurare le impostazioni di rilevamento, di azione e di rapporto della scansione all'accesso. Per ulteriori informazioni vedere "Configurazione della scansione all'accesso" a pagina 11.
- Il pulsante **Chiudi** consente di chiudere la finestra di stato VShield.

Configurazione della scansione all'accesso

Utilizzare il Configuration Manager di VShield per configurare la scansione all'accesso. È possibile avviare il Configuration Manager in uno dei modi seguenti:

- Selezionare **Proprietà** dalla finestra di stato VShield. Per ulteriori informazioni sulla visualizzazione di questa finestra consultare "Utilizzo della finestra di stato VShield".
- Eseguire VSHCFG16.EXE, contenuto nella directory di installazione (la posizione predefinita è **C:\Neta\Viruscan**).

Viene visualizzato il Configuration Manager di VShield con la pagina Rilevamento in primo piano (Figura 3-2).

Configurazione del rilevamento di VShield

Utilizzare la pagina Rilevamento (Figura 3-2) per selezionare gli elementi da sottoporre a scansione e per programmare la scansione.

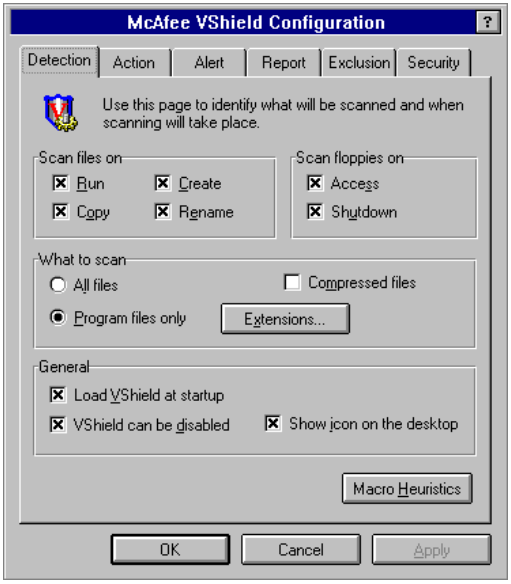

Figura 3-2.. Configuration Manager di VShield (pagina Rilevamento)

Per configurare le opzioni di rilevamento, procedere come segue:

1. Selezionare l'evento o gli eventi che determineranno l'avvio della scansione da parte di VShield.

   - **Esegui** consente di eseguire la scansione quando viene eseguito un file.
   - **Crea** consente di eseguire la scansione quando viene creato un file.
   - **Copia** consente di eseguire la scansione quando viene copiato un file.
   - **Rinomina** consente di eseguire la scansione quando viene rinominato un file.

   NOTA: Network Associates consiglia di selezionare tutte le opzioni sopra riportate per garantire la massima protezione.

2. Selezionare l'evento o gli eventi che determineranno l'avvio della scansione dei dischetti da parte di VShield.

   - **Accesso** consente di eseguire la scansione quando si accede a un dischetto.
   - **Arresto** consente di eseguire la scansione del dischetto ad ogni arresto del sistema.

   NOTA: Network Associates consiglia di selezionare tutte le opzioni sopra riportate per garantire la massima protezione.

3. Selezionare i tipi di file che si desidera siano sottoposti a scansione da VShield.

   - **Tutti i file** consente di sottoporre a scansione tutti i file indipendentemente dal tipo.
   - **Solo file di programma** consente di sottoporre a scansione solo i file con determinate estensioni. Per cambiare le estensioni incluse in questo elenco, fare clic su **Estensioni**.

     NOTA: Le estensioni predefinite sono .EXE, .COM, .DO? e .XL?. Il punto interrogativo è un carattere jolly. Secondo questo elenco, verranno sottoposti a scansione i file di documento e di modello di Word ed Excel (.DOC, .DOT, .XLS e .XLT) nonché i file di programma.

- **File compressi** consente di sottoporre a scansione i file compressi con PKLITE o LZEXE.

4. Configurare le preferenze generali.

   - **Carica VShield all'avvio** consente di attivare la scansione all'accesso quando si avvia Windows.
   - **VShield può essere disattivato** consente la disattivazione della scansione all'accesso.
   - **Visualizza icona sul desktop** consente di visualizzare la finestra di stato VShield e selezionare le proprietà di VShield utilizzando un'icona del desktop.

   NOTA: Network Associates consiglia di selezionare tutte le opzioni. Tuttavia, è possibile che gli amministratori di sistema desiderino attivare solo **Carica VShield all'avvio** nella configurazione del software per gli utenti. Per ulteriori informazioni sulle funzioni di blocco di VShield da parte dell'amministratore consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

   ---

5. Se lo si desidera, fare clic su **Euristica delle macro** per definire le impostazioni di scansione euristica delle macro. Esse consentiranno di impostare la scansione utilizzata da VirusScan per ripulire dai virus macro i documenti Microsoft Word ed Excel. Viene visualizzata la finestra di dialogo Impostazioni di scansione euristica delle macro (Figura 3-3).

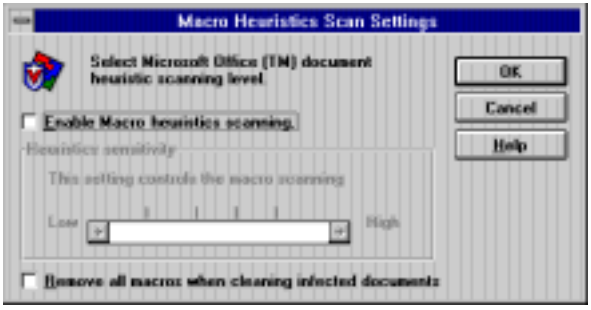

Figura 3-3.. Finestra di dialogo Impostazioni di scansione euristica delle macro

a. Attivare e disattivare la scansione euristica delle macro. In base all'impostazione predefinita, è attivata.

b. Per impostare la sensibilità della scansione euristica delle macro, utilizzare il dispositivo di scorrimento.

c. Stabilire se si desidera che VirusScan rimuova le macro quando pulisce documenti infetti. In base all'impostazione predefinita, VirusScan rimuove le macro.

d. Fare clic su **OK**.

NOTA: Se si porta il dispositivo di scorrimento su Alto *e* si seleziona Rimuovi macro durante pulitura documenti infetti, VirusScan rimuove tutte le macro da ciascun documento di Word o Excel sottoposto a scansione e non solo le macro simili a virus.

---

6. Utilizzare uno dei metodi riportati di seguito:

   - Fare clic su **Applica** per salvare le modifiche senza uscire dal Configuration Manager di VShield.
   - Fare clic su **OK** per salvare le modifiche e tornare alla finestra Stato di VShield.
   - Fare clic su **Annulla** per tornare alla finestra di stato VShield senza salvare le modifiche.
   - Per bloccare e proteggere tramite password le modifiche eseguite, consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

Configurazione delle azioni di VShield

Utilizzare la pagina Azione (Figura 3-4) per selezionare l'azione che VShield dovrebbe eseguire qualora rilevi un virus.

Figura 3-4.. Configuration Manager di VShield (pagina Azione)

Per configurare queste impostazioni, procedere come segue:

1. Nell'elenco Al rilevamento di un virus, selezionare una delle seguenti azioni:

   - **Richiedi azione**: se si utilizza questa opzione, quando rileva un virus VShield richiede di specificare l'azione desiderata. Le opzioni possibili sono:

     – **Pulisci file**.

     – **Elimina file**.

     – **Escludi file**.

     – **Interrompi accesso**.

     – **Continua accesso**. Questa azione è consigliata per sistemi assistiti.

- **Sposta file infetti automaticamente**: se si utilizza questa opzione, ciascun file infetto viene spostato automaticamente nella cartella scelta. Specificare un percorso nella casella Cartella di spostamento oppure scegliere **Sfoglia** per individuare una cartella.

  Questo percorso può essere relativo. Ad esempio, se si digita `\Infetti` nella casella di testo, verrà creata una cartella Infetti sull'unità dove è stato rilevato il virus. Il file infetto verrà spostato in quella cartella.

  NOTA: Se non è possibile pulire un file infetto o se VShield non possiede l'accesso al file corretto, l'accesso al file verrà negato.

- **Pulisci file infetti automaticamente**: se si utilizza questa opzione, ciascun file infetto verrà pulito senza alcuna richiesta specifica.
- **Elimina file infetti automaticamente**: se si utilizza questa opzione, ciascun file infetto verrà eliminato senza alcuna richiesta specifica. Occorre quindi ripristinare una copia non infetta del file eliminato dai backup.
- **Nega l'accesso ai file infetti e continua**: se si utilizza questa opzione, i programmi presenti sul sistema non possono accedere a un file infetto finché non si specifica a VShield l'azione richiesta in merito a tale file. Questa azione è consigliata per i sistemi non assistiti durante le scansioni.

2. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche senza uscire dal Configuration Manager.
   - Fare clic su **OK** per salvare le modifiche e tornare alla finestra Stato di VShield.
   - Fare clic su **Annulla** per tornare alla finestra di stato VShield senza salvare le modifiche.
   - Per bloccare e proteggere tramite password le modifiche eseguite, consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

Configurazione degli avvisi di VShield

Utilizzare la pagina Avviso (Figura 3-5) per scegliere il modo in cui VShield avverte l'utente quando rileva un virus.

Figura 3-5.. Configuration Manager di VShield (pagina Avviso)

Per configurare gli avvisi di VShield, procedere come segue:

1. Selezionare **Invia avviso alla rete** se si desidera che VShield invii un avviso ad un percorso di rete controllato da NetShield, la soluzione antivirus di Network Associates per i server. Fare clic su **Sfoglia** per accedere alla directory desiderata.

   NOTA: Questa directory dovrebbe contenere il file dell'avviso centralizzato, CENTALERT.TXT. Per ulteriori informazioni sull'avviso centralizzato, consultare la documentazione relativa a NetShield.

   ---

2. Selezionare **Riproduci segnale acustico** e/o **Visualizza messaggio personalizzato**. È possibile personalizzare il messaggio facendo clic nella casella di testo e modificando il relativo testo.

3. Utilizzare uno dei metodi riportati di seguito:

   - Fare clic su **Applica** per salvare le modifiche senza uscire dal Configuration Manager.
   - Fare clic su **OK** per salvare le modifiche e tornare alla finestra Stato di VShield.
   - Fare clic su **Annulla** per tornare alla finestra di stato VShield senza salvare le modifiche.
   - Per bloccare e proteggere tramite password le modifiche eseguite, consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

Configurazione dei rapporti di VShield

Utilizzare la pagina Rapporto (Figura 3-6) per configurare la registrazione dell'attività dei virus e determinare quali informazioni verranno incluse nel registro.

Figura 3-6.. Configuration Manager di VShield (pagina Rapporto)

NOTA: Questo file di registro è un file di testo che può essere visualizzato utilizzando un editor di testi qualsiasi, ad esempio il Blocco note.

Per configurare le impostazioni relative ai rapporti, procedere come segue:

1. Selezionare **Registra su file**, quindi effettuare una delle seguenti operazioni:
   - Immettere un percorso e un nome di file nella casella di testo
   - Scegliere un percorso facendo clic sul pulsante **Sfoglia**.
2. Limitare le dimensioni del file di registro selezionando la casella di controllo **Limita dimensioni file di registro a** e specificando un valore compreso tra 10 KB e 999 KB.

NOTA: Il percorso predefinito per il file di registro è **C:\Neta\Viruscan\VSHLOG.TXT**. La dimensione massima predefinita del file di registro è di 100KB.

---

3. Scegliere le informazioni da includere nel file di registro. Le opzioni includono:
   - Rilevamento virus
   - Pulizia virus
   - Eliminazione file infetti
   - Spostamento file infetti
   - Impostazioni sessione
   - Riepilogo sessione
   - Data e ora
   - Nome utente.
4. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche senza uscire dal Configuration Manager.
   - Fare clic su **OK** per salvare le modifiche e tornare alla finestra Stato di VShield.
   - Fare clic su **Annulla** per tornare alla finestra di stato VShield senza salvare le modifiche.
   - Per bloccare e proteggere tramite password le modifiche eseguite, consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

Configurazione delle esclusioni di VShield

Utilizzare la pagina Esclusione (Figura 3-7) per definire gli elementi da escludere dalle scansioni.

Figura 3-7.. Configuration Manager di VShield (pagina Esclusione)

NOTA: La cartella **C:\Neta\Viruscan\Infected** viene esclusa automaticamente.

Aggiunta di un elemento all'elenco delle esclusioni

Per aggiungere un elemento all'elenco delle esclusioni, procedere come segue:

1. Fare clic su **Aggiungi** nella pagina Esclusione. Viene visualizzata la finestra di dialogo Escludi elemento (Figura 3-8 a pagina 21).

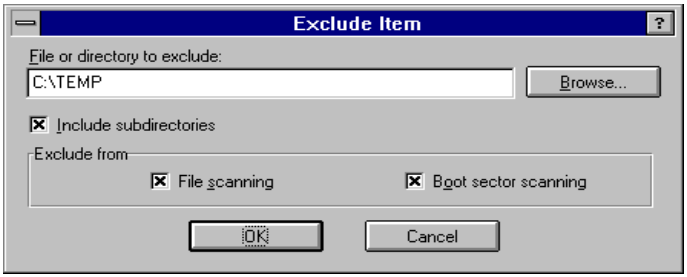

Figura 3-8.. Finestra di dialogo Escludi elemento

2. Digitare il percorso del file o della cartella che si desidera escludere dalla scansione oppure fare clic su **Sfoglia** per individuare la cartella.

NOTA: La funzione Sfoglia consente di accedere unicamente alle cartelle. Per escludere un file, digitare manualmente il percorso e il nome dello stesso nella finestra di dialogo Escludi elemento.

---

3. Selezionare **Includi sottocartelle** per escludere tutte le sottocartelle all'interno della cartella selezionata.
4. Se lo si desidera, escludere la cartella dalla scansione dei file o dalla scansione del settore di boot selezionando le relative caselle.
5. Fare clic su **OK**.
6. Utilizzare uno dei metodi riportati di seguito:

   - Fare clic su **Applica** per salvare le modifiche senza uscire dal Configuration Manager.
   - Fare clic su **OK** per salvare le modifiche e tornare alla finestra Stato di VShield.
   - Fare clic su **Annulla** per tornare alla finestra di stato VShield senza salvare le modifiche.
   - Per bloccare e proteggere tramite password le modifiche eseguite, consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

Rimozione di un elemento dall'elenco delle esclusioni

Per rimuovere un elemento dall'elenco, procedere come segue:

1. Selezionare l'elemento, quindi fare clic su **Rimuovi**.
2. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche senza uscire dal Configuration Manager.
   - Fare clic su **OK** per salvare le modifiche e tornare alla finestra Stato di VShield.
   - Fare clic su **Annulla** per tornare alla finestra di stato VShield senza salvare le modifiche.
   - Per bloccare e proteggere tramite password le modifiche eseguite, consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

Modifica di un elemento nell'elenco delle esclusioni

Per modificare un elemento esistente nell'elenco delle esclusioni, procedere come segue:

1. Selezionare l'elemento, quindi fare clic su **Modifica**.
2. Viene visualizzata la finestra di dialogo Escludi elemento (Figura 3-8 a pagina 21). Apportare le modifiche, quindi fare clic su **OK**.
3. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche senza uscire dal Configuration Manager.
   - Fare clic su **OK** per salvare le modifiche e tornare alla finestra Stato di VShield.
   - Fare clic su **Annulla** per tornare alla finestra di stato VShield senza salvare le modifiche.
   - Per bloccare e proteggere tramite password le modifiche eseguite, consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

Configurazione del sistema di sicurezza di VShield

Utilizzare la pagina Sicurezza (Figura 3-9) per bloccare le impostazioni di VShield e proteggerle tramite password. Questa funzione è particolarmente utile per gli amministratori di sistema che desiderano impedire agli utenti di compromettere la sicurezza del sistema modificando le impostazioni di VShield.

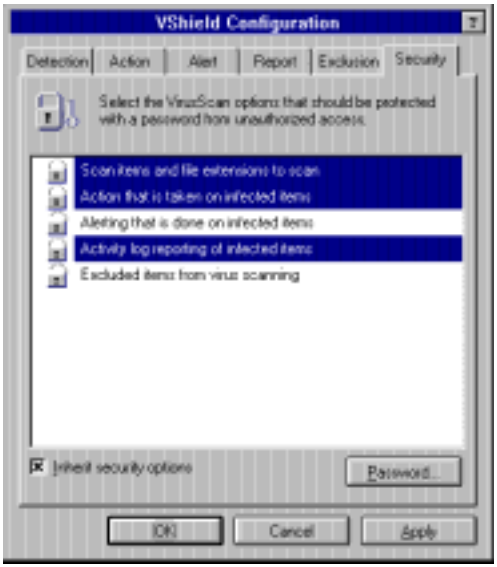

Figura 3-9.. Configuration Manager di VShield (pagina Sicurezza)

Per bloccare le impostazioni di VShield, procedere come segue:

1. Selezionare tra le seguenti le impostazioni di VShield da proteggere tramite password:

   - **Elementi di scansione ed estensioni di file da sottoporre a scansione**
   - **Azione intrapresa su elementi infetti**
   - **Avvisi effettuati su elementi infetti**
   - **Rapporto di registro attività di elementi infetti**
   - **Elementi esclusi dalla ricerca di virus**.

NOTA: Ciascuna impostazione protetta tramite password verrà evidenziata e presenterà a sinistra un lucchetto chiuso.

---

2. Fare clic sul pulsante **Password** per creare o modificare una password. Verrà richiesto di immettere e confermare la password.
3. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche senza uscire dal Configuration Manager.
   - Fare clic su **OK** per salvare le modifiche e tornare alla finestra Stato di VShield.
   - Fare clic su **Annulla** per tornare alla finestra di stato VShield senza salvare le modifiche.
   - Per bloccare e proteggere tramite password le modifiche eseguite, consultare "Configurazione del sistema di sicurezza di VShield" a pagina 23.

Scansione su richiesta 4

Definizione della scansione su richiesta

La scansione su richiesta è uno dei tre componenti della strategia di protezione utilizzata da VirusScan per Windows 3.1*x*. Gli altri componenti sono la scansione all'accesso e la scansione pianificata.

La scansione su richiesta consente di eseguire scansioni di elementi specifici durante le normali operazioni e scansioni di nuovi supporti o di file specifici per rilevare l'eventuale presenza di virus nel computer. VirusScan rileva immediatamente i virus conosciuti, siano essi di boot, di file, di tipo camuffati, multipartito, cifrati e polimorfi presenti nei file, nelle unità e nei dischetti.

In questo capitolo sono illustrate le procedure per avviare il componente su richiesta di VirusScan, nonché le procedure necessarie per configurare e personalizzare le funzioni di scansione.

Avvio di VirusScan

Per avviare VirusScan, fare doppio clic sull'icona VirusScan nel gruppo di programmi VirusScan. Durante l'operazione di caricamento, VirusScan effettua un controllo dei propri file di programma e della memoria del computer per verificare che non siano infetti da virus.

Una volta completato il controllo, viene visualizzata la finestra principale di VirusScan (Figura 4-1), con la pagina Rilevamento in primo piano.

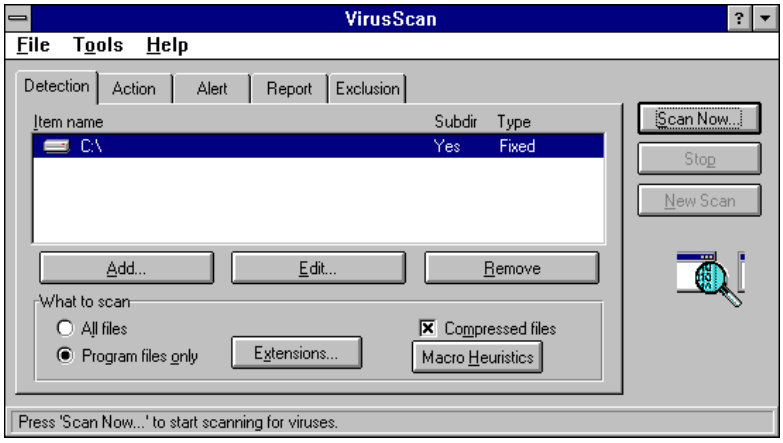

Figura 4-1.. Finestra principale di VirusScan (pagina Rilevamento)

NOTA: Se VirusScan non riesce ad eseguire il controllo o esce da Windows durante l'operazione di caricamento, spegnere il computer ed eseguire il programma dalla riga di comando VirusScan dal disco di emergenza. Per le istruzioni relative alla creazione di un disco di emergenza, vedere "Creazione di un disco di emergenza" a pagina 76.

Nella finestra principale è possibile configurare le impostazioni della scansione, avviare la scansione su richiesta, visualizzare il registro attività e l'elenco dei virus, stampare rapporti e visualizzare i risultati della scansione.

Configurazione della scansione su richiesta

È possibile accedere alle funzioni configurabili di VirusScan attraverso cinque pagine - scheda. Nelle sezioni successive, è illustrato come utilizzare tali pagine allo scopo di configurare VirusScan in base alle proprie esigenze.

Configurazione del rilevamento di VirusScan

Prima di eseguire la scansione o di pulire il sistema con VirusScan, è necessario specificare gli elementi da includere nella scansione attraverso la pagina Rilevamento.

Per selezionare le unità, le directory o i file da sottoporre a scansione, procedere come segue:

1. Avviare VirusScan. Viene visualizzata la finestra principale di VirusScan, con la pagina Rilevamento in primo piano (Figura 4-1 a pagina 25).
2. Per aggiungere un elemento alla scansione, fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo Aggiungi elemento alla scansione (Figura 4-2 a pagina 27). (L'unità C: viene selezionata per impostazione predefinita.)

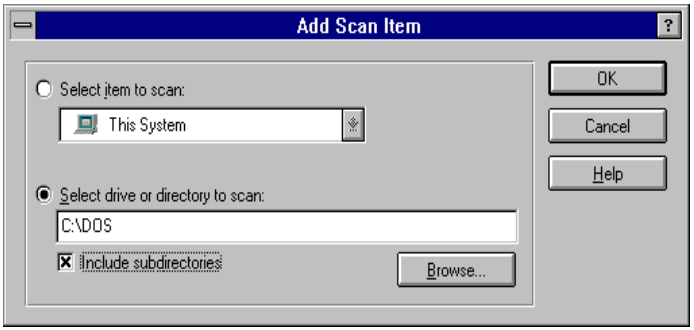

Figura 4-2.. Finestra di dialogo Aggiungi elemento di scansione

3. Per aggiungere gruppi di unità o di supporti, selezionare **Selezionare elemento per la scansione**, quindi scegliere una delle seguenti opzioni:

   – **Risorse del computer** esegue la scansione di tutti i volumi fissi, rimovibili e di rete collegati al computer.

   – **Tutti i supporti rimovibili** consente la scansione di tutti i supporti rimovibili locali, ad esempio i dischi floppy e i CD-ROM.

   – **Tutti i dischi fissi** consente la scansione di tutte le unità disco rigido locali.

   – **Tutte le unità di rete** esegue la scansione di tutti i volumi di rete mappati.

   NOTA: Verranno sottoposte a scansione tutte le directory e le sottodirectory presenti nella posizione selezionata.

   ---

4. Per aggiungere un'unità, un file o una cartella specifica, selezionare **Seleziona unità o directory per la scansione** ed eseguire una delle operazioni riportate di seguito:

   – Fare clic nella casella di testo e specificare il percorso per l'elemento da sottoporre a scansione.

   – Fare clic su **Sfoglia** per accedere al file, all'unità o alla cartella.

5. È possibile selezionare Includi sottodirectory per sottoporre a scansione le sottodirectory nell'unità o nella directory selezionata al Passaggio 4.

6. Fare clic su **OK**. Gli elementi selezionati vengono visualizzati nell'elenco Selezioni.

7. Per rimuovere un elemento dall'elenco di scansione, selezionarlo e fare clic su **Rimuovi**. L'elemento verrà eliminato.

8. Selezionare i tipi di file che si desidera sottoporre a scansione.

   - Selezionare **Tutti i file** per sottoporre a scansione tutti i file, indipendentemente dal tipo. La scansione sarà più completa, ma meno rapida.
   - Selezionare **Solo file di programma** per sottoporre a scansione solo i file con determinate estensioni. Per modificare le estensioni incluse in questo elenco, fare clic su **Estensioni**.

     NOTA: Le estensioni predefinite sono .EXE, .COM, .DO? e .XL? (il punto interrogativo è un carattere jolly). In base a questo elenco, saranno sottoposti a scansione i file di documento e modello di Word ed Excel (.DOC, .DOT, .XLS e .XLT), così come i file di programma.

   - Selezionare **File compressi** per eseguire la scansione dei file interni compressi con PKLITE o LZEXE.

9. Opzionalmente, fare clic su **Euristica macro** per impostare la scansione utilizzata da VirusScan per ripulire dai virus macro i documenti di Microsoft Word ed Excel. Viene visualizzata la finestra di dialogo Impostazioni di scansione euristica delle macro (Figura 4-3).

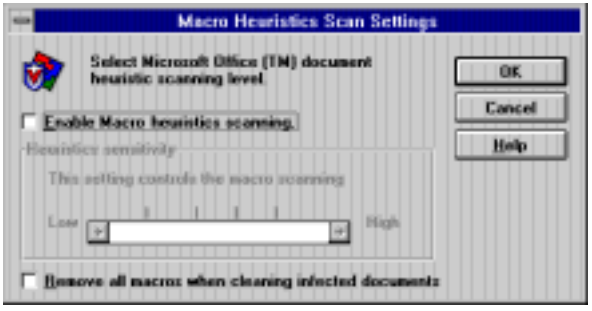

Figura 4-3.. Finestra di dialogo Impostazioni di scansione euristica delle macro

a. Attivare e disattivare la scansione euristica delle macro. In base all'impostazione predefinita, è attivata.

b. Utilizzare il dispositivo di scorrimento per impostare la sensibilità della scansione.

c. Stabilire se si desidera che VirusScan rimuova le macro quando pulisce documenti infetti. In base all'impostazione predefinita, VirusScan rimuove le macro.

d. Fare clic su **OK**.

NOTA: Se si porta il dispositivo di scorrimento su Alto *e* si seleziona Rimuovi macro durante pulitura documenti infetti, VirusScan rimuove tutte le macro da ciascun documento di Word o Excel sottoposto a scansione e non solo le macro simili a virus.

---

10. Utilizzare uno dei metodi riportati di seguito:

- Se si desidera salvare queste selezioni in un file di impostazioni, vedere "Salvataggio delle impostazioni di scansione" a pagina 37.
- Per configurare ulteriormente VirusScan, selezionare un'altra pagina.
- Per eseguire subito la scansione utilizzando le impostazioni correnti, fare clic su **Scansione**.
- Per bloccare e proteggere tramite password tali impostazioni, vedere "Utilizzo della protezione tramite password" a pagina 41.

Configurazione delle azioni di VirusScan

Per definire le azioni che VirusScan eseguirà al rilevamento di un virus, eseguire la procedura riportata di seguito:

1. Avviare VirusScan e selezionare la pagina Azione. Viene visualizzata la finestra principale di VirusScan con la pagina Azione in primo piano (Figura 4-4 a pagina 30).

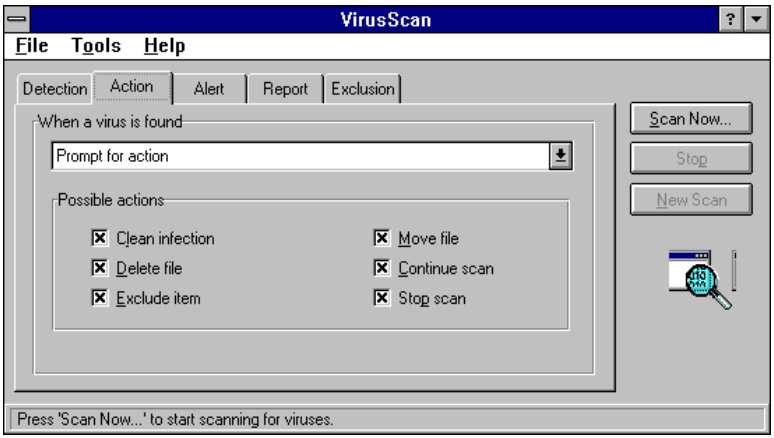

Figura 4-4.. Finestra principale di VirusScan (pagina Azione)

2. Selezionare una delle seguenti azioni:

   - **Richiedi azione**: se si utilizza questa opzione, quando rileva un virus VirusScan richiede di specificare l'azione desiderata. Utilizzare questa opzione se è prevista la presenza di un utente durante la scansione.

     NOTA: Scegliere le azioni disponibili per l'utente selezionando le caselle di controllo appropriate in Azioni possibili.

   - **Sposta file infetti in una directory**: selezionare questa opzione se si desidera che VirusScan sposti automaticamente tutti i file infetti in una directory di quarantena.

     NOTA: Sarà necessario specificare la directory nella quale si desidera spostare i file. La directory predefinita è **\infetti**. A meno che non si specifichi l'intero percorso (ad esempio., **C:\personale\infetti**), VirusScan creerà la cartella nella directory principale dell'unità nella quale il virus è stato rilevato (ad esempio., **C:\infetti**).

- **Pulisci file infetti**: utilizzare questa opzione se si desidera che VirusScan elimini automaticamente i virus dai file infetti.
- **Elimina file infetti**: selezionare questa opzione se si desidera che VirusScan elimini automaticamente i file infetti rilevati.

NOTA: In tal modo, i file infetti verranno rimossi in modo definitivo dal sistema. Sarà necessario ripristinare i file eliminati dalle copie di backup.

- **Continua scansione**: utilizzare questa opzione se si desidera ignorare i file infetti e continuare la scansione. In questo modo, VirusScan non esegue alcuna azione quando rileva un virus.

3. Utilizzare uno dei metodi riportati di seguito:
   - Se si desidera salvare queste selezioni in un file di impostazioni, vedere "Salvataggio delle impostazioni di scansione" a pagina 37.
   - Per configurare ulteriormente VirusScan, selezionare un'altra pagina.
   - Per eseguire subito la scansione utilizzando le impostazioni correnti, fare clic su **Scansione**.
   - Per bloccare e proteggere tramite password tali impostazioni, vedere "Utilizzo della protezione tramite password" a pagina 41.

Configurazione degli avvisi di VirusScan

È possibile configurare VirusScan perché invii un avviso quando rileva la presenza di un virus. Per configurare le funzioni di avviso di VirusScan, procedere come segue:

1. Avviare VirusScan e selezionare la pagina Avviso. Viene visualizzata la finestra principale di VirusScan (Figura 4-5 a pagina 32), con la pagina Avviso in primo piano.

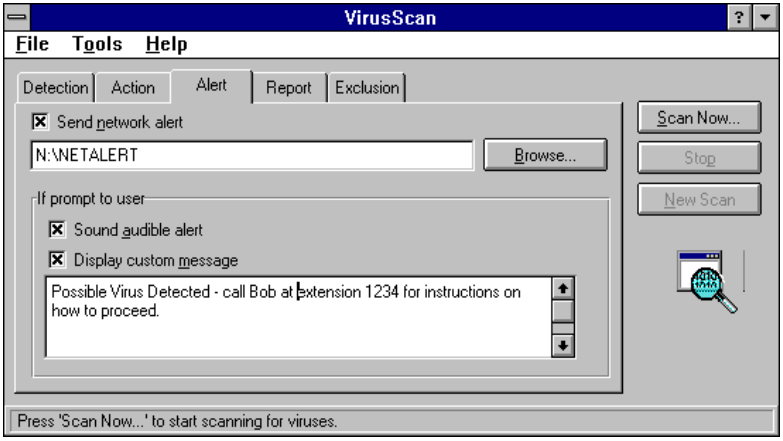

Figura 4-5.. Finestra principale di VirusScan (pagina Avviso)

2. Fare clic su **Invia avviso alla rete** se si desidera che VShield invii un avviso ad un percorso di rete controllato da NetShield, la soluzione antivirus di Network Associates per i server. Fare clic su **Sfoglia** per accedere alla directory desiderata.

NOTA: Questa directory dovrebbe contenere il file dell'avviso centralizzato, CENTALERT.TXT. Per ulteriori informazioni sull'avviso centralizzato, consultare la documentazione relativa a NetShield.

---

3. Se si è selezionato **Richiedi azione** nella pagina Azione, selezionare **Riproduci segnale acustico** e / o **Visualizza messaggio personalizzato**. È possibile personalizzare il messaggio facendo clic nella casella di testo e modificando il relativo testo.
4. Utilizzare uno dei metodi riportati di seguito:
   - Se si desidera salvare queste selezioni in un file di impostazioni, vedere "Salvataggio delle impostazioni di scansione" a pagina 37.
   - Per configurare ulteriormente VirusScan, selezionare un'altra pagina.
   - Per eseguire subito la scansione utilizzando le impostazioni correnti, fare clic su **Scansione**.
   - Per bloccare e proteggere tramite password tali impostazioni, vedere "Utilizzo della protezione tramite password" a pagina 41.

Configurazione dei rapporti di VirusScan

Per configurare la modalità di registrazione dell'attività di VirusScan, procedere come segue:

1. Avviare VirusScan e fare clic sulla pagina Rapporto. Viene visualizzata la finestra principale di VirusScan, con la pagina Rapporto in primo piano (Figura 4-6).

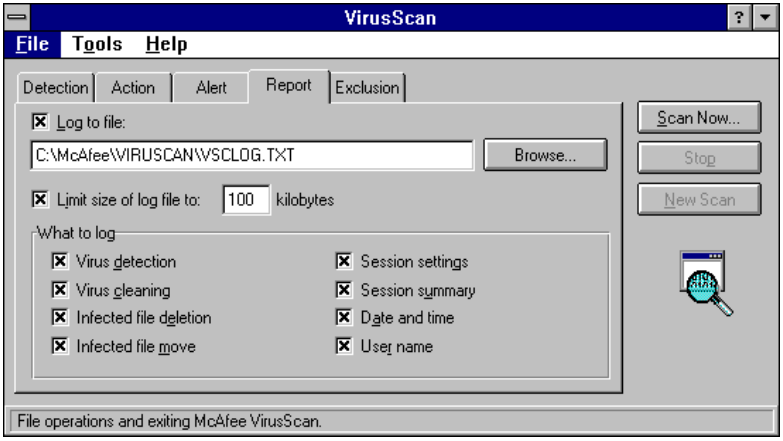

Figura 4-6.. Finestra principale di VirusScan (pagina Rapporto)

2. Selezionare **Registra su file**, quindi effettuare una delle seguenti operazioni:
   - Immettere un percorso e un nome di file nella casella di testo
   - Scegliere un percorso facendo clic sul pulsante **Sfoglia**.
3. Limitare le dimensioni del file di registro selezionando **Limita dimensioni**e specificando la dimensione massima.

NOTA: Il percorso predefinito per il file di registro è **C:\Neta\Viruscan\VSHLOG.TXT**. È un semplice file di testo che è possibile visualizzare utilizzando un qualsiasi editor di testi (ad esempio Blocco note) oppure selezionando **Visualizza registro attività** dal menu File.

---

4. Scegliere le informazioni da includere nel file di registro. Le opzioni includono:
   - Rilevamento virus
   - Pulizia virus
   - Eliminazione file infetti
   - Spostamento file infetti
   - Impostazioni sessione
   - Riepilogo sessione
   - Data e ora
   - Nome utente.
5. Utilizzare uno dei metodi riportati di seguito:
   - Se si desidera salvare queste selezioni in un file di impostazioni, vedere "Salvataggio delle impostazioni di scansione" a pagina 37.
   - Per configurare ulteriormente VirusScan, selezionare un'altra pagina.
   - Per eseguire subito la scansione utilizzando le impostazioni correnti, fare clic su **Scansione**.
   - Per bloccare e proteggere tramite password tali impostazioni, vedere "Utilizzo della protezione tramite password" a pagina 41.

Configurazione delle esclusioni di VirusScan

La pagina Esclusione (Figura 4-7) consente di definire quali file, cartelle o volumi debbano essere esclusi dalla scansione.

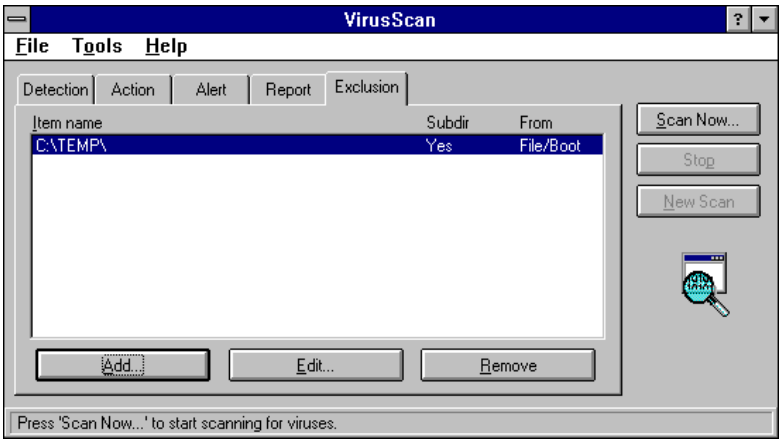

Figura 4-7.. Finestra principale di VirusScan (pagina Esclusione)

NOTA: La cartella **C:\Neta\Viruscan\Infected** viene esclusa automaticamente.

Aggiunta di un elemento all'elenco delle esclusioni

Per aggiungere un elemento all'elenco delle esclusioni, procedere come segue:

1. Nella pagina Esclusione, fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo Escludi elemento (Figura 4-8).

Figura 4-8.. Finestra di dialogo Escludi elemento

2. Digitare il percorso dell'elemento che si desidera escludere oppure fare clic su **Sfoglia**per specificare l'elemento. È possibile escludere un file, una cartella o un intero disco.
3. Selezionare **Includi sottocartelle** se si desidera escludere tutte le sottocartelle all'interno della cartella selezionata.
4. Se lo si desidera escludere la cartella dalla scansione dei file o dalla scansione del settore di boot selezionando le relative caselle.
5. Fare clic su **OK**.
6. Utilizzare uno dei metodi riportati di seguito:
   - Se si desidera salvare queste selezioni in un file di impostazioni, vedere "Salvataggio delle impostazioni di scansione" a pagina 37.
   - Per configurare ulteriormente VirusScan, selezionare un'altra pagina.
   - Per eseguire subito la scansione utilizzando le impostazioni correnti, fare clic su **Scansione**.
   - Per bloccare e proteggere tramite password tali impostazioni, vedere "Utilizzo della protezione tramite password" a pagina 41.

Rimozione di un elemento dall'elenco delle esclusioni

Per rimuovere un elemento dall'elenco, procedere come segue:

1. Nella pagina Esclusione, selezionare l'elemento da rimuovere.
2. Fare clic su **Rimuovi**.
3. Utilizzare uno dei metodi riportati di seguito:
   - Se si desidera salvare queste selezioni in un file di impostazioni, vedere "Salvataggio delle impostazioni di scansione" a pagina 37.
   - Per configurare ulteriormente VirusScan, selezionare un'altra pagina.
   - Per eseguire subito la scansione utilizzando le impostazioni correnti, fare clic su **Scansione**.
   - Per bloccare e proteggere tramite password tali impostazioni, vedere "Utilizzo della protezione tramite password" a pagina 41.

Modifica di un elemento nell'elenco delle esclusioni

Se si desidera modificare un elemento esistente nell'elenco delle esclusioni, procedere come segue:

1. Nella pagina Esclusione, selezionare l'elemento da modificare.
2. Fare clic su **Modifica**.
3. Viene visualizzata la finestra di dialogo Escludi elemento (Figura 4-8 a pagina 35). Apportare le modifiche, quindi fare clic su **OK**.
4. Utilizzare uno dei metodi riportati di seguito:
    - Se si desidera salvare queste selezioni in un file di impostazioni, vedere "Salvataggio delle impostazioni di scansione" a pagina 37.
    - Per configurare ulteriormente VirusScan, selezionare un'altra pagina.
    - Per eseguire subito la scansione utilizzando le impostazioni correnti, fare clic su **Scansione**.
    - Per bloccare e proteggere tramite password tali impostazioni, vedere "Utilizzo della protezione tramite password" a pagina 41.

Salvataggio delle impostazioni di scansione

Il menu File di VirusScan offre due opzioni per il salvataggio delle impostazioni:

- Salva come predefinite
- Salva impostazioni.

In entrambi i casi, le impostazioni verranno salvate in un file .VSC, un file di testo di configurazione contenente le impostazioni di VirusScan. Il nome di ciascuna variabile è seguito dal segno uguale (=) e da un valore che definisce quali impostazioni sono state selezionate per la configurazione di VirusScan.

Le successive sottosezioni indicano quando utilizzare ciascuna opzione di salvataggio.

Quando salvare le opzioni come predefinite

Se si desidera utilizzare una configurazione modificata come impostazione predefinita in VirusScan, scegliere **Salva come predefinite**. Le modifiche verranno salvate nel file DEFAULT.VSC.

Quando salvare le impostazioni

Se è necessaria più di una configurazione VirusScan (nel caso in cui, ad esempio, si desideri sottoporre a scansione due unità locali con impostazioni di VirusScan differenti) è consigliabile selezionare **Salva impostazioni**. Verrà richiesto di immettere un nome per un nuovo file .VSC e le impostazioni correnti di VirusScan verranno salvate in quel file. Una volta salvato il file, sarà possibile utilizzarlo facendo doppio clic sul nome del file in File Manager di Windows.

NOTA: Al primo utilizzo, potrebbe essere necessario associare il file .VSC a VirusScan. Consultare la documentazione di Windows per le istruzioni.

Visualizzazione delle informazioni relative al virus

L'Elenco virus è un elenco completo dei virus rilevati da VirusScan. Esso fornisce una descrizione dei virus che comprende il tipo di infezione, le caratteristiche e le dimensioni del virus e lo stato di pulizia.

Visualizzazione dell’elenco virus

Per visualizzare e utilizzare Elenco virus, procedere come segue:

1. Avviare VirusScan. Viene visualizzata la finestra principale di VirusScan (Figura 4-1 a pagina 25).

2. Selezionare **Elenco virus** dal menu Strumenti. Viene visualizzata la finestra Elenco virus (Figura 4-9).

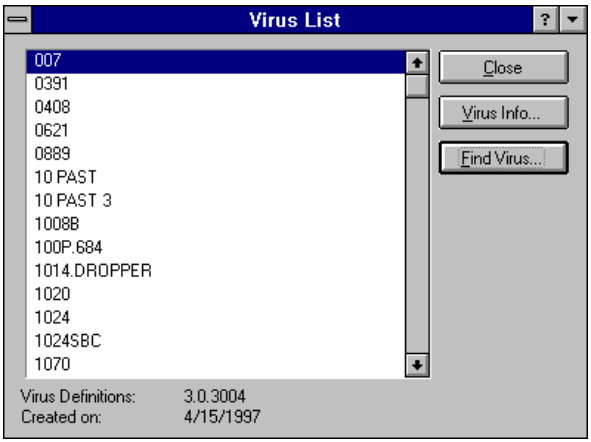

Figura 4-9.. Finestra Elenco virus

3. Per visualizzare le informazioni relative a un virus, Utilizzare uno dei metodi riportati di seguito:

   - Selezionarlo dall'elenco e fare clic su **Info Virus**. Viene visualizzata la finestra Informazioni sui virus (Figura 4-10 a pagina 40).
   - Fare clic su **Trova virus** e digitare il nome del virus nell'apposita casella di testo. Quando il nome del virus desiderato viene visualizzato nell'elenco, chiudere la casella di testo e fare clic su **Info virus**. Viene visualizzata la finestra Informazioni sui virus (Figura 4-10 a pagina 40).

Finestra di informazioni relative a un virus

La finestra di informazioni relative ai virus (Figura 4-10) fornisce informazioni dettagliate sui virus selezionati nella finestra Elenco virus.

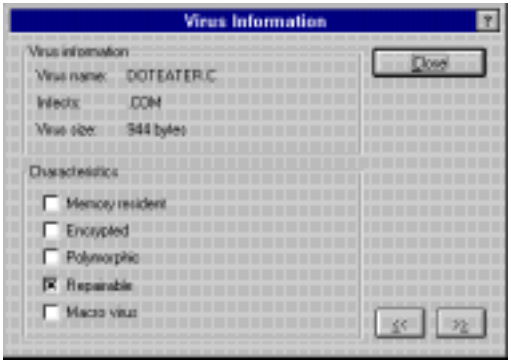

Figura 4-10.. Finestra di informazioni relative ai virus

La sezione Informazioni sui virus fornisce informazioni essenziali sui virus:

- **Nome virusè** il nome del virus.
- **Infetta** indica cosa viene attaccato dal virus, ad esempio i file di un determinato tipo, il settore di boot o il record di boot principale.
- **Dimensione del virus** fornisce le dimensioni del virus in byte.

La sezione Caratteristiche descrive il comportamento del virus selezionato:

- **Residente in memoria** indica che il virus è un programma residente in memoria che agisce in modo simile a un TSR o a un driver di periferica e che rimane attivo in memoria quando il computer è in funzione.
- **Cifrato** indica che il virus tenta di evitare il rilevamento tramite l'autocifratura.
- **Polimorfico** indica che il virus tenta di evitare il rilevamento modificando la propria struttura interna o le tecniche di cifratura.
- **Ripristinabile** indica che è disponibile uno strumento di rimozione per il virus.

- **Dimensione del virus** indica la quantità, espressa in byte, in base alla quale il virus accresce le dimensioni del file che ha infettato.

NOTA: Le dimensioni predefinite di un record di boot principale o di un virus del settore di boot è di 512 byte.

Utilizzo della protezione tramite password

Le impostazioni di VirusScan possono essere protette tramite password per impedire le modifiche non desiderate. Gli amministratori di rete possono utilizzare tale opzione per impedire che gli utenti mettano in pericolo il sistema di sicurezza modificando le impostazioni di VirusScan. Se si desidera utilizzare la protezione tramite password, procedere come segue:

1. Avviare VirusScan. Viene visualizzata la finestra principale di VirusScan (vedere la Figura 4-1 a pagina 25).
2. Dal menu Strumenti, selezionare Protetto da password. Verrà visualizzata la finestra di dialogo Password di protezione (Figura 4-11).

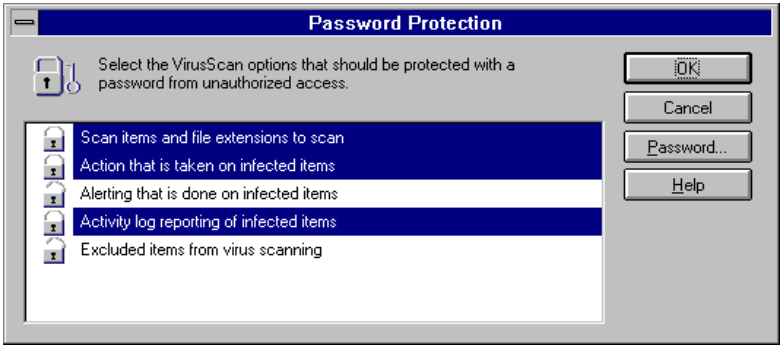

Figura 4-11.. Finestra di dialogo Password di protezione

3. Selezionare dall'elenco gli elementi da proteggere tramite password.
4. Fare clic su **Password** per immettere una password. Verrà richiesto di confermarla.
5. Utilizzare uno dei metodi riportati di seguito:
   - Se si desidera salvare le impostazioni e tornare alla finestra principale, fare clic su **OK**.
   - Se invece si desidera annullare le modifiche e tornare alla finestra principale, fare clic su **Annulla**.

Scansione pianificata 5

La scansione pianificata è uno dei tre componenti della strategia di protezione utilizzata da VirusScan per Windows 3.1*x*. Gli altri componenti sono la scansione all'accesso e la scansione su richiesta. Tramite la scansione pianificata, VirusScan può avviare automaticamente la scansione ad un orario prestabilito. La scansione può essere pianificata una volta, ogni giorno, ogni settimana, ogni mese oppure ogni ora.

In questo capitolo sono illustrate le procedure per l'utilizzo di VirusScan Console per configurare e personalizzare la scansione pianificata.

Utilizzo di VirusScan Console

Utilizzare VirusScan Console (Figura 5-1) per configurare la scansione pianificata. Avviare VirusScan Console facendo doppio clic sulla relativa icona nel gruppo di programmi VirusScan oppure selezionando **McAfee VirusScan Console** dal menu Strumenti di VirusScan.

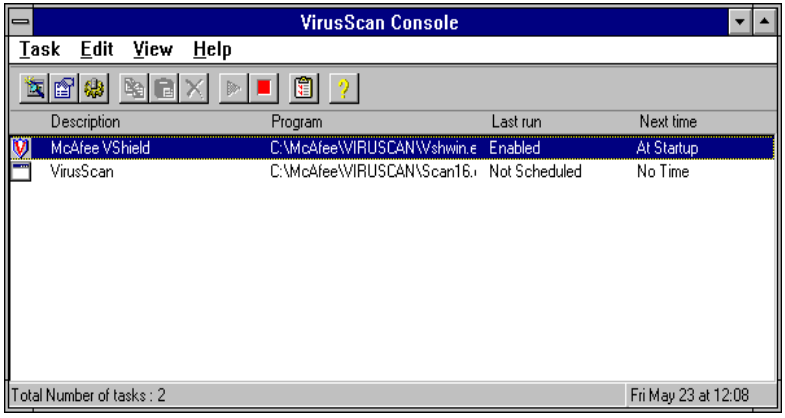

Figura 5-1.. VirusScan Console

Per visualizzare le proprietà di un'attività, fare doppio clic sul relativo nome oppure fare clic con il pulsante destro del mouse sull'attività desiderata e selezionare **Proprietà**. Viene visualizzata la finestra Proprietà attività (Figura 5-2 a pagina 44), con la scheda Programma in primo piano.

Creazione di un'attività di scansione

VirusScan Console utilizza le attività di scansione per gestire e registrare la scansione pianificata. È possibile configurare e programmare ogni attività separatamente, utilizzando le schede della finestra Proprietà attività.

Selezione del programma da eseguire

Per selezionare il programma di una nuova attività di scansione, procedere come segue:

1. In VirusScan Console, scegliere **Nuova attività** dal menu Attività oppure fare clic con il pulsante destro del mouse sull'elenco delle operazioni e selezionare **Nuova attività**. Viene visualizzata la finestra Proprietà attività (Figura 5-2) con la scheda Programma in primo piano.

Figura 5-2.. Finestra Proprietà attività (scheda Programma)

2. La posizione predefinita del file di programma VirusScan (**C:\Neta\Viruscan\SCAN16.EXE**) viene visualizzata automaticamente nel campo Programma. Se lo si desidera, è possibile immettere un altro percorso nella casella di testo oppure cercare l'esatta posizione.
3. Se si desidera utilizzare VirusScan Console per un altro programma, immetterne il percorso nel campo Programma.

NOTA: Per immettere un parametro di programma, è possibile utilizzare il campo Parametro. Ad esempio, se si sta programmando Notepad.exe, è possibile digitare il nome di un file di testo (ad esempio., WHATSNEW.TXT) da aprire all'avvio del programma.

---

4. Immettere il nome dell'attività nel campo Descrizione.
5. Se si desidera impostare una password per l'attività, fare clic su **Imposta password**. La finestra di dialogo visualizzata richiederà la digitazione e la conferma della password.
6. Configurare le opzioni di scansione per l'attività. A tale scopo, consultare "Configurazione di un'attività di scansione" a pagina 48.
7. Fare clic su **Esegui ora** se si desidera avviare subito la scansione.
8. Fare clic su uno dei seguenti pulsanti:
   - **OK** consente di salvare le modifiche e tornare a VirusScan Console.
   - **Annulla** consente di abbandonare le modifiche e tornare a VirusScan Console.
   - **Applica** consente di applicare le modifiche apportate. È quindi possibile selezionare un'altra pagina.

Impostazione della pianificazione dell'attività

Per impostare la pianificazione di un'attività di scansione, procedere come segue:

1. Selezionare la scheda Pianificazione (Figura 5-3). (L'aspetto della finestra varierà leggermente in base all'opzione selezionata.)

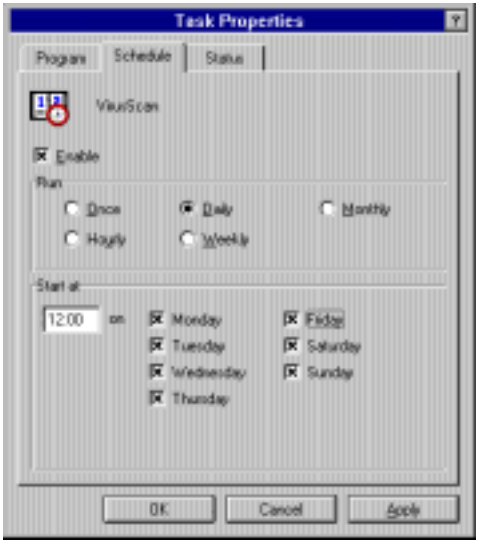

Figura 5-3.. Finestra Proprietà attività (scheda Pianificazione)

2. Selezionare o deselezionare **Attiva** per attivare o disattivare l'operazione.

NOTA: Se non viene attivata, l'attività non verrà inserita nella pianificazione.

---

3. Specificare la frequenza della scansione:
   - Se si seleziona **Una volta**, sarà necessario specificare la data e l'ora dell'attività.
   - Se si seleziona **Ogni giorno**, sarà necessario selezionare i giorni della settimana e l'ora in cui si desidera eseguire l'attività.
   - Se si seleziona **Ogni mese**, sarà necessario selezionare il giorno del mese e l'ora in cui si desidera eseguire l'attività.

– Se si seleziona **Ogni ora**, sarà necessario selezionare di quanti minuti dopo l'ora si desidera eseguire l'attività.

– Se si seleziona **Ogni settimana**, sarà necessario selezionare i giorni e l'ora in cui si desidera eseguire l'attività.

NOTA: L'ora deve essere immessa nel formato 24 ore (ad esempio, 20:27 e non 8:27 p.m.) per tutte le opzioni ad eccezione di **Ogni ora**.

---

4. Fare clic su uno dei seguenti pulsanti:
   - **OK** consente di salvare le modifiche e tornare a VirusScan Console.
   - **Annulla** consente di abbandonare le modifiche e tornare a VirusScan Console.
   - **Applica** consente di applicare le modifiche apportate. È quindi possibile selezionare un'altra pagina.

Visualizzazione delle proprietà dell'attività

1. Se si desidera visualizzare le statistiche relative all'attività corrente, selezionare la scheda Stato (Figura 5-4).

Figura 5-4.. Finestra Proprietà attività (scheda Stato)

2. Fare clic su **OK** per uscire dalla finestra Proprietà attività e tornare a VirusScan Console.

Operazione di scansione copiata, incollata o eliminata

L'elenco delle attività di VirusScan Console consente di copiare o incollare le attività. La creazione di attività diverse con configurazioni simili è resa in tal modo rapida e semplice.

- Per copiare un'attività, scegliere **Copia** dal menu Modifica oppure fare clic con il pulsante destro del mouse sull'attività desiderata e selezionare **Copia**.
- Per incollare un'attività, selezionare **Incolla** dal menu Modifica oppure fare clic con il pulsante destro del mouse sull'elenco delle attività e scegliere **Incolla**.
- Per eliminare un'attività, selezionare l'attività e premere **CANC**.

Configurazione di un'attività di scansione

Per configurare il percorso e il tipo di elemento che si desidera sottoporre a scansione con VirusScan, fare clic su **Configura** sulla scheda Programma della finestra Proprietà attività. Viene visualizzata la finestra di configurazione, con la pagina Rilevamento in primo piano (Figura 5-5).

Figura 5-5.. Finestra di configurazione (pagina Rilevamento)

La finestra di configurazione è suddivisa in cinque pagine - scheda. Per passare da una all'altra, fare clic sulla pagina desiderata nella parte superiore della finestra. Le sezioni successive forniscono una descrizione dettagliata di ciascuna scheda.

Utilizzo della pagina Rilevamento

Utilizzare la pagina Rilevamento per specificare quali unità, file e cartelle sottoporre a scansione con VirusScan. Per configurare le opzioni di rilevamento per una scansione, procedere come segue:

1. Aggiungere uno o più elementi all'elenco di scansione. Per aggiungere un elemento all'elenco di scansione, selezionarlo da Seleziona elemento per la scansione.
   - **Risorse del computer** esegue la scansione di tutti i volumi fissi, rimovibili e di rete collegati al computer.
   - **Tutti i supporti rimovibili** esegue la scansione di tutti i supporti rimovibili locali, ad esempio i dischi floppy e i CD-ROM.
   - **Tutti i dischi fissi** esegue la scansione di tutte le unità disco rigido locali.
   - **Tutte le unità di rete** esegue la scansione di tutti i volumi di rete mappati.

   NOTA: Verranno sottoposte a scansione tutte le directory e le sottodirectory presenti nella posizione selezionata.

2. Aggiungere una specifica unità, file o cartella. Fare clic su **Seleziona unità o cartella per la scansione** e indicare il percorso dell'elemento da sottoporre a scansione.

   NOTA: Fare clic su **Sfoglia** per accedere al file, all'unità o alla cartella.

3. Fare clic su **OK**. Gli elementi selezionati vengono visualizzati nell'elenco Selezioni.
4. Per rimuovere un elemento dall'elenco delle scansioni, selezionarlo dall'elenco e fare clic su **Rimuovi**.

5. Selezionare i tipi di file che si desidera sottoporre a scansione con VirusScan.

   - **Tutti i file** sottopone a scansione tutti i file, indipendentemente dal tipo. La scansione sarà più completa, ma meno rapida.
   - **Solo file di programmi** sottopone a scansione solo i file con determinate estensioni. Per modificare le estensioni incluse in questo elenco, fare clic su **Estensioni**.

     NOTA: Le estensioni predefinite sono .EXE, .COM, .DO? e .XL? (il punto interrogativo è un carattere jolly). In base a questo elenco, saranno sottoposti a scansione i file di documento e modello di Word ed Excel (.DOC, .DOT, .XLS e .XLT), così come i file di programma.

   - **File compressi** esegue la scansione dei file compressi con PKLITE o LZEXE.

6. Selezionare **Scansione memoria** se si desidera sottoporre a scansione la memoria del computer per rilevare la presenza di virus.
7. Selezionare **Avvia automaticamente** se si desidera che l'attività si avvii automaticamente all'ora pianificata.

   NOTA: Se non si seleziona **Avvia automaticamente**, VirusScan verrà avviato all'ora pianificata, ma l'attività non verrà eseguita fino a quando non si farà clic su **Avvia scansione**.

   ---

8. Selezionare **Scansione settori di boot** se si desidera sottoporre a scansione il settore o i settori di boot dell'unità o delle unità specificate nell'attività.
9. Opzionalmente, fare clic su **Euristica macro** per impostare la scansione utilizzata da VirusScan per ripulire dai virus macro i documenti di Microsoft Word ed Excel. Viene visualizzata la finestra di dialogo Impostazioni di scansione euristica delle macro (Figura 5-6 a pagina 51).

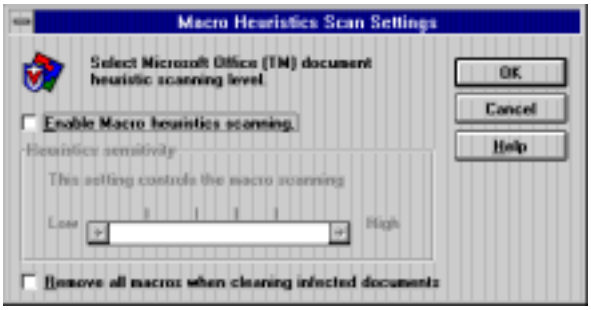

Figura 5-6.. Finestra di dialogo Impostazioni di scansione euristica delle macro

a. Attivare e disattivare la scansione euristica delle macro. In base all'impostazione predefinita, è attivata.

b. Utilizzare il dispositivo di scorrimento per impostare la sensibilità della scansione.

c. Stabilire se si desidera che VirusScan rimuova le macro quando pulisce documenti infetti. In base all'impostazione predefinita, VirusScan rimuove le macro.

NOTA: Se si porta il dispositivo di scorrimento su Alto *e* si seleziona Rimuovi macro durante pulitura documenti infetti, VirusScan rimuove tutte le macro da ciascun documento di Word o Excel sottoposto a scansione e non solo le macro simili a virus.

---

d. Fare clic su **OK**.

10. Utilizzare uno dei metodi riportati di seguito:

- Fare clic su **Applica** per salvare le modifiche.
- Fare clic su **OK** per salvare le modifiche e tornare a VirusScan Console.
- Fare clic su **Annulla**per tornare a VirusScan Console senza aver salvato le modifiche.
- Se si desidera bloccare e proteggere le modifiche tramite password, vedere "Utilizzo della pagina Sicurezza" a pagina 59 se si desidera bloccare e proteggere le modifiche tramite password.

Utilizzo della pagina Azione

Utilizzare la pagina Azione per definire la strategia che VirusScan adotterà al rilevamento di un virus.

Per configurare le opzioni di azione per una scansione, procedere come segue:

1. Selezionare la pagina Azione. Viene visualizzata la finestra di configurazione con la pagina Azione in primo piano (Figura 5-7).

Figura 5-7.. Finestra di configurazione (pagina Azione)

2. Fare clic sulla freccia situata accanto alla casella di riepilogo, quindi selezionare un'azione dall'elenco:

   - **Richiedi azione**: VirusScan chiederà quale azione eseguire ogni volta che rileva un virus. Utilizzare questa opzione se è prevista la presenza di un utente durante la scansione.

     Scegliere le azioni disponibili per VirusScan selezionando le caselle di controllo appropriate in Azioni possibili.

- **Sposta file infetti in una cartella** consente di spostare automaticamente tutti i file infetti in una cartella di quarantena.

  Sarà necessario specificare la cartella nella quale si desidera spostare i file. La directory predefinita è **\Infetti**. A meno che non si specifichi l'intero percorso, (ad esempio, **C:\Personale\Infetti**), VirusScan creerà la cartella nella directory principale dell'unità nella quale il virus è stato rilevato (ad esempio, **C:\Infetti**).

- **Pulisci file infetti** elimina automaticamente i virus dai file infetti.
- **Elimina file infetti** elimina automaticamente i file infetti.

NOTA: In questo modo, i file infetti verranno rimossi in modo permanente dal sistema. Sarà necessario ripristinare i file eliminati dalle copie di backup.

- **Continua scansione**: selezionando tale opzione, VirusScan continua la scansione e non esegue alcuna azione quando rileva un virus.

3. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche.
   - Fare clic su **OK** per salvare le modifiche e tornare a VirusScan Console.
   - Fare clic su **Annulla**per tornare a VirusScan Console senza aver salvato le modifiche.
   - Se si desidera bloccare e proteggere le modifiche tramite password, vedere "Utilizzo della pagina Sicurezza" a pagina 59 se si desidera bloccare e proteggere le modifiche tramite password.

Utilizzo della pagina Avviso

Utilizzare la pagina Avviso per indicare il metodo che VirusScan dovrà impiegare per notificare il rilevamento di un virus. Per configurare le opzioni di avviso per una scansione, procedere come segue:

1. Selezionare la pagina Avviso. Viene visualizzata la finestra di configurazione, con la pagina Avviso in primo piano (Figura 5-8 a pagina 54).

Figura 5-8.. Finestra di configurazione (pagina Avviso)

2. Se si desidera che VirusScan invii un avviso di rete ad un server che esegue NetShield, selezionare **Invia avviso di rete** e specificare il percorso del file di avviso.

NOTA: Il percorso dovrà essere indirizzato alla cartella contenente il file di avviso centralizzato, CENTALERT.TXT. Per ulteriori informazioni sull'avviso centralizzato, consultare la documentazione di NetShield.

---

3. Se è stata selezionata l'opzione **Richiedi azione** nella pagina Azione, selezionare le caselle appropriate in modo che VirusScan emetta un segnale acustico e/o visualizzi un messaggio personalizzato. È possibile modificare il messaggio personalizzato digitando il nuovo testo nella casella di testo.
4. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche.
   - Fare clic su **OK** per salvare le modifiche e tornare a VirusScan Console.

- Fare clic su **Annulla** per tornare a VirusScan Console senza aver salvato le modifiche.
- Se si desidera bloccare e proteggere le modifiche tramite password, vedere "Utilizzo della pagina Sicurezza" a pagina 59 se si desidera bloccare e proteggere le modifiche tramite password.

Utilizzo della pagina Rapporto

Utilizzare la pagina Rapporto per specificare se VirusScan debba registrare le azioni e, nel caso, quali informazioni includere nel registro. Per configurare le opzioni di rapporto per una scansione, procedere come segue:

1. Selezionare la pagina Rapporto. Viene visualizzata la finestra di configurazione con la pagina Rapporto in primo piano (Figura 5-9).

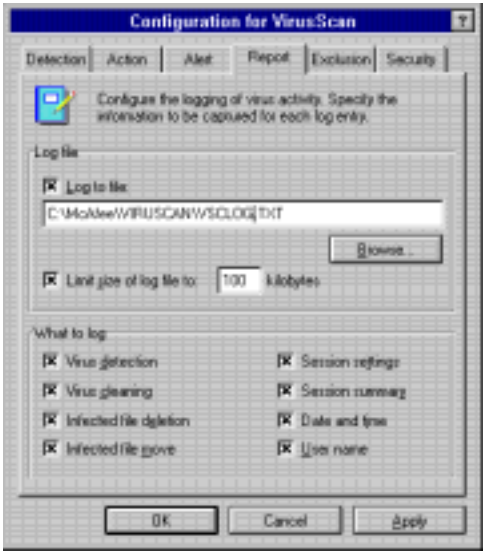

Figura 5-9.. Finestra di configurazione (pagina Rapporto)

2. Per consentire la registrazione dell'attività di scansione , selezionare **Registra su file** e immettere il percorso ad un file di testo.

   Il percorso predefinito è **C:\neta\virusscan\VSCLOG.TXT**. È un semplice file di testo che è possibile visualizzare utilizzando un qualsiasi editor di testi, ad esempio Blocco note, oppure selezionando **Visualizza registro attività** dal menu File.

3. Se si desidera limitare le dimensioni del file di registro, fare clic sulla casella di controllo **Limita dimensioni file di registro a** e specificare una dimensione massima.
4. Selezionare le caselle di controllo desiderate per specificare quali informazioni includere nel file di registro. Le opzioni disponibili sono:
   - Rilevamento virus
   - Pulizia virus
   - Eliminazione file infetti
   - Spostamento file infetti
   - Impostazioni sessione
   - Riepilogo sessione
   - Data e ora
   - Nome utente.
5. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche.
   - Fare clic su **OK** per salvare le modifiche e tornare a VirusScan Console.
   - Fare clic su **Annulla** per tornare a VirusScan Console senza aver salvato le modifiche.
   - Se si desidera bloccare e proteggere le modifiche tramite password, vedere "Utilizzo della pagina Sicurezza" a pagina 59 se si desidera bloccare e proteggere le modifiche tramite password.

Utilizzo della pagina Esclusione

Utilizzare la pagina Esclusione (Figura 5-10) per indicare quali file, cartelle o volumi escludere dalla scansione effettuata da VirusScan.

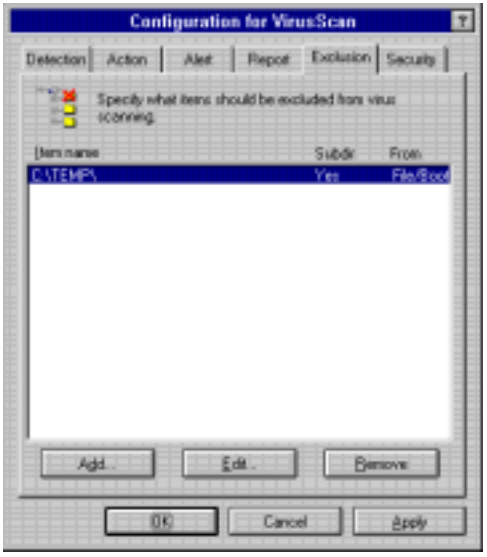

Figura 5-10.. Finestra di configurazione (pagina Esclusione)

Aggiunta di un elemento all'elenco delle esclusioni

Se si desidera aggiungere un elemento all'elenco delle esclusioni, procedere come segue:

1. Nella pagina Esclusione, fare clic su **Aggiungi**. Viene visualizzata la finestra di dialogo Escludi elemento (Figura 5-11).

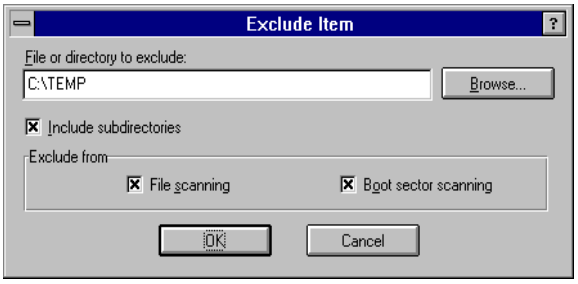

Figura 5-11.. Finestra di dialogo Escludi elemento

2. Immettere il percorso per l'elemento che si desidera escludere oppure fare clic su **Sfoglia** per individuarlo. È possibile escludere un file, una cartella o un intero disco.
3. Selezionare **Includi sottocartelle** se non si desidera che VirusScan sottoponga a scansione le sottocartelle della cartella esclusa.
4. Indicare se si desidera escludere la cartella dalla scansione dei file o dalla scansione del settore di boot selezionando la casella o le caselle appropriate.
5. Fare clic su **OK**.
6. Selezionare il tipo o i tipi di scansione da cui si desidera escludere l'elemento:
   - Per escludere l'elemento dalla scansione dei file, selezionare **Scansione file**
   - Per escludere l'elemento dalla scansione del settore di boot, selezionare **Scansione settore di boot**.
7. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche.
   - Fare clic su **OK** per salvare le modifiche e tornare a VirusScan Console.
   - Fare clic su **Annulla** per tornare a VirusScan Console senza aver salvato le modifiche.
   - Se si desidera bloccare e proteggere le modifiche tramite password, vedere "Utilizzo della pagina Sicurezza" a pagina 59 se si desidera bloccare e proteggere le modifiche tramite password.

Rimozione di un elemento dall'elenco delle esclusioni

Per rimuovere un elemento dall'elenco, procedere come segue:

1. Nella pagina Esclusione, selezionare l'elemento che si desidera rimuovere e quindi fare clic su **Rimuovi**.
2. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche.
   - Fare clic su **OK** per salvare le modifiche e tornare a VirusScan Console.

- Fare clic su **Annulla** per tornare a VirusScan Console senza aver salvato le modifiche.
- Se si desidera bloccare e proteggere le modifiche tramite password, vedere "Utilizzo della pagina Sicurezza" a pagina 59 se si desidera bloccare e proteggere le modifiche tramite password.

Modifica di un elemento nell'elenco delle esclusioni

Per modificare un elemento esistente nell'elenco delle esclusioni, procedere come segue:

1. Nella pagina Esclusione, selezionare l'elemento che si desidera modificare e fare clic su **Modifica**.
2. Viene visualizzata la finestra di dialogo Escludi elemento (Figura 5-11 a pagina 57). Apportare le modifiche desiderate, quindi fare clic su OK.
3. Utilizzare uno dei metodi riportati di seguito:
   - Fare clic su **Applica** per salvare le modifiche.
   - Fare clic su **OK** per salvare le modifiche e tornare a VirusScan Console.
   - Fare clic su **Annulla** per tornare a VirusScan Console senza aver salvato le modifiche.
   - Se si desidera bloccare e proteggere le modifiche tramite password, vedere "Utilizzo della pagina Sicurezza" a pagina 59 se si desidera bloccare e proteggere le modifiche tramite password.

Utilizzo della pagina Sicurezza

Utilizzare la pagina Sicurezza per proteggere le impostazioni di VirusScan e impedire modifiche involontarie. Per configurare le opzioni di sicurezza per una scansione, procedere come segue:

1. Selezionare la pagina Sicurezza (Figura 5-12 a pagina 60).

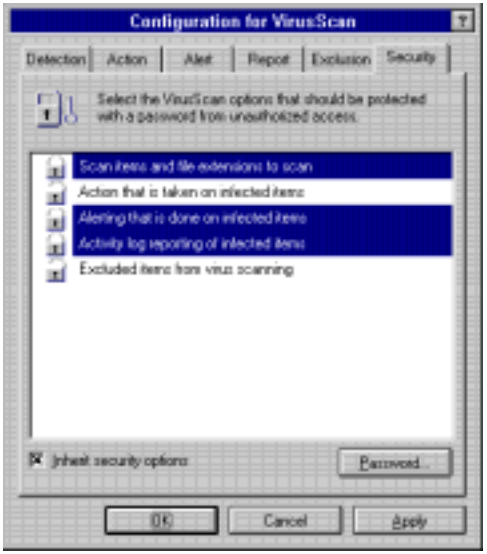

Figura 5-12.. Finestra di configurazione (pagina Sicurezza)

2. Selezionare le impostazioni di VirusScan che si desidera proteggere tramite password:
   - **Elementi di scansione ed estensioni di file da scandire**
   - **Azione intrapresa su elementi infetti**
   - **Avviso su elementi infetti**
   - **Rapporto registro attività di elementi infetti**
   - **Elementi esclusi dalla scansione di virus**.

NOTA: Le impostazioni protette da password verranno evidenziate nell'elenco e il lucchetto alla loro sinistra sarà chiuso.

---

3. Selezionare la casella di controllo **Usa opzioni di sicurezza** se si desidera che le opzioni selezionate siano presenti per impostazione predefinita nelle copie dell'attività.

NOTA: Se si seleziona **Usa opzioni di sicurezza** per l'attività principale di VirusScan, le opzioni di sicurezza di tale attività verranno utilizzate sia per **tutte** le nuove attività che per le copie dell'attività principale di VirusScan.

---

4. Se non è ancora stata impostata una password, impostarne una facendo clic sul pulsante **Password**. Verrà richiesto di immettere e confermare la password.

   Se è già stata impostata una password, è possibile cambiarla in qualsiasi momento facendo clic su **Password**. Verrà richiesto di immettere e confermare la nuova password.

5. Utilizzare uno dei metodi riportati di seguito:

   - Fare clic su **Applica** per salvare le modifiche.
   - Fare clic su **OK** per salvare le modifiche e tornare a VirusScan Console.
   - Fare clic su **Annulla** per tornare a VirusScan Console senza aver salvato le modifiche.

Rimozione dei virus 6

Se si sospetta la presenza di un virus

Se si sospetta o si è certi della presenza di un virus nel sistema prima dell'installazione di VirusScan per Windows 3.1*x*, attenersi alla seguente procedura per creare un ambiente di lavoro privo di virus.

1. Spegnere il computer.

   NOTA: Non riavviare il computer utilizzando il pulsante di reset né la combinazione di tasti CTRL+ALT+CANC poiché con queste procedure alcuni virus potrebbero rimanere intatti.

2. Creare un disco di emergenza. Per ulteriori dettagli vedere la sezione "Creazione di un disco di emergenza" a pagina 76.
3. Inserire il disco di emergenza nell'unità disco A:, quindi accendere il computer.
4. Utilizzare uno dei metodi riportati di seguito:
   - Se si è creato il disco di emergenza con il programma di utility apposito, seguire semplicemente le istruzioni riportate sullo schermo.
   - Se si utilizza un dischetto di boot creato manualmente, digitare:

     ```
     SCAN /ADL /ALL /CLEAN
     ```

     al prompt dei comandi . In questo modo verrà avviata la versione di VirusScan che utilizza i comandi DOS e comparirà il relativo stato di avanzamento.

   NOTA: Per informazioni dettagliate sulle opzioni della riga di comando di VirusScan, vedere Appendice D, "Riferimento".

Se i virus sono stati rimossi

Se VirusScan riesce a rimuovere tutti i virus, spegnere il computer ed estrarre il dischetto. Riavviare il computer e riprendere le attività iniziate precedentemente. Se si stava installando VirusScan, iniziare la procedura di installazione descritta nel Capitolo 2, "Installazione di VirusScan".

Per individuare ed eliminare l'origine dell'infezione, eseguire la scansione di tutti i dischetti subito dopo l'installazione.

Se i virus non sono stati rimossi

Se VirusScan non è in grado di rimuovere un virus, viene visualizzato uno dei seguenti messaggi:

- Impossibile rimuovere il virus.
- Nessuno strumento di rimozione disponibile per questo virus.

Se viene visualizzato uno dei suddetti messaggi, fare riferimento alla documentazione contenuta nel sito Web Network Associates relativa alla rimozione manuale dei virus. Per informazioni dirette, vedere "Come contattare il servizio clienti" a pagina xiv.

Se VirusScan rileva la presenza di un virus

I virus attaccano il sistema infettando i file, di solito i programmi eseguibili o i documenti. Spesso questi file vengono danneggiati nel momento stesso in cui si verifica l'infezione. VirusScan elimina la maggior parte delle infezioni da virus dai file. Tuttavia, alcuni virus sono progettati per danneggiare i file in modo irreparabile. Questi file "danneggiati" irreversibilmente possono essere spostati da VirusScan in una directory di quarantena o eliminati del tutto per prevenire la diffusione dell'infezione nel sistema.

Rimozione di un virus rilevato in un file

Se VirusScan rileva la presenza di un virus in un file, adotterà le misure specificate nel processo di configurazione. Vedere "Configurazione delle azioni di VShield" a pagina 15.

Rimozione di un virus rilevato nella memoria

Se VirusScan rileva un virus nel sistema, pulire subito il sistema allo scopo di prevenire la diffusione del virus all'interno del PC o della rete. Rimuovere i virus dai file qualora si è certi o si sospetta che siano infetti.

Se un virus è residente in memoria o se ha infettato il record MBR (Master Boot Record) o il settore di avvio, spegnere il computer e riavviarlo dal disco di emergenza. Quindi rimuovere il virus utilizzando i comandi DOS di VirusScan. Per ulteriori informazioni, vedere "Se si sospetta la presenza di un virus" a pagina 63 e Appendice C, "Installazioni condivise". Se è stato rilevato un virus in memoria, assicurarsi di utilizzare soltanto lo scanner della riga di comando per pulire il sistema.

Falsi allarmi

Un falso allarme è la segnalazione di un virus in un file o nella memoria quando non è effettivamente presente alcun virus. I falsi allarmi possono verificarsi quando si utilizzano più programmi software antivirus, in quanto alcuni registrano nella memoria le stringhe relative alle firme dei virus senza alcuna protezione. Di conseguenza, VirusScan potrebbe "rilevare" tale codice e considerarlo alla stregua dei virus. I falsi allarmi potrebbero essere generati dal BIOS del sistema, dall'uso di codici di convalida, nonché da fattori di altra natura.

Considerare sempre i virus rilevati da VirusScan come reali e pericolosi ed eseguire le operazioni necessarie per rimuoverli dal sistema. Tuttavia, se si hanno ragioni valide per ritenere che VirusScan generi falsi allarmi (ad esempio, se ha rilevato un virus in un solo file utilizzato senza problemi per anni), consultare il seguente elenco di origini potenziali:

- Se sono in esecuzione più programmi antivirus, VirusScan potrebbe inviare un falso allarme. Configurare il computer in modo che sia in esecuzione un solo programma antivirus alla volta. Nel file AUTOEXEC.BAT eliminare le righe che si riferiscono ad altri programmi antivirus. Spegnere il computer, attendere alcuni secondi e riaccenderlo per assicurarsi che tutto il codice degli altri programmi antivirus sia stato eliminato dalla memoria.
- Alcuni chip BIOS includono una funzione antivirus che potrebbe essere l'origine dei falsi allarmi. Per ulteriori dettagli, consultare il manuale di riferimento del computer.

- Se si impostano i codici di convalida / ripristino, con le scansioni successive verranno rilevati dei cambiamenti nei file convalidati. Questo può generare falsi allarmi in presenza di file eseguibili ad automodifica o autocontrollo. Quando si utilizzano i codici di convalida, specificare un elenco di eccezioni per escludere tali file dal controllo.
- Alcuni PC Hewlett-Packard e Zenith della precedente generazione modificano il settore di boot ad ogni avvio del sistema. VirusScan potrebbe rilevare queste modifiche come possibili infezioni, anche se potrebbe non essere presente alcun virus. Consultare il manuale di riferimento del computer per determinare se il PC presenta un codice che si automodifica. Per risolvere questo problema, salvare le informazioni di convalida / ripristino negli stessi file eseguibili; con questo metodo non si salvano le informazioni sul settore di boot o sul record MBR.
- VirusScan potrebbe segnalare dei virus nel settore di boot o nel record MBR di determinati dischetti protetti da copia.

Network Associates Servizi di assistenza

A

La scelta dell'antivirus e del software di protezione di Network Associates assicura il funzionamento uniforme ed efficace della tecnologia informativa. Il piano di assistenza di Network Associates consente di estendere la protezione ottenuta dal software fornendo agli utenti le informazioni tecniche necessarie per l'installazione, il monitoraggio, la manutenzione e l'aggiornamento del sistema con la tecnologia d'avanguardia di Network Associates. Un piano di assistenza personalizzato per le particolari necessità dell'utente consentirà di ottenere un sistema o una rete che opera in modo affidabile nell'ambiente di elaborazione per mesi o per anni.

I piani di assistenza di Network Associates si dividono in due sezioni principali. Le aziende possono scegliere fra i tre livelli di assistenza del programma PrimeSupport di Network Associates. I proprietari di prodotti Network Associates acquistati presso punti di vendita al dettaglio possono scegliere dal programma Personal Support un piano adeguato alle proprie necessità.

Opzioni PrimeSupport per le aziende

Il programma PrimeSupport di Network Associates dispone delle opzioni Basic, Extended e Anytime. Ciascuna opzione dispone di una gamma di funzioni che forniscono assistenza tempestiva ed economica adeguata alle necessità dell'utente.

PrimeSupport Basic

L'opzione Basic di PrimeSupport fornisce l'accesso tramite telefono all'assistenza di base per i prodotti fornita da personale esperto del supporto tecnico di Network Associates. Se il prodotto Network Associates è stato acquistato con una licenza di abbonamento, l'opzione Basic di PrimeSupport viene fornita come parte del pacchetto per la durata di due anni dalla data di acquisto. Se il prodotto Network Associates è stato acquistato con una licenza senza scadenza, è possibile rinnovare il piano PrimeSupport Basic con una spesa annuale.

PrimeSupport Basic include i seguenti servizi:

- Assistenza tecnica telefonica disponibile dalle 8.00 alle 20.00 (ora degli Stati Uniti centrali), dal lunedì al venerdì.
- Accesso illimitato alle informazioni di supporto di Network Associates, disponibile 24 ore su 24 tramite il sito Web di Network Associates.
- Aggiornamenti ai file di dati e ai prodotti tramite il sito Web di Network Associates.

PrimeSupport Extended

PrimeSupport Extended fornisce un'assistenza preventiva e personalizzata da parte di un rappresentante del supporto tecnico. Si entrerà in contatto con un professionista con una conoscenza approfondita del prodotto Network Associates che contatterà l'utente con una frequenza prestabilita per fornirgli assistenza nell'utilizzo e nella manutenzione dei prodotti Network Associates. Attraverso questo sistema di contatto regolare, il tecnico assegnato a PrimeSupport Extended fornisce la possibilità di prevenire i problemi prima ancora che questi si verifichino. Se tuttavia si verificasse un'emergenza, PrimeSupport Extended fornisce un tempo di risposta previsto che indica all'utente quanto dovrà attendere per ottenere un aiuto. È possibile acquistare PrimeSupport Extended su base annuale quando si acquista un prodotto Network Associates sia con licenza di abbonamento che con licenza senza scadenza.

PrimeSupport Extended include i seguenti servizi:

- Contatto con un rappresentante del supporto tecnico.
- Contatti di assistenza preventiva tramite telefono o posta elettronica da parte del tecnico assegnato ad intervalli prestabiliti.
- Tempi di risposta previsti: il rappresentante del supporto tecnico risponderà entro un'ora alle chiamate effettuate tramite cercapersone, entro quattro ore a chiamate effettuate tramite casella vocale e entro 12 ore a chiamate effettuate tramite posta elettronica.
- Assistenza tecnica telefonica disponibile dalle 7.00 alle 19.00 (ora degli Stati Uniti centrali), dal lunedì al venerdì.
- Accesso illimitato alle informazioni di supporto di Network Associates, disponibile 24 ore su 24 tramite il sito Web di Network Associates.
- Aggiornamenti ai file di dati e ai prodotti tramite il sito Web di Network Associates.
- Possibilità di designare un massimo di cinque persone all'interno dell'azienda per il contatto con i clienti.

PrimeSupport Anytime

PrimeSupport Anytime fornisce l'assistenza preventiva personalizzata 24 ore su 24 per i prodotti Network Associates utilizzati nei sistemi informativi aziendali a tutti i livelli. PrimeSupport Anytime fornisce gli stessi servizi di PrimeSupport Extended 24 ore su 24, sette giorni su sette con tempi di risposta previsti più brevi. È possibile acquistare PrimeSupport Anytime su base annuale quando si acquista un prodotto Network Associates sia con licenza di abbonamento che con licenza senza scadenza.

PrimeSupport Anytime include i seguenti servizi:

- Contatto con un rappresentante del supporto tecnico.
- Contatti di assistenza preventiva tramite telefono o posta elettronica da parte del tecnico assegnato ad intervalli prestabiliti.
- Tempi di risposta previsti: il rappresentante del supporto tecnico risponderà entro mezz'ora alle chiamate effettuate tramite cercapersone, entro un'ora a chiamate effettuate tramite casella vocale ed entro quattro ore a chiamate effettuate tramite posta elettronica.
- Assistenza tecnica telefonica disponibile 24 ore su 24, sette giorni su sette.
- Accesso illimitato alle informazioni di supporto di Network Associates, disponibile 24 ore su 24 tramite il sito Web di Network Associates.
- Aggiornamenti ai file di dati e ai prodotti tramite il sito Web di Network Associates.
- Possibilità di designare un massimo di dieci persone all'interno dell'azienda per il contatto con i clienti.

Tabella A-1. Panoramica di PrimeSupport

Caratteristiche	Basic	Extended	Anytime
Supporto tecnico telefonico	Lunedì - Venerdì 8.00 - 20.00.	Lunedì - Venerdì 7.00 - 19.00.	24 ore su 24, sette giorni su sette
Supporto tecnico tramite sito Web	Sì	Sì	Sì
Aggiornamenti software	Sì	Sì	Sì
Tecnico di supporto assegnato	—	Sì	Sì
Contatto di assistenza preventiva	—	Sì	Sì
Contatti cliente designati	—	5	10

Tabella A-1. Panoramica di PrimeSupport

Caratteristiche	Basic	Extended	Anytime
Tempo di risposta previsto	—	Cercapersone: 1 ora	Cercapersone: 30 minuti
		Casella vocale: 4 ore	Casella vocale: 1 ora
		Posta elettronica: 12 ore	Posta elettronica: 4 ore

Per ordinare PrimeSupport

Per ordinare PrimeSupport Basic, PrimeSupport Extended o PrimeSupport Anytime per i prodotti Network Associates:

- Contattare il rappresentante autorizzato, oppure
- Contattare i servizi di assistenza Network Associates al numero 1-800-988-5737 o al numero 1-650-473-2000 dalle 6.00 alle 17.00 (orario del Pacifico), dal lunedì al venerdì.

Il programma PrimeSupport descritto in questo manuale è disponibile solo in America del Nord. Per informazioni relative alle opzioni del programma PrimeSupport disponibili fuori dall'America del Nord contattare l'ufficio vendite della propria zona. Le informazioni relative ai contatti sono riportate sulla copertina del manuale.

Servizi di assistenza per privati

Tutti coloro che hanno acquistato prodotti Network Associates presso punti vendita al dettaglio o dal sito Web, hanno diritto ad alcuni servizi di assistenza compresi nell'acquisto del prodotto. Il livello di assistenza previsto dipende dal prodotto acquistato. Esempi dei servizi previsti sono:

- Aggiornamenti gratuiti ai file di dati (.DAT) per la durata del prodotto tramite il sito Web di Network Associates, la funzione di Aggiornamento automatico del prodotto o il servizio SecureCast. È possibile aggiornare i file di dati anche utilizzando il proprio browser Web per visitare il sito che si trova al seguente indirizzo:

  http://www.nai.com/download/updates/updates.asp

- Aggiornamenti gratuiti al programma (file eseguibile) per un anno tramite il sito Web di Network Associates, la funzione di Aggiornamento automatico del prodotto o il servizio SecureCast. Se è stata acquistata una versione "Deluxe" di un prodotto Network Associates, sono previsti aggiornamenti gratuiti del programma per due anni. È possibile aggiornare il software anche utilizzando il proprio browser Web per visitare il sito che si trova al seguente indirizzo:

  http://www.nai.com/download/upgrades/upgrades.asp

- Accesso gratuito 24 ore su 24, sette giorni su sette, all'assistenza in linea o elettronica tramite il sistema voce e fax di Network Associates, il sito Web di Network Associates e attraverso altri servizi elettronici quali America Online e CompuServe.

  Per contattare i servizi elettronici di Network Associates, selezionare una delle seguenti opzioni:

  – Sistema fax e voce automatico: (408) 988-3034

  – Sito web di Network Associates: **http://support.nai.com**

  – CompuServe GO NAI

  – America Online: parola chiave NAI

- 90 giorni di supporto tecnico gratuito da parte dei rappresentati del supporto disponibile nelle normali ore di ufficio, dalle 8.00 alle 20.00 (ora degli Stati Uniti centrali), dal lunedì al venerdì.

  Al termine del periodo di assistenza gratuita, è possibile usufruire di una gamma di opzioni di assistenza personalizzata specifiche per le singole esigenze. Contattare l'Assistenza clienti di Network Associates al numero (972) 278-6100 per ulteriori informazioni sulle opzioni disponibili, oppure visitare il sito web di Network Associates all'indirizzo:

  http://www.nai.com/services/support/support.asp

Consulenza e addestramento di Network Associates

Network Associates fornisce consulenza di esperti e addestramento completo per aumentare ai massimi livelli la protezione e le prestazioni della rete attraverso il programma Total Service Solutions.

Servizi di consulenza professionale

I servizi di consulenza professionale di Network Associates forniscono un'assistenza per tutte le fasi della crescita della rete, a partire dalla pianificazione e la progettazione, durante l'implementazione e per la gestione. I consulenti di Network Associates rappresentano una risorsa supplementare esperta con una linea di azione indipendente nella risoluzione dei problemi. Sarà possibile ottenere assistenza per l'integrazione dei prodotti Network Associates nel proprio ambiente, insieme all'assistenza per la risoluzione dei problemi o l'individuazione delle linee base per le prestazioni della rete. Inoltre, i consulenti di Network Associates sviluppano e forniscono ai clienti soluzioni per il raggiungimento degli scopi prefissati nei progetti, a partire dalla durata e dalle implementazioni su larga scala fino alla risoluzione rapida dei problemi.

Servizi di addestramento completo

I servizi di addestramento completo di Network Associates forniscono addestramento basilare e avanzato per i professionisti che operano sulle reti attraverso istruzioni pratiche che possono essere utilizzate immediatamente. Il programma dei servizi di addestramento completo verte sui malfunzionamenti della rete, sulla gestione delle prestazioni e sulla risoluzione dei problemi a tutti i livelli. Network Associates offre inoltre un addestramento modulare sui prodotti che consente di conoscere le caratteristiche e le funzionalità del proprio software.

È possibile iscriversi ai servizi di addestramento completo in qualsiasi periodo dell'anno presso i centri di addestramento di Network Associates oppure è possibile seguire dei corsi personalizzati a domicilio. Tutti i corsi garantiscono un apprendimento in varie fasi che consente di raggiungere i massimi livelli di conoscenza. Network Associates è un membro fondatore del consorzio CNX (Certified Network Expert).

Per ulteriori informazioni su questi programmi, contattare il rivenditore autorizzato oppure contattare Total Service Solutions al numero 1-800-395-3151.

Prevenzione delle infezioni B

Suggerimenti per un ambiente di sistema sicuro

VirusScan per Windows 3.1*x* è uno strumento efficace per la prevenzione, il rilevamento e il ripristino dalle infezioni da virus. È molto più efficace, tuttavia, se utilizzato in combinazione con un programma di sicurezza completo comprendente una serie di misure di sicurezza, ad esempio backup regolari, un sistema di protezione tramite password, corsi di preparazione e nozioni di approfondimento.

Per creare un ambiente di sistema sicuro e ridurre al minimo le probabilità di infezioni, Network Associates consiglia di procedere nel modo seguente:

- Seguire le procedure di installazione descritte nel Capitolo 2, "Installazione di VirusScan". Se si sospetta la presenza di un virus, pulire il sistema prima di installare VirusScan. Per questa procedura, consultare la sezione "Se si sospetta la presenza di un virus" a pagina 63.
- Configurare il file AUTOEXEC.BAT affinché VShield venga caricato automaticamente all'avvio.

NOTA: Il file AUTOEXEC.BAT viene automaticamente modificato se si seguono le procedure di installazione consigliate.

- Creare un disco di emergenza contenente la versione dalla riga di comando di VirusScan seguendo la procedura descritta in "Creazione di un disco di emergenza" a pagina 76. Accertarsi che il dischetto sia protetto da scrittura in modo che non possa infettarsi.
- Eseguire backup frequenti dei file importanti. Anche con VirusScan alcuni virus, così come gli incendi, il furto o gli atti vandalici, possono rendere un disco irrecuperabile se non è disponibile un backup recente.

Benché lo scopo di questo manuale sia di fornire un programma completo di protezione, le procedure illustrate in questa appendice consentono di comprendere con maggiore chiarezza che cosa sono i virus, come influenzano il sistema e cosa si può fare per evitare le infezioni.

Rilevamento di virus nuovi e sconosciuti

Ci sono due modi per affrontare il problema dei virus nuovi o sconosciuti che potrebbero infettare il sistema:

- Aggiornare i file di dati di VirusScan
- Aggiornare i file di programma di VirusScan.

VirusScan utilizza i file di dati (.DAT) per rilevare i virus. L'aggiornamento regolare di questi file consente di proteggere il sistema anche dai virus più nuovi. Network Associates aggiorna questi file ogni mese per fornire una protezione anche dai virus più recenti. Con minore frequenza, Network Associates modifica il programma stesso per aumentare la protezione e aggiungere funzioni. Quando questo avviene, è consigliabile aggiornare l'installazione all'ultima versione di VirusScan.

Aggiornamento dei file di dati di VirusScan

Per fornire la migliore protezione possibile contro i virus, Network Associates aggiorna costantemente i file che VirusScan utilizza per rilevare i virus. Dopo un certo periodo di tempo, VirusScan avverte l'utente di aggiornare il database di definizione dei virus. Per garantire sempre la massima protezione, Network Associates consiglia di aggiornare regolarmente questi file.

Definizione di file di dati

I file CLEAN.DAT, NAMES.DAT e SCAN.DAT forniscono informazioni sui virus al software di VirusScan. Questi sono i file di dati trattati nella presente sezione.

Perché richiedere un nuovo file di dati

Nuovi virus vengono scoperti ad una velocità di oltre 200 al mese. Spesso, questi virus non possono essere rilevati utilizzando i file di dati forniti con versioni precedenti. I file di dati forniti con la copia di VirusScan in uso potrebbero non rilevare un virus scoperto dopo che è stato acquistato il prodotto.

I ricercatori di virus di Network Associates lavorano costantemente per aggiornare i file di dati con nuove definizioni di virus.

NOTA: Network Associates fornisce aggiornamenti in linea di firme di virus per tutta la durata del prodotto. Tuttavia, non è possibile garantire la compatibilità dei file contenenti le firme dei virus con una versione precedente del software. Eseguendo l'aggiornamento alla versione più recente di VirusScan, è possibile ottenere il miglior livello di difesa dai virus.

Come applicare il file di dati

Per aggiornare il file di dati, procedere come segue:

1. Scaricare il file di dati (ad esempio, DAT-3004.ZIP) da uno dei servizi elettronici di Network Associates. Sulla maggior parte dei servizi, questo file è reperibile nell'area relativa agli antivirus.

   NOTA: L'accesso a questi aggiornamenti è legalmente limitato nei termini descritti nel file README.1ST associato al software e citato nel contratto di licenza del software.

2. Copiare il file in una nuova directory.
3. Il file è compresso. Decomprimere il file utilizzando un software di decompressione compatibile con PKUNZIP. Se non si dispone del software di decompressione, è possibile scaricare PKUNZIP (shareware) dai siti elettronici di Network Associates.
4. Individuare le directory sull'unità disco rigido dove è installato VirusScan (in genere, in **C:\Neta\Viruscan)**. Questa ubicazione varia a seconda della versione del software di cui si dispone e se durante l'installazione è stata specificata una diversa directory.
5. Copiare i nuovi file nella directory o nelle directory appropriate sovrascrivendo i file di dati precedenti.

   NOTA: Parte del software potrebbe trovarsi in più di una directory. In questo caso, collocare i file aggiornati in ciascuna directory.

6. È necessario riavviare il computer perché VirusScan riconosca e possa utilizzare i file aggiornati.

Convalida dei file di programma di VirusScan

Quando si scarica un file da una qualsiasi origine diversa dal bulletin board di Network Associates o da altri servizi di Network Associates, è necessario verificare che il file sia autentico e inalterato e che non sia infetto. Il software antivirus di Network Associates include un programma di utilità chiamato Validate, che può essere utilizzato per assicurarsi che la versione di VirusScan sia autentica. Quando si riceve una nuova versione di VirusScan, eseguire Validate su tutti i file di programma. Per informazioni più dettagliate sul programma Validate, consultare il file di testo README.1ST fornito con il software.

Creazione di un disco di emergenza

Per ripristinare un sistema in caso di infezione, è necessario disporre di un disco di emergenza. Questa sezione descrive come crearlo.

Per creare un disco di emergenza è necessario accertarsi che il sistema non sia infetto. I virus che risiedono nel sistema potrebbero essere trasferiti sul disco di emergenza e, di conseguenza, reinfettare il sistema.

Se si sospetta che il computer sia infetto, accedere ad un altro computer e sottoporlo a scansione. Se non si rileva alcun virus, attenersi alla procedura di seguito descritta relativa all'utilizzo dell'utility di creazione dei dischi di emergenza fornita con VirusScan.

NOTA: Se si sospetta che il computer sia infetto e non si ha a disposizione un altro computer con VirusScan installato, consultare "Creazione di un dischetto di boot pulito" a pagina 77, che illustra come creare manualmente un dischetto di boot pulito. Questo dischetto può essere utilizzato come sostitutivo del disco di emergenza fino a quando non viene installato VirusScan e creato un disco di emergenza.

---

1. Inserire un dischetto vuoto nell'unità A:.
2. Eseguire l'utility di creazione dei dischi di emergenza facendo doppio clic sulla relativa icona nel gruppo di programmi di VirusScan.
3. Seguire le istruzioni a video. Se si verifica un problema durante la creazione del disco di emergenza, assicurarsi che il disco inserito non sia protetto da scrittura.
4. Una volta terminata la creazione del disco di emergenza, rimuovere il dischetto dall'unità. Proteggere il dischetto da scrittura, etichettarlo e riporlo in un luogo sicuro. Per ulteriori informazioni, consultare "Protezione da scrittura di un dischetto" a pagina 79.

Creazione di un dischetto di boot pulito

Se si sta utilizzando un computer su cui non è installato VirusScan, è possibile creare un dischetto di boot pulito. Questo dischetto può essere utilizzato come sostitutivo del disco di emergenza fino a quando non viene installato VirusScan e creato un disco di emergenza.

Per creare un dischetto di boot pulito, avviare questa procedura dal prompt di DOS (è necessario passare al DOS o aprire una finestra DOS):

NOTA: Questa procedura deve essere eseguita su un sistema privo di virus.

---

1. Inserire un dischetto vuoto nell'unità A:.
2. Formattare il dischetto digitando il seguente comando al prompt **C:\>**:

   ```
   format a: /s /u
   ```

3. Tutte le informazioni presenti sul dischetto verranno sovrascritte.

   NOTA: Se si utilizza DOS 5.0 o una versione precedente, non digitare /u. Se non si è sicuri di quale versione si sta utilizzando, digitare **ver** al prompt **C:\>** per ottenere le informazioni relative alla versione.

   ---

4. Quando il sistema chiede di immettere l'etichetta di volume, immettere un nome appropriato utilizzando non più di undici caratteri.
5. Accedere alla directory predefinita di VirusScan digitando il seguente comando al prompt **C:\>**:

   ```
   cd \mcafee\viruscan
   ```

6. Copiare la versione DOS di VirusScan sul dischetto digitando i seguenti comandi al prompt **C:\mcafee\viruscan**:

   ```
   copy scan.exe a:
   copy scan.dat a:
   copy clean.dat a:
   copy names.dat a:
   ```

7. Tornare alla directory principale digitando il seguente comando al prompt **C:\mcafee\viruscan**:

   ```
   cd\
   ```

8. Copiare i programmi DOS utili sul dischetto digitando i seguenti comandi al prompt C:\:

   ```
   copy c:\dos\chkdsk.* a:
   ```

9. Ripetere l'ultima operazione per ogni altro programma utile che si desidera aggiungere al dischetto. Di seguito sono elencati alcuni di questi programmi:

   - debug.*
   - diskcopy.*
   - fdisk.*
   - format.*
   - label.*
   - mem.*
   - sys.*
   - unerase.*
   - xcopy.*

   NOTA: Se si utilizza un'utility di compressione dei dischi, assicurarsi di copiare i driver necessari per poter accedere ai dischetti compressi sul disco di emergenza. Per ulteriori informazioni su questi driver, consultare la documentazione relativa all'utility di compressione.

   ---

10. Etichettare e proteggere da scrittura il dischetto e riporlo in un luogo sicuro. Per ulteriori informazioni consultare "Protezione da scrittura di un dischetto" a pagina 79.

Protezione da scrittura di un dischetto

I dischetti sono dispositivi portatili e convenienti per la memorizzazione e il recupero dei dati del computer. Essi vengono utilizzati per salvare (scrittura) e ripristinare i file (lettura). Sono anche il veicolo di trasmissione dei virus più comune all'interno del computer.

Un modo per evitare la diffusione dell'infezione attraverso i dischetti è quello di *proteggere da scrittura* i dischetti affinché sia solo possibile leggere i dati. Se il sistema è stato infettato da un virus, la funzione di protezione da scrittura mantiene puliti i dischetti, evitando l'infezione del sistema dopo la pulizia.

NOTA: È opportuno sottoporre a scansione e pulire i dischetti non protetti da scrittura prima di proteggerli.

Protezione da scrittura dei dischetti da 3,5 pollici

1. Posizionare il dischetto con la parte metallica rivolta verso l'alto.

   Esaminare il foro rettangolare posizionato nell'angolo superiore sinistro. Dovrebbe essere visibile una linguetta in plastica quadrata che è possibile spostare verso l'alto e verso il basso.

2. Per proteggere da scrittura il dischetto, far scorrere verso l'alto la linguetta in plastica, ossia verso il bordo superiore del dischetto in modo da aprire il foro.

Installazioni condivise C

Procedura generale

1. Accedere con un account a livello amministratore alla workstation condivisa Windows 3.1*x*.
2. Eseguire la procedura di installazione riportata a pagina 5. Se necessario, cambiare la directory per l'installazione condivisa.
3. Una volta terminata l'installazione, riavviare il computer e riaccedere con il medesimo account a livello amministratore.
4. Apportare le modifiche descritte nella sezione riportata di seguito.

Modifiche ai file

File Win.ini

Aggiungere nella sezione [VirusScan] del file WIN.INI la stringa seguente:

```
naiinipath=x:\test\folder
```

Questa stringa rende possibile un posizionamento alternato del file AVCONSOL.INI.

File Autoexec.bat

Se si desidera posizionare i DAT in una cartella a parte, è necessario aggiungere una stringa simile alla seguente nel file AUTOEXEC.BAT.

```
set mcafee.scan=x:\test\DATS
```

Questa stringa consente a SCAN.EXE o SCANPM.EXE di continuare a funzionare come previsto.

File Avconsol.ini

Nuove stringhe

Nella sezione [VirusScan Console] del file AVCONSOL.INI vi sono due nuove stringhe.

- `RefreshRate=3` indica l'impostazione predefinita, in secondi, della frequenza con cui AVCONSOL.EXE verifica la presenza di modifiche nei file .INI. È necessario impostare un valore compreso tra 1 e 10 secondi.

  NOTA: L'accesso alla rete viene ridotto in maniera significativa se si imposta un valore più alto.

- `NewTaskPath=x:\new=vscfile` indica la posizione predefinita in cui viene memorizzata la nuova attività creata in AVCONSOL.EXE.

File di configurazione di VShield

È possibile cambiare la posizione del file di configurazione di VShield modificando [Item-0] in AVCONSOL.INI. In [Item-0], dovrebbe essere presente una stringa SzVshFile.

Aggiungere una stringa simile alla seguente:

```
SzVshFile=x:\test\directory
```

In tal modo si ha la possibilità di ricercare la directory in cui si desidera archiviare il file di configurazione di VShield.

NOTA: Se la stringa SzVshFile non è presente, aggiungerla ad [Item-0].

File di configurazione di Scan16

Se si desidera posizionare i file di configurazione dell'attività Scan16 in una directory separata, modificare la stringa SzVscFile sotto ciascun elemento di AVCONSOL.INI che indichi un'attività Scan16.

Limitazioni

Particolari tipi di installazioni condivise impongono delle limitazioni sugli aggiornamenti di stato e sugli accessi.

Aggiornamenti di stato

Se ad AVCONSOL.EXE si accede tramite un account a livello utente che ha accesso in sola lettura alla directory in cui sono archiviati i file di configurazione, lo stato non verrà aggiornato da alcuna funzionalità che l'account tenterà di utilizzare. Anche se l'account utente esegue un'attività pianificata, non vi sarà alcuna traccia dell'esecuzione dell'attività.

NOTA: Questa limitazione non si applica agli account a livello amministratore.

Accesso

Se i file eseguibili vengono installati in una directory in cui gli account utente hanno accesso in sola lettura, le directory di accesso dovranno consentire accesso in lettura e scrittura in modo che sia possibile un accesso corretto.

Se i risultati di sistema per tutti gli utenti vengono registrati nello stesso file di registro, il file di registro dovrà essere impostato alle dimensioni massime.

Riferimento D

Opzioni della riga di comando di VirusScan

La tabella riportata di seguito elenca tutte le opzioni di VirusScan che è possibile utilizzare quando si esegue quando si utilizza lo scanner della riga di comando DOS, SCAN.EXE. Per eseguire VirusScan per Windows 3.1*x* dalla riga di comando, utilizzare il comando `cd` per passare alla directory nella quale è stato installato VirusScan. Quindi digitare `scan /?` per visualizzare un elenco di opzioni con le relative descrizioni sulle modalità di utilizzo.

NOTA: Quando si specifica un nome di file come parte di un'opzione della riga di comando, è necessario includere il percorso completo per il file se non si trova nella directory di installazione di VirusScan.

Opzione della riga di comando	Descrizione
/? o /HELP	Non esegue la scansione, ma visualizza un elenco delle opzioni della riga di comando di VirusScan con una breve descrizione. Utilizzare una di queste opzioni sulla riga di comando senza altre opzioni.
/ADL	Esegue la scansione di tutte le unità locali (incluse le unità compresse, CD-ROM e PCMCIA, ma non i dischetti), oltre a quelle specificate sulla riga di comando. Per sottoporre a scansione sia le unità locali che quelle di rete, utilizzare /ADL e /ADN insieme sulla stessa riga di comando.
/ADN	Esegue la scansione dei virus di tutte le unità di rete, oltre a quelle specificate sulla riga di comando. Per sottoporre a scansione sia le unità locali che quelle di rete, utilizzare /ADL e /ADN insieme sulla stessa riga di comando.

Opzione della riga di comando	Descrizione
/AF nomefile	Memorizza i codici di convalida e ripristino in*nomefile.* Facilita il rilevamento di virus nuovi o sconosciuti. /AF registra i dati di convalida e di ripristino per i file eseguibili, il settore di boot e il record di boot principale nel file specificato su disco rigido o su dischetto. Il file di registro è convalidato per circa 89 byte per file. È necessario specificare un *nomefile*, che può contenere il percorso completo. Se il percorso di destinazione è un'unità di rete, è necessario disporre dei diritti necessari per creare ed eliminare i file su tale unità. Se *nomefile* esiste, VirusScan lo aggiorna. /AF impiega approssimativamente il 300% di tempo in più per eseguire la scansione. **NOTA:** /AF ha la stessa funzione di /AV, ma memorizza i dati in un file separato invece di modificare i file eseguibili stessi. L'opzione /AF non memorizza le informazioni relative al record di boot principale o al settore di boot dell'unità sottoposta a scansione.
/ALERTPATH <directory>	Designa <directory> come percorso di rete controllato da NetShield per l'avviso centralizzato.
/ALL	Ignora le impostazioni predefinite ed esegue la scansione di tutti i file. Questa opzione aumenta in modo considerevole il tempo richiesto per la scansione. È opportuno utilizzarla nel caso sia stato rilevato un virus o se ne sospetti la presenza. **NOTA:** L'elenco di estensioni per gli eseguibili standard è stato modificato rispetto alle versioni precedenti di VirusScan.
/APPEND	Se utilizzata con /REPORT, accoda il testo del messaggio di rapporto al file di rapporto specificato, se esistente. Altrimenti, l'opzione /REPORT sovrascrive il file di rapporto specificato, se esistente.
/AV	Per facilitare il rilevamento di virus nuovi e sconosciuti e il relativo ripristino, /AV aggiunge i dati di convalida a e di ripristino a ciascun file eseguibile standard (.EXE, .COM, .SYS, .BIN, .OVL e .DLL), aumentando di 98 byte le dimensioni di ogni file. Per aggiornare i file su un'unità di rete condivisa, è necessario disporre dei diritti di accesso di aggiornamento. Per escludere i file con automodifica o con autoverifica e i file danneggiati che potrebbero causare falsi allarmi, utilizzare l'opzione /EXCLUDE. Se si utilizza una qualsiasi combinazione delle opzioni /AV, /CV o /RV sulla stessa riga di comando, si verifica un errore. **NOTA:** L'opzione /AV non memorizza le informazioni relative al record di boot principale o al settore di boot dell'unità sottoposta a scansione.
/BOOT	Esegue solo la scansione del settore di boot e del record di boot principale sull'unità specificata.

Opzione della riga di comando	Descrizione
`/CF nomefile`	Facilita il rilevamento di virus nuovi o sconosciuti. Controlla i dati di convalida memorizzati dall'opzione /AF in *nomefile*. Se si modifica un file o un'area di sistema, VirusScan informa che può essersi verificata un'infezione da virus. L'opzione /CF impiega approssimativamente il 250% di tempo in più per eseguire la scansione. Se si utilizza una qualsiasi combinazione delle opzioni /AF, /CF o /RF sulla stessa riga di comando, si verifica un errore. **NOTA:** Alcuni PC Hewlett-Packard e Zenith della precedente generazione modificano il settore di boot ad ogni avvio del sistema. Se si utilizza /CF, VirusScan informa che il settore di boot è stato modificato anche se non è presente alcun virus. Consultare il manuale di riferimento del computer per verificare se il PC dispone di un codice di boot con automodifica.
`/CLEAN`	Pulisce i file infetti.
`/CLEANDOC`	Elimina i virus dai file di documento di Word infetti.
`/CLEANDOCALL`	Pulisce tutte le macro dai file di documento di Word infetti.
`/CONTACTFILE nomefile`	Identifica un file contenente una stringa di messaggio da visualizzare quando viene rilevato un virus. Questa opzione è particolarmente utile negli ambienti di rete, poiché consente di conservare il messaggio in un file centrale invece che su ogni workstation. Sono validi tutti i caratteri, ad eccezione della barra rovesciata (\). I messaggi che iniziano con una barra (/) o con un trattino (-) devono essere inseriti tra virgolette.
`/CV`	Facilita il rilevamento di virus nuovi o sconosciuti. Controlla i dati di convalida aggiunti dall'opzione /AV. Se è stato modificato un file, VirusScan informa che può essersi verificata un'infezione da virus. L'opzione /CV impiega approssimativamente il 50% di tempo in più per eseguire la scansione. Se si utilizza una qualsiasi combinazione delle opzioni /AV, /CV o /RV sulla stessa riga di comando, si verifica un errore. **NOTA:** L'opzione /CV non controlla il settore di boot per individuare eventuali modifiche.
`/DEL`	Elimina i file infetti.
`/EXCLUDE nomefile`	Esclude dalla scansione i file elencati in *nomefile*. Questa opzione consente di escludere i file dalla convalida /AF e /AV e dalla verifica /CF e /CV. I file con automodifica o con autoverifica possono causare falsi allarmi durante la scansione.

Opzione della riga di comando	Descrizione
/FAST	Velocizza la scansione. Riduce il tempo di scansione di circa il 15%. Tramite l'utilizzo dell'opzione /FAST, VirusScan esamina una piccola parte di ogni file per rilevare i virus. L'utilizzo di /FAST potrebbe non consentire di trovare alcune infezioni rilevabili tramite una scansione più completa e, di conseguenza, più lenta. Non utilizzare questa opzione nel caso sia stato trovato un virus o se ne sospetti la presenza.
/FORCE	Elimina i virus della tabella di partizione tramite la scrittura di un record di boot principale generico sul record di boot del disco.
/FREQUENCY ore	Il numero di ore che si desidera intercorra tra scansioni successive (ad esempio: /FREQUENCY 1). Negli ambienti con rischio di infezioni da virus molto basso, è opportuno utilizzare questa opzione per evitare scansioni non necessarie o troppo frequenti. Diminuendo il numero di *ore* specificato si aumenta la frequenza di scansione e la protezione dalle infezioni.
/LOAD nomefile	Esegue una scansione utilizzando le informazioni salvate in *nomefile*. È possibile memorizzare tutte le impostazioni personalizzate in un file di configurazione a parte (un file di testo ASCII), quindi utilizzare /LOAD per caricare le impostazioni dal file.
/LOCK	Blocca il sistema per impedire ulteriori infezioni se VirusScan trova un virus. /LOCK è utile negli ambienti di rete altamente vulnerabili, ad esempio i laboratori informatici aperti a tutti. È consigliabile utilizzare /LOCK con /CONTACTFILE per comunicare agli utenti le azioni da eseguire e le persone da contattare nel caso venga rilevato un virus e si blocchi il sistema.
/LOG	Memorizza la data e l'ora in cui viene eseguito VirusScan aggiornando o creando un file denominato SCAN.LOG nella directory principale dell'unità corrente.

Opzione della riga di comando	Descrizione
/MANY	Esegue la scansione consecutiva di più dischetti su una singola unità. VirusScan chiede la conferma per ogni dischetto. Dopo aver creato un sistema privo di virus, utilizzare questa opzione per sottoporre rapidamente a scansione più dischetti. È necessario che il programma VirusScan si trovi su un disco che non verrà rimosso durante la scansione. Ad esempio, se si esegue la scansione dei dischi inseriti nell'unità A: del computer e il programma viene eseguito da un disco presente nell'unità A: esso cesserà di essere disponibile non appena si rimuoverà il disco per inserirne un altro. Il comando seguente causerà un errore durante l'esecuzione: a:\scan a: /many
/MAXFILESIZE xxx.x	Sottopone a scansione soltanto i file con dimensioni non superiori a xxx.x megabyte.
/MEMEXCL	Esclude l'area di memoria dalla scansione. L'impostazione predefinita è A000-FFFF, 0000=Scan all. Questa opzione della riga di comando è stata aggiunta per evitare che VirusScan controlli le aree della memoria superiore che potrebbero contenere hardware con memoria mappata e causare falsi allarmi.
/MOVE directory	Sposta tutti i file infetti trovati durante la scansione nella directory specificata. Per conservare la struttura di unità e directory, questa opzione non ha effetto se il record di boot principale o il settore di boot sono infetti, dato che non si tratta di file.
/NOBEEP	Disattiva il segnale acustico che viene emesso ogni volta che VirusScan trova un virus.
/NOBREAK	Disattiva CTRL-C e CTRL-INTERR durante le scansioni. Gli utenti non potranno interrompere le scansioni in corso tramite CTRL-C o CTRL-INTERR. Utilizzare questa opzione con /LOG per creare un utile controllo a ritroso delle scansioni programmate regolarmente.
/NOCOMP	Non controlla i file eseguibili compressi creati con i programmi di compressione dei file LZEXE o PKLITE. Riduce i tempi di scansione quando è necessaria una scansione completa. Altrimenti, in base all'impostazione predefinita, VirusScan controlla i file eseguibili o ad autodecompressione creati con i programmi di compressione dei file LZEXE o PKLITE. VirusScan decomprime ogni file in memoria e controlla le firme dei virus, impiegando tempi più lunghi ma garantendo una scansione più completa. Se si utilizza /NOCOMP, VirusScan non controlla i file compressi per rilevare i virus, sebbene controlli le modifiche apportate a tali file se sono convalidate tramite i codici di convalida e ripristino.

Opzione della riga di comando	Descrizione
/NODDA	Non si ha l'accesso diretto al disco. Impedisce l'accesso di VirusScan al record di boot. Questa funzione è stata aggiunta per consentire l'esecuzione di VirusScan in Windows NT. Può essere necessario utilizzare questa opzione su alcune unità dipendenti da periferiche.
/NODOC	Non esegue la scansione dei file di documento di Word.
/NOEMS	Impedisce a VirusScan l'utilizzo della memoria espansa (LIM EMS 3.2), garantendo la disponibilità di EMS per altri programmi.
/NOEXPIRE	Disattiva il messaggio relativo alla "data di scadenza" se i file di dati di VirusScan non sono aggiornati.
/NOMEM	Riduce i tempi di scansione evitando di controllare la memoria per rilevare i virus. Utilizzare /NOMEM soltanto quando si è assolutamente certi dell'assenza di virus nel computer. VirusScan è in grado di controllare la memoria di sistema per rilevare tutti i virus informatici critici e conosciuti che possono risiedere nella memoria. Oltre alla memoria principale da 0KB a 640KB, VirusScan controlla la memoria di sistema da 640KB a 1088KB che può essere utilizzata dai virus informatici sui sistemi 286 e successivi. La memoria superiore a 1088KB non viene utilizzata direttamente dal processore e attualmente non è soggetta ai virus.
/PAUSE	Attiva la pausa dello schermo. Se si utilizza l'opzione /PAUSE, viene visualizzato il messaggio di richiesta "Premere un tasto per continuare" quando VirusScan riempie lo schermo di messaggi (ad esempio, quando si utilizzano le opzioni /SHOWLOG o /VIRLIST). Altrimenti, in base all'impostazione predefinita, VirusScan riempie e fa scorrere lo schermo in modo continuo e senza interruzioni, consentendo così l'esecuzione su PC con varie unità o con gravi infezioni senza richiedere interventi da parte dell'utente. È consigliabile non utilizzare /PAUSE quando si registrano i messaggi di VirusScan tramite le opzioni di rapporto (/REPORT, /RPTCOR, /RPTMOD, e /RPTERR).
/PLAD	Conserva le date dell'ultimo accesso (solo sulle unità di proprietà esclusiva). Impedisce la modifica dell'attributo della data dell'ultimo accesso sui file memorizzati su un'unità di rete in un ambiente di rete di proprietà esclusiva. In genere, le unità di rete di proprietà esclusiva aggiornano la data dell'ultimo accesso quando VirusScan apre ed esamina un file. Tuttavia, alcuni sistemi di backup a nastro utilizzano questa data per decidere se è necessario eseguire il backup del file. Utilizzare /PLAD per evitare che la data dell'ultimo accesso venga modificata dalla scansione.

Opzione della riga di comando	Descrizione
/REPORT nomefile	Crea un rapporto relativo ai file infetti e agli errori di sistema. Salva l'output di VirusScan in *nomefile* un file di testo in formato ASCII. Se *nomefile* esiste, /REPORT lo cancella e lo sostituisce oppure, se si utilizza /APPEND, aggiunge le informazioni di rapporto al fondo del file esistente. È possibile includere l'unità e la directory di destinazione (ad esempio D:\VSREPRT\ALL.TXT), tuttavia, se la destinazione è un'unità di rete, è necessario disporre dei diritti di creazione ed eliminazione dei file su tale unità. È anche possibile utilizzare /RPTALL, /RPTCOR, /RPTMOD e /RPTERR per aggiungere al rapporto i file sottoposti a scansione, corrotti, modificati e gli errori di sistema.
/RF nomefile	Rimuove i dati di ripristino e convalida da *nomefile*, il file creato tramite l'opzione /AF. Se *nomefile* risiede su un'unità di rete condivisa, è necessario disporre dei diritti necessari per l'eliminazione dei file su tale unità. Se si utilizza una qualsiasi combinazione delle opzioni /AF, /CF o /RF sulla stessa riga di comando, si verifica un errore.
/RPTALL	Aggiunge al file di rapporto un elenco dei file sottoposti a scansione. Questa opzione viene utilizzata con /REPORT.
/RPTCOR	Quando viene utilizzata con /REPORT, questa opzione aggiunge al file di rapporto i nomi dei file corrotti. Un file corrotto potrebbe essere un file danneggiato da un virus. È possibile utilizzare /RPTCOR con /RPTMOD e /RPTERR sulla stessa riga di comando. **NOTA:** Alcuni file che richiedono un file sovrapposto o eseguibile per funzionare correttamente (Ossia, quei file che non sono eseguibili da soli) potrebbero causare letture errate.
/RPTERR	Aggiunge al file di rapporto un elenco degli errori di sistema. Questa opzione viene utilizzata con /REPORT. Gli errori di sistema comprendono i problemi di lettura o scrittura su dischetti o unità disco rigido, i problemi del file system o di rete, i problemi nella creazione di rapporti e altri problemi relativi al sistema. È possibile utilizzare /RPTERR con /RPTCOR e /RPTMOD sulla stessa riga di comando.
/RPTMOD	Aggiunge al file di rapporto un elenco dei file modificati. Questa opzione viene utilizzata con /REPORT. VirusScan rileva i file modificati quando i codici di convalida e ripristino non corrispondono (tramite le opzioni /CF o /CV). È possibile utilizzare /RPTMOD con /RPTCOR e /RPTERR sulla stessa riga di comando.

Opzione della riga di comando	Descrizione
/RV	Rimuove i dati di convalida e ripristino dai file convalidati con l'opzione /AV. Per aggiornare i file su un'unità di rete condivisa, è necessario disporre dei diritti di accesso per l'aggiornamento. Se si utilizza una qualsiasi combinazione delle opzioni /AV, /CV o /RV sulla stessa riga di comando, si verifica un errore.
/SHOWLOG	Visualizza il contenuto di SCAN.LOG. SCAN.LOG memorizza la data e l'ora di esecuzione di VirusScan tramite l'aggiornamento o la creazione di un file denominato SCAN.LOG nella directory corrente e la data e l'ora delle scansioni precedenti registrate nel file SCAN.LOG tramite l'opzione /LOG. Il file SCAN.LOG contiene testo e alcune formattazioni speciali. Per interrompere lo scorrimento quando lo schermo si riempie di messaggi, utilizzare l'opzione /PAUSE.
/SUB	Esegue la scansione delle sottodirectory all'interno di una directory. In base all'impostazione predefinita, quando si sottopone a scansione una directory invece di un'unità, VirusScan ne esamina soltanto i file, non le sottodirectory. Utilizzare /SUB per sottoporre a scansione tutte le sottodirectory all'interno della directory specificata. Non utilizzare /SUB se si esegue la scansione di un'intera unità.
/VIRLIST	Visualizza il nome e una breve descrizione di ogni virus rilevato da VirusScan. Per interrompere lo scorrimento quando lo schermo si riempie di messaggi, utilizzare l'opzione /PAUSE. Utilizzare /VIRLIST da sola o con /PAUSE sulla riga di comando. È possibile salvare in un file l'elenco dei nomi e delle descrizioni dei virus reindirizzando l'output del comando. Ad esempio, immettere in DOS: scan /virlist > nomefile.txt **NOTA:** Dato che VirusScan è in grado di rilevare molti virus, questo file contiene più di 250 pagine.

Livelli di errore DOS di VirusScan

Quando si esegue VirusScan in ambiente DOS, viene impostato un livello di errore DOS. È possibile utilizzare ERRORLEVEL nei file batch per eseguire azioni diverse a seconda dei risultati della scansione.

NOTA: Per ulteriori informazioni, consultare la documentazione del sistema operativo DOS in uso.

VirusScan può restituire i seguenti livelli di errore:

ERRORLEVEL	Descrizione
0	Non si è verificato alcun errore; non è stato trovato alcun virus.
1	Si è verificato un errore durante l'accesso a un file (lettura o scrittura).
2	Un file di dati di VirusScan è corrotto.
3	Si è verificato un errore durante l'accesso a un disco (lettura o scrittura).
4	Si è verificato un errore durante l'accesso al file creato con l'opzione /AF; il file è stato danneggiato.
5	La memoria è insufficiente per caricare il programma o completare l'operazione.
6	Si è verificato un errore di programma interno (errore di memoria esaurita).
7	Si è verificato un errore durante l'accesso a un file di messaggi internazionale (MCAFEE.MSG).
8	Un file richiesto per eseguire VirusScan, ad esempio SCAN.DAT, è mancante.
9	Le opzioni o gli argomenti delle opzioni specificati sulla riga di comando sono incompatibili o sconosciuti.
10	È stato trovato un virus nella memoria.
11	Si è verificato un errore di programma interno.
12	Si è verificato un errore durante il tentativo di rimuovere un virus, ad esempio non è stato trovato il file CLEAN.DAT, oppure VirusScan non è stato in grado di rimuovere il virus.
13	Uno o più virus sono stati trovati nel record di boot principale, nel settore di boot o nei file.
14	Il file SCAN.DAT non è aggiornato; aggiornare i file di dati di VirusScan.
15	L'autoverifica di VirusScan è fallita; potrebbe essere infetta o danneggiata.

ERRORLEVEL	Descrizione
16	Si è verificato un errore durante l'accesso all'unità o al file specificato.
17	Non è stata specificata alcuna unità, directory o file; nessun elemento da sottoporre a scansione.
18	È stato modificato un file convalidato (opzioni /CF o /CV).
19-99	Riservati.
100+	Errore del sistema operativo; VirusScan aggiunge 100 al numero originale.
102	Sono stati utilizzati i tasti CTRL+C o CTRL+INTERR per interrompere la scansione. È possibile disattivare CTRL+C o CTRL+INTERR con l'opzione della riga di comando /NOBREAK.

Formato di file VSH

Il file VSH è un file di testo di configurazione, con formato simile al file INI di Windows e che contiene le impostazioni di VShield. Ogni variabile nel file dispone di un nome seguito dal segno uguale (=) e di un valore. I valori definiscono le impostazioni selezionate per la configurazione di VShield. Le variabili sono suddivise in sette gruppi: General, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, SecurityOptions ed ExclusionOptions. Per modificare il file VSH, aprirlo con un editor di testi, ad esempio Blocco note.

NOTA: Nelle variabili booleane, i valori possibili sono 0 e 1. Il valore 0 abilita VirusScan a disattivare l'impostazione, mentre il valore 1 indica che l'impostazione è attivata.

General

Variabile	Descrizione
bLoadAtStartup	Tipo: Booleana (1/0) Definisce se VShield deve essere caricato all'avvio del sistema avvio Valore predefinito: 1
bCanBeDisabled	Tipo: Booleana (1/0) Definisce se VShield può essere disattivato Valore predefinito: 1

Variabile	Descrizione
bShowTaskbarIcon	Tipo: Booleana (1/0) Definisce se l'icona della barra delle applicazioni di VShield viene visualizzata Valore predefinito: 1
bNoSplash	Tipo: Booleana (1/0) Abilita VShield a non visualizzare lo schermo introduttivo all'avvio del programma Valore predefinito: 0

DetectionOptions

Variabile	Descrizione
szProgramExtensions	Tipo: Stringa Definisce le estensioni da sottoporre a scansione Valore predefinito: EXE COM DO? XL?
szDefaultProgramExtensions -	Tipo: Stringa Definisce le estensioni da utilizzare come estensioni di programma predefinite durante la configurazione di scansione Valore predefinito: EXE COM DO? XL?
bScanOnExecute	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione quando i file vengono eseguiti Valore predefinito: 1
bScanOnOpen	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione quando i file vengono aperti Valore predefinito: 1
bScanOnCreate	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione quando i file vengono creati Valore predefinito: 1
bScanOnRename	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione quando i file vengono rinominati Valore predefinito: 1
bScanOnBootAccess	Tipo: Booleana (1/0) Abilita VShield ad eseguire la scansione del record di boot di un'unità disco la prima volta cui vi si accede Valore predefinito: 1

Variabile	Descrizione
bScanAllFiles	Tipo: Booleana (1/0) Abilita il programma ad eseguire la scansione di tutti i file Valore predefinito: 0
bScanCompressed	Tipo: Booleana (1/0) Abilita il programma ad eseguire la scansione dei file compressi (PkLite, LZEXE) Valore predefinito: 1

AlertOptions

Variabile	Descrizione
bNetworkAlert	Tipo: Booleana (1/0) Abilita VShield ad inviare un avviso di rete ad una cartella controllata da NetShield per l'avviso centralizzato. Valore predefinito: 0
szNetworkAlertPath	Tipo: Stringa Specifica il percorso controllato da NetShield per l'avviso centralizzato. Valore predefinito: Nessuno

ActionOptions

Variabile	Descrizione
szCustomMessage	Tipo: Stringa Definisce il messaggio personalizzato da visualizzare al rilevamento di un virus se l'azione è impostata su Richiedi azione Valore predefinito: Rilevato possibile virus
szMoveToFolder	Tipo: Stringa Definisce la cartella in cui spostare i file infetti Valore predefinito: \Infetti

Variabile	Descrizione
uVshieldAction	Tipo: Numero intero (1-5) Abilita VShield ad eseguire l'azione specificata quando viene rilevato un virus Valori possibili: 1 - Richiedi azione 2 - Sposta file infetti nella cartella 3 - Pulisci file infetti automaticamente (L'accesso è impedito se i file non possono essere puliti) 4 - Elimina file infetti automaticamente 5 - Impedisci l'accesso ai file infetti Valore predefinito: 1
bButtonClean	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di pulire il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonDelete	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di eliminare il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonExclude	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di escludere il file se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bButtonStop	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di impedire l'accesso al file infetto se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1

Variabile	Descrizione
bButtonContinue	Tipo: Booleana (1/0) Abilita VShield a fornire all'utente l'opzione di continuare l'evento intercettato se Richiedi azione è selezionata e viene rilevato un virus Valore predefinito: 1
bDisplayMessage	Tipo: Booleana (1/0) Definisce se visualizzare il messaggio personalizzato nella finestra di dialogo Richiedi azione al rilevamento di un virus Valore predefinito: 0

ReportOptions

Variabile	Descrizione
szLogFileName	Tipo: Stringa Definisce il nome del file di registro Valore predefinito: C:\McAfee\Viruscan\Vshlog.txt
bLogToFile	Tipo: Booleana (1/0) Definisce se i risultati della scansione devono essere registrati nel file di registro Valore predefinito: 1
bLimitSize	Tipo: Booleana (1/0) Definisce se le dimensioni del file devono essere limitate Valore predefinito: 1
uMaxKilobytes	Tipo: Numero intero (10-999) Definisce le dimensioni massime in kilobyte del file di registro Valore predefinito: 100
bLogDetection	Tipo: Booleana (1/0) Definisce se i risultati della scansione devono essere registrati Valore predefinito: 1
bLogClean	Tipo: Booleana (1/0) Definisce se i risultati della pulizia devono essere registrati Valore predefinito: 1
bLogDelete	Tipo: Booleana (1/0) Definisce se le operazioni di eliminazione dei file infetti devono essere registrate Valore predefinito: 1

Variabile	Descrizione
bLogMove	Tipo: Booleana (1/0) Definisce se le operazioni di spostamento dei file infetti devono essere registrate Valore predefinito: 1
bLogSettings	Tipo: Booleana (1/0) Definisce se le impostazioni della sessione devono essere registrate alla chiusura Valore predefinito: 1
bLogSummary	Tipo: Booleana (1/0) Definisce se il riepilogo della sessione deve essere registrato alla chiusura Valore predefinito: 1
bLogDateTime	Tipo: Booleana (1/0) Definisce se la data e l'ora di un evento devono essere registrate Valore predefinito: 1
bLogUserName	Tipo: Booleana (1/0) Definisce se il nome utente deve essere registrato Valore predefinito: 1

SecurityOptions

Variabile	Descrizione
szPasswordProtect	Tipo: Stringa Questa opzione non è configurabile dall'utente. Valore predefinito: 0
szPasswordCRC	Tipo: Stringa Questa opzione non è configurabile dall'utente. Valore predefinito: 0

ExclusionOptions

Variabile	Descrizione
szExclusionsFileName	Tipo: Stringa Questa opzione non è configurabile dall'utente.
NumExcludedItems	Tipo: Numero intero (0-n) Definisce il numero di elementi esclusi dalla scansione all'accesso Valore predefinito: 0
ExcludedItem_x, dove x è un indice a base zero	Tipo: Stringa Abilita VShield ad escludere l'elemento dalla scansione all'accesso Valore predefinito: \Recycled|*.*|1|1 * * La stringa è suddivisa in campi tramite il carattere pipe (|): Campo 1: cartella dell'elemento da escludere. Lasciare vuoto nel caso di file singoli nel sistema. Campo 2: file dell'elemento da escludere. Lasciare vuoto se si esclude una cartella senza specificare il nome del file. Campo 3: numero intero (1-3) Valori possibili: 1 - Esclude dalla scansione di accesso ai file 2 - Esclude dalla scansione del record di boot 3 - Esclude sia dalla scansione del record di boot che dalla scansione di accesso ai file Campo 4: booleano (1/0) Valori possibili: 1 - Abilita VShield ad escludere le sottocartelle dell'elemento escluso 2 - Abilita VShield a non escludere le sottocartelle

Formato di file VSC

Il file VSC è un file di testo di configurazione, con formato simile al file INI di Windows e che contiene le impostazioni di VirusScan. Ogni variabile nel file dispone di un nome seguito dal segno uguale (=) e di un valore. I valori definiscono le impostazioni selezionate per la configurazione di VirusScan. Le variabili sono suddivise in otto gruppi: ScanOptions, DetectionOptions, AlertOptions, ActionOptions, ReportOptions, ScanItems, SecurityOptions ed ExcludedItems. Per modificare il file VSC, aprirlo con un editor di testi, ad esempio Blocco note.

NOTA: Nelle variabili booleane, i valori possibili sono 0 e 1. Il valore 0 abilita VirusScan a disattivare l'impostazione, mentre il valore 1 indica che l'impostazione è attivata.

ScanOptions

Variabile	Descrizione
bAutoStart	Tipo: Booleana (0/1) Abilita VirusScan ad avviare automaticamente la scansione all'avvio Valore predefinito: 0
bAutoExit	Tipo: Booleana (0/1) Abilita VirusScan a chiudersi automaticamente al termine della scansione Valore predefinito: 0
bAlwaysExit	Tipo: Booleana (0/1) NECESSARIA DESCRIZIONE Valore predefinito: 0
bSkipMemoryScan	Tipo: Booleana (0/1) Abilita VirusScan a non eseguire la scansione della memoria Valore predefinito: 0
bSkipBootScan	Tipo: Booleana (0/1) Abilita VirusScan a non eseguire la scansione dei settori di boot Valore predefinito: 0
bSkipSplash	Tipo: Booleana (0/1) Abilita VirusScan a non visualizzare lo schermo introduttivo all'avvio Valore predefinito: 0

DetectionOptions

Variabile	Descrizione
bScanAllFiles	Tipo: Booleana (0/1) Abilita VirusScan ad eseguire la scansione di tutti i tipi di file Valore predefinito: 0
bScanCompressed	Tipo: Booleana (0/1) Abilita VirusScan ad eseguire la scansione dei file compressi Valore predefinito: 1
szProgramExtensions	Tipo: Stringa Specifica quali estensioni di file verranno sottoposte a scansione da VirusScan Valore predefinito: EXE COM DO? XL?
szDefaultProgramExtensions	Tipo: Stringa Specifica il valore predefinito di szProgramExtensions Valore predefinito: EXE COM DO? XL?

AlertOptions

Variabile	Descrizione
bNetworkAlert	Tipo: Booleana (0/1) Abilita VirusScan ad inviare un file di avviso (.ALR) ad un percorso di rete controllato da NetShield per l'avviso centralizzato quando viene rilevato un virus Valore predefinito: 0
bSoundAlert	Tipo: Booleana (0/1) Abilita VirusScan ad emettere un segnale acustico di avviso quando viene rilevato un virus Valore predefinito: 1
szNetworkAlertPath	Tipo: Stringa Specifica il percorso di avviso di rete controllato da NetShield per l'avviso centralizzato. La cartella alla quale è indirizzato il percorso deve contenere il file di avviso centralizzato, CENTALRT.TXT Valore predefinito: Nessuno

ActionOptions

Variabile	Descrizione
bDisplayMessage	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare un messaggio quando rileva un virus Valore predefinito: 0
ScanAction	Tipo: Numero intero (0-5) Abilita VirusScan ad eseguire l'azione specificata quando viene rilevato un virus Valori possibili: 0 - Richiedi azione 1 - Sposta automaticamente 2 - Pulisci automaticamente 3 - Elimina automaticamente 4 - Continua Valore predefinito: 0
bButtonClean	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Pulisci se ScanAction=0 Valore predefinito: 1
bButtonDelete	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Elimina se ScanAction=0 Valore predefinito: 1
bButtonExclude	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Escludi se ScanAction=0 Valore predefinito: 1
bButtonMove	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Sposta se ScanAction=0 Valore predefinito: 1
bButtonContinue	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Continua se ScanAction=0 Valore predefinito: 1
bButtonStop	Tipo: Booleana (0/1) Abilita VirusScan a visualizzare il pulsante Interrompi se ScanAction=0 Valore predefinito: 1

Variabile	Descrizione
szMoveToFolder	Tipo: Stringa Indica dove devono essere spostati i file infetti Valore predefinito: \Infetti
szCustomMessage	Tipo: Stringa Indica il messaggio di testo da visualizzare al rilevamento di virus Valore predefinito: Rilevato possibile virus

ReportOptions

Variabile	Descrizione
bLogToFile	Tipo: Booleana (0/1) Abilita VirusScan a registrare su file l'attività di scansione Valore predefinito: 1
bLimitSize	Tipo: Booleana (0/1) Abilita VirusScan a limitare le dimensioni del file di registro Valore predefinito: 1
uMaxKilobytes	Tipo: Numero intero (10-999) Specifica le dimensioni massime in kilobyte del file di registro Valore predefinito: 10
bLogDetection	Tipo: Booleana (0/1) Abilita VirusScan a registrare il rilevamento dei virus Valore predefinito: 1
bLogClean	Tipo: Booleana (0/1) Abilita VirusScan a registrare la pulizia dei virus Valore predefinito: 1
bLogDelete	Tipo: Booleana (0/1) Abilita VirusScan a registrare le eliminazioni dei file Valore predefinito: 1
bLogMove	Tipo: Booleana (0/1) Abilita VirusScan a registrare gli spostamenti dei file Valore predefinito: 1
bLogSettings	Tipo: Booleana (0/1) Abilita VirusScan a registrare le impostazioni di sessione Valore predefinito: 1

Variabile	Descrizione
bLogSummary	Tipo: Booleana (0/1) Abilita VirusScan a registrare i riepiloghi di sessione Valore predefinito: 1
bLogDateTime	Tipo: Booleana (0/1) Abilita VirusScan a registrare la data e l'ora dell'attività di scansione Valore predefinito: 1
bLogUserName	Tipo: Booleana (0/1) Abilita VirusScan a registrare il nome utente Valore predefinito: 1
szLogFileName	Tipo: Stringa Specifica il percorso per il file di registro Valore predefinito: C:\McAfee\Viruscan\VSCLOG.TXT

ScanItems

Variabile	Descrizione
ScanItem_x, dove x è un indice a base zero	Tipo: Stringa Abilita VirusScan ad eseguire la scansione dell'elemento Valore predefinito: C:\\|1 * * La stringa è suddivisa in campi tramite il carattere pipe (|): Campo 1: percorso dell'elemento da sottoporre a scansione. Campo 2: booleano (1/0) Valori possibili: 1 - Abilita VirusScan ad eseguire la scansione delle sottocartelle dell'elemento 2 - Abilita VirusScan a non eseguire la scansione delle sottocartelle dell'elemento

SecurityOptions

Variabile	Descrizione
szPasswordProtect	Tipo: Stringa Questa variabile non è configurabile dall'utente. Valore predefinito: 0
szPasswordCRC	Tipo: Stringa Questa variabile non è configurabile dall'utente. Valore predefinito: 0
szSerialNumber	Tipo: Stringa Questa variabile non è configurabile dall'utente. Valore predefinito: 0

ExcludedItems

Variabile	Descrizione
NumExcludeItems	Tipo: Numero intero (0-n) Definisce il numero di elementi esclusi dalla scansione Valore predefinito: 1
ExcludedItem_x, dove x è un indice a base zero	Tipo: Stringa Abilita VirusScan ad escludere l'elemento dalla scansione Valore predefinito: \Recycled|*.*|1|1 * * La stringa è suddivisa in campi tramite il carattere pipe (|): Campo 1: cartella dell'elemento da escludere. Lasciare vuoto nel caso di file singoli nel sistema. Campo 2: file dell'elemento da escludere. Lasciare vuoto se si esclude una cartella senza specificare il nome del file. Campo 3: numero intero (1-3) Valori possibili: 1 - Esclude dalla scansione di file 2 - Esclude dalla scansione del record di boot 3 - Esclude sia dalla scansione del record di boot che dalla scansione di file Campo 4: booleano (1/0) Valori possibili: 1 - Abilita VirusScan ad escludere le sottocartelle dell'elemento escluso 2 - Abilita VirusScan a non escludere le sottocartelle

Glossario

avvio a caldo	Riavvio di un computer effettuato premendo CTRL+ALT+CANC. Vedere anche “boot” e “avvio a freddo.”
avvio a freddo	Accendere un computer o riavviare un computer spegnendolo, attendendo alcuni secondi, quindi riaccendendolo. Altri metodi di riavvio, ad esempio la pressione del pulsante reset o della combinazione di tastiCTRL+ALT+CANC, potrebbero non rimuovere tutte le tracce di un'infezione da virus dalla memoria. Vedere anche “boot” e “avvio a caldo.”
BIOS	Chip di memoria di sola lettura contenente le istruzioni codificate per l'utilizzo di componenti hardware come la tastiera o il monitor. Sempre presente nei computer portatili, il BIOS (ROM di boot) non è suscettibile alle infezioni (a differenza del settore di boot di un disco). Alcuni chip BIOS contengono funzioni antivirus che possono generare falsi allarmi, problemi nel corso dell'installazione e di altro tipo.
blocco di memoria superiore (UMB)	La memoria presente nell'intervallo compreso tra 640 KB e 1024 KB, immediatamente al di sopra del limite del DOS di 640 KB di memoria convenzionale.
boot	Avvio del computer. Il computer carica le istruzioni di avvio dalla ROM di boot di un disco (BIOS) o dal settore di boot. Vedere anche “avvio a freddo” e “avvio a caldo.”
codici di convalida	Informazioni relative a un file eseguibile che VirusScan registra per rilevare infezioni da virus. Vedere anche “codici di ripristino.”
codici di ripristino	Informazioni relative a un file eseguibile che VirusScan registra per ripristinarlo (ripararlo) qualora venga danneggiato da un virus. Vedere anche “codici di convalida.”
convalidare	Controllare che un file sia autentico e non sia stato alterato. La maggior parte dei metodi di convalida si basa sull'elaborazione di una statistica relativa a tutti i dati del file, che probabilmente saranno diversi se il file è stato modificato.
disco di boot	Dischetto protetto da scrittura contenente i file di boot e di sistema del computer. È possibile utilizzare questo dischetto per avviare il computer. È importante utilizzare un disco di boot sul quale non è stato rilevato alcun virus per non rischiare di reinfettare il computer.
disinfettare	Debellare un virus affinché non si diffonda o non danneggi ulteriormente un sistema.

elenco delle eccezioni	Elenco dei file ai quali non è possibile aggiungere i codici di convalida poiché possiedono già funzioni di rilevamento virus incorporate, contengono il codice per l'automodifica o non possono essere infettati da un virus. Tali file vengono in genere ignorati nel corso del controllo di convalida in quanto potrebbero causare un falso allarme.
errori di sistema	Errori che impediscono a VirusScan di completare il proprio lavoro. Le condizioni di errore del sistema includono errori di formattazione del disco, errori relativi ai supporti, errori del file system, errori di rete, errori di accesso ai dispositivi e tentativi di segnalazione non riusciti.
eseguibile compresso	File compresso utilizzando un'utility di compressione dei file come LZEXE o PKLITE. Vedere anche “file compresso.”
eseguibile, file	File contenente istruzioni codificate che devono essere eseguite dal computer. I file eseguibili includono programmi e overlay (codice di programma ausiliario che non può essere direttamente eseguito dall'utente).
falso allarme	Segnalazione di un'infezione virale che in effetti non esiste.
file compresso	File compresso utilizzando una utility di compressione dei file come LZEXE o PKLITE. Vedere anche “eseguibile compresso.”
file danneggiato	File irrimediabilmente danneggiato, ad esempio da un virus.
file infetto	File contaminato da un virus.
file modificato	File modificato dopo l'aggiunta dei codici di convalida, probabilmente da parte di un virus.
infezione degli overlay	Contaminazione da virus di un file contenente un codice di programma ausiliario caricato dal programma principale.
infezione della memoria	Contaminazione della memoria da parte di un virus. L'unico modo sicuro per eliminare l'infezione dalla memoria è quello di *spegnere il computer,* riavviarlo da un dischetto di boot pulito e pulire l'origine dell'infezione utilizzando VirusScan.
infezione del settore di boot	Contaminazione del settore di boot da parte di un virus. L'infezione del settore di boot è particolarmente pericolosa in quanto le informazioni contenute in questo settore vengono caricate nella memoria *prima* dell'esecuzione del codice di protezione antivirus. L'unico modo sicuro per eliminare un'infezione dal settore di boot è quello di avviare il computer da un dischetto di boot pulito e di rimuovere l'infezione con VirusScan.

memoria	Supporto di memorizzazione nel quale i dati o il codice di programma vengono conservati temporaneamente mentre vengono utilizzati dal computer. Il DOS supporta fino a un massimo di 640 KB di memoria convenzionale. Oltre a quel limite, si può accedere alla memoria espansa, alla memoria estesa o a un blocco di memoria superiore (UMB, upper memory block).
memoria convenzionale	Fino a 640KB (1 MB) di memoria principale nella quale il DOS esegue i programmi.
memoria espansa	La memoria del computer al di sopra del limite del DOS di 1MB di memoria convenzionale alla quale ha accesso il paging della memoria. Per sfruttare al meglio la memoria espansa, è richiesto un software speciale, conforme alle specifiche della memoria espansa.
memoria estesa	Memoria lineare al di sopra del limite del DOS di 1 MB di memoria convenzionale. Spesso usata per i dischi RAM e gli spooler di stampa.
operazione di lettura	Qualsiasi operazione nella quale le informazioni vengono lette da un disco, inclusa l'unità disco rigido, un disco floppy, un CD-ROM o un'unità di rete. Tra i comandi DOS che eseguono operazioni di lettura si hanno DIR (elenco delle directory), TYPE (visualizzazione del contenuto di un file) e COPY(copia dei file). Vedere anche “operazione di scrittura.”
operazione di scrittura	Qualsiasi operazione nella quale le informazioni vengono registrate su un disco. Tra i comandi che eseguono operazioni di scrittura si hanno quelli di salvataggio, spostamento e copia dei file. Vedere anche “operazione di lettura.”
programma ad automodifica	Software che modifica i propri file di programma, spesso per proteggersi contro i virus o la copia illegale. Questi programmi dovrebbero essere inclusi in un elenco di eccezioni per evitare che tali modifiche vengano segnalate da VirusScan come falsi allarmi.
protezione da scrittura	Meccanismo che protegge i file o i dischi da modifiche non autorizzate. Un file viene protetto da scrittura cambiando i relativi attributi di sistema. Un dischetto viene protetto da scrittura spostando l'apposita linguetta in modo da aprire il foro quadrato (dischetti da 3,5 pollici) o coprendo la tacca con una linguetta di protezione (dischetti da 5,25 pollici).
rapida	Opzione di scansione più rapida del normale, ma meno completa in quanto controlla una parte più limitata di ogni file.
record MBR (Master Boot Record)	Porzione di disco rigido contenente una tabella di partizione che divide l'unità in "parti", alcune delle quali vengono assegnate ai sistemi operativi diversi dal DOS. Il record MBR accede al settore di boot.

rilevamento	Scansione della memoria e dei dischi alla ricerca di indizi che segnalino la presenza di un virus. Alcuni metodi di rilevamento includono la ricerca di stringhe o motivi virali comuni, il confronto dell'attività di file sospetti con l'attività di virus conosciuti e il controllo di file per rilevare modifiche non autorizzate.
settore di boot	Porzione di un disco contenente le istruzioni codificate per il sistema operativo relative all'avvio del computer.
virus	Programma software che si associa ad un altro programma su disco o si nasconde nella memoria di un computer e si diffonde da un programma all'altro. I virus possono danneggiare i dati, causare blocchi del sistema, visualizzare messaggi e così via.
virus macro	Virus che infetta le macro, ad esempio quelle utilizzate da applicazioni come Microsoft Word ed Excel. Sebbene il testo di un documento creato in una di queste applicazioni non contenga codice eseguibile e quindi non possa essere contaminato, un documento può contenere macro infettabili. I virus macro costituiscono il segmento a crescita più rapida dell'intera famiglia dei virus: il numero di virus macro conosciuti raddoppia ogni tre mesi.
virus polimorfo	Un virus che tenta di sfuggire al rilevamento modificando la propria struttura interna o le proprie tecniche di codifica.
virus sconosciuto	Virus non ancora identificato ed elencato in SCAN.DAT. VirusScan è in grado di rilevare virus sconosciuti osservando le modifiche nei file probabilmente provocate da un'infezione.

Indice

E

F

G

I

L

M

N

O

P

R

S

T

U

V