

# **NOD32**

S i s t e m a   a n t i v i r u s

## **Manuale per l'utente**

Copyright © 1997 – 2003 ESET, LLC. - Future Time S.r.l.  
Tutti i diritti riservati.

*È vietata la riproduzione o la trasmissione del presente documento in qualunque forma o con qualsiasi mezzo, elettronico o cartaceo, per qualunque scopo, senza l'espresso consenso scritto di ESET, L.L.C. o di Future Time S.r.l.*

*Le informazioni contenute nel presente documento sono soggette a modifiche senza preavviso.*

*I nomi di alcuni prodotti di programma e i nomi aziendali usati nel presente documento possono essere marchi registrati o marchi di proprietà di altre società.*

**Future Time S.r.l.**  
Viale Luca Gaurico, 257  
00143 R O M A

Sito web: <http://www.nod32.it/>

Ufficio Vendite: tel. 06 503 17 12 fax 06 503 70 78  
Assistenza tecnica: tel. 06 503 42 27 o [supporto@nod32.it](mailto:supporto@nod32.it)

# Indice:

<b>1</b>	<b>Installazione.....</b>	<b>4</b>
1.1	Installazione del software .....	4
1.2	Tipo di installazione.....	5
1.3	Nome utente e password .....	6
1.4	Collegamento Internet.....	7
1.5	Scanner residente .....	9
<b>2</b>	<b>Cosa fare dopo l'installazione.....</b>	<b>10</b>
2.1	Verificare che sia in funzione: .....	10
2.1.1	Verificare che il database sia aggiornato .....	11
2.1.2	Eeguire la scansione del sistema .....	12
<b>3</b>	<b>Che succede se si rileva un virus? .....</b>	<b>13</b>
3.1.1	Durante scansione on-demand (NOD32): .....	13
3.1.2	Durante il normale uso del computer: .....	14
<b>4</b>	<b>Appendice A: Risoluzione dei problemi.....</b>	<b>15</b>
<b>5</b>	<b>Appendice B: Tipi di installazione.....</b>	<b>16</b>
<b>6</b>	<b>Appendice C: Invio dei campioni di virus ai laboratori Eset.....</b>	<b>17</b>
<b>7</b>	<b>Appendice D: Altre fonti di informazione .....</b>	<b>22</b>
<b>8</b>	<b>Glossario .....</b>	<b>18</b>
<b>9</b>	<b>Indice.....</b>	<b>23</b>

# 1 Installazione

---

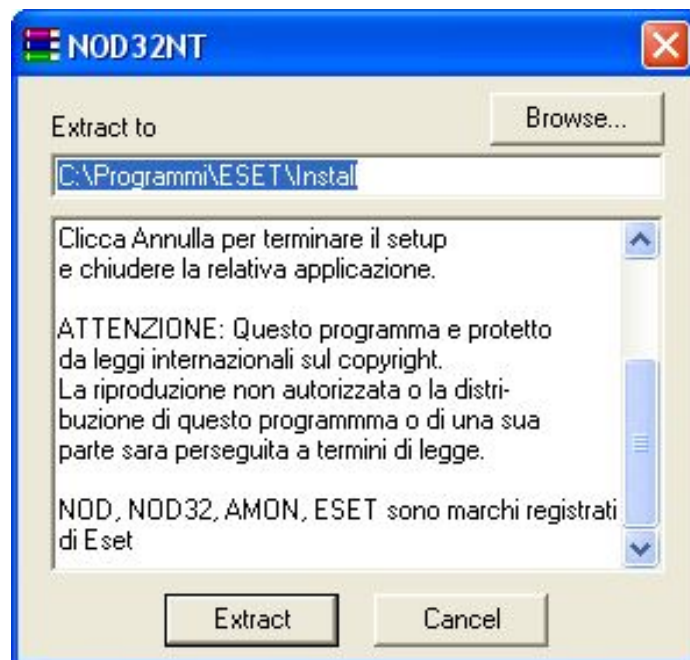
Prima dell'installazione, verificare che l'unità del disco dove si prevede di installare NOD32 disponga di spazio sufficiente. L'installazione richiede circa 20 MB di spazio libero su disco. Se nel sistema è stato precedentemente installato un altro programma antivirus, lo scanner residente (o on-access) può entrare in conflitto con NOD32. Solitamente questi tipi di scanner visualizzano un'icona nella barra di sistema (l'area della barra delle attività accanto all'orologio del sistema). Se è presente, deve essere completamente disinstallato. Il modo più semplice per evitare problemi consiste nel disinstallare qualsiasi altro software antivirus prima di installare NOD32.

## 1.1 Installazione del software

Il paragrafo descrive l'installazione da un CD o da un file scaricato da Internet:

- Per installare NOD32 inserire il CD originale nell'apposita unità e, una volta avviato, seguire le istruzioni mostrate dal programma di *autorun* (NOD32RUN.EXE). Se l'installazione non parte automaticamente, è necessario eseguire il file NOD32RUN.EXE dalla directory di base del CD (Esplora CD).
- Per installare NOD32 da Internet, scaricare il programma di installazione dal sito web di NOD32 ([www.nod32.it/download/download.htm](http://www.nod32.it/download/download.htm)). Verificare di disporre della versione idonea al proprio sistema operativo (per esempio "Windows 95/98/Me" o "Windows NT/2000/2003/XP"). Quando verrà richiesto di salvare o aprire il file, selezionare Apri: l'installazione partirà in automatico al termine del download. Oppure, se si è scelto salvare il file, eseguirlo semplicemente dalla cartella dove è stato salvato.

Nel caso in cui NOD32 sia stato scaricato da Internet, per prima cosa è necessario estrarre i file di installazione dall'archivio di installazione. Il programma di installazione chiede in quale cartella eseguire l'estrazione. Usare quella suggerita per default a meno che non esista una motivazione specifica per cambiarla. Fare clic su "Estrai" per continuare.

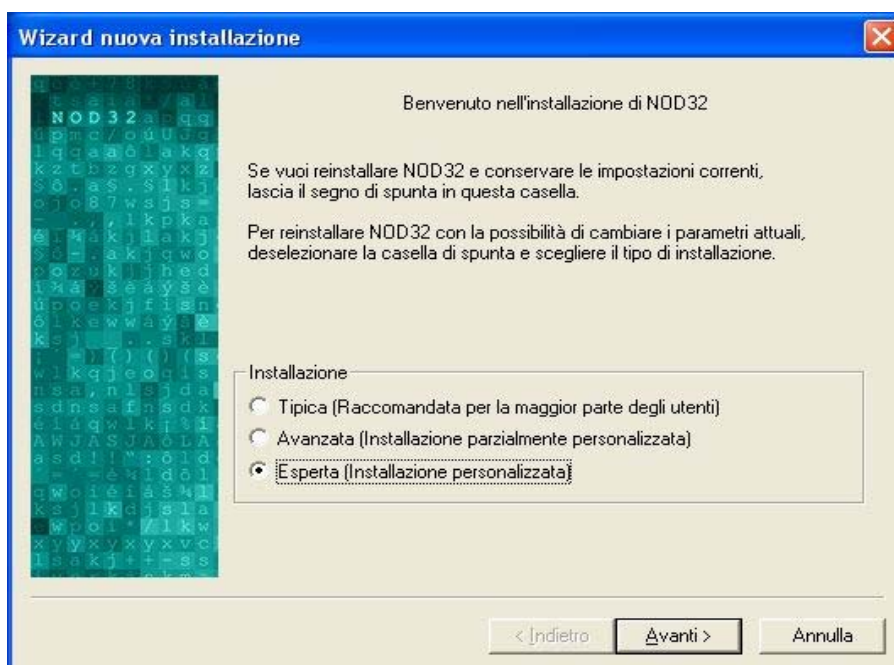


La procedura di installazione verifica la presenza di un'altra versione di NOD32 e, se la trova, chiede di usare le impostazioni della versione corrente. Questa operazione permette di importare il nome utente e la password di aggiornamento e le altre impostazioni nella nuova versione. Se

non si desidera mantenere le impostazioni correnti, eliminare il segno di spunta dalla casella di scelta .

## 1.2 Tipo di installazione

Se non si sta eseguendo un aggiornamento da una versione precedente, oppure se non si sceglie di utilizzare di nuovo le impostazioni correnti, scegliere il tipo di installazione.

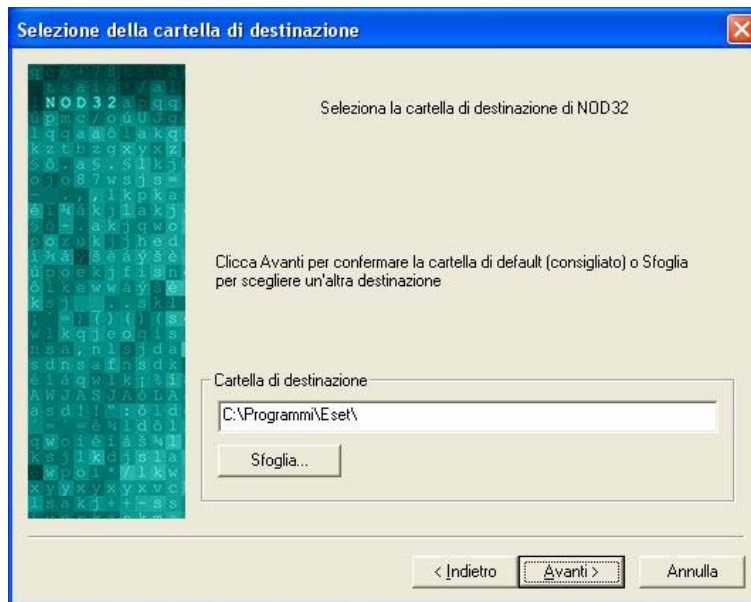


- **Tipica** – consigliata per la maggior parte degli utenti.
- **Avanzata** – utile per gli amministratori di sistema.
- **Esperti** – imposta manualmente tutte le opzioni di installazione.

*(vedere l'Appendice B per informazioni dettagliate)*

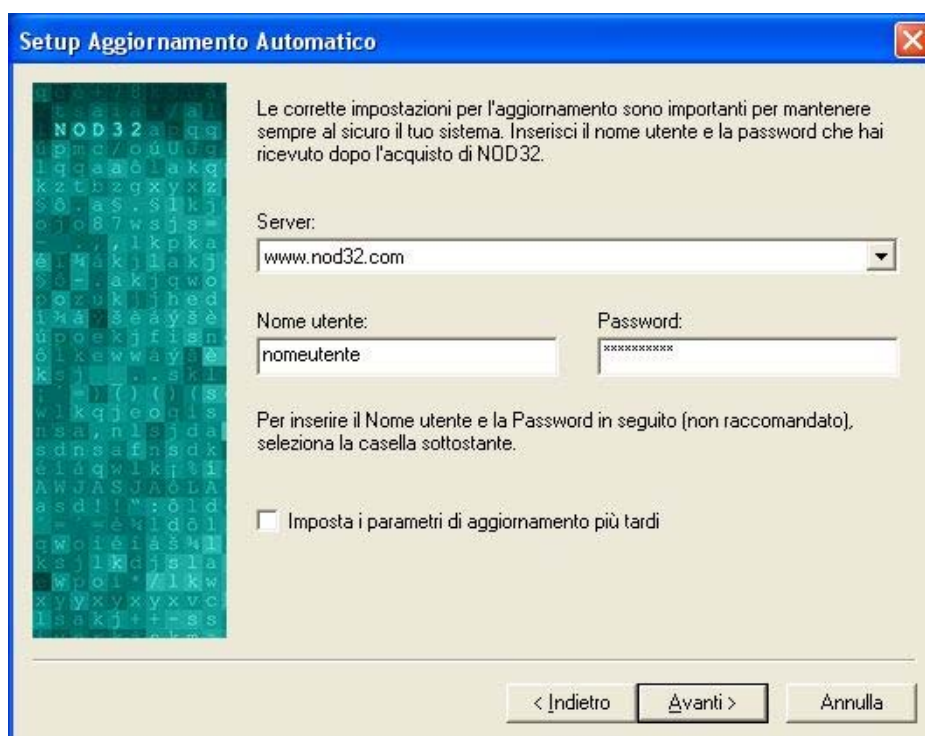
Quindi, leggere e scegliere di accettare o rifiutare il Contratto di Licenza del Software. Si osservi che in caso di rifiuto, non è possibile procedere con l'installazione.

Selezionare la cartella di installazione del programma. Quella di default è idonea per la maggior parte degli utenti.



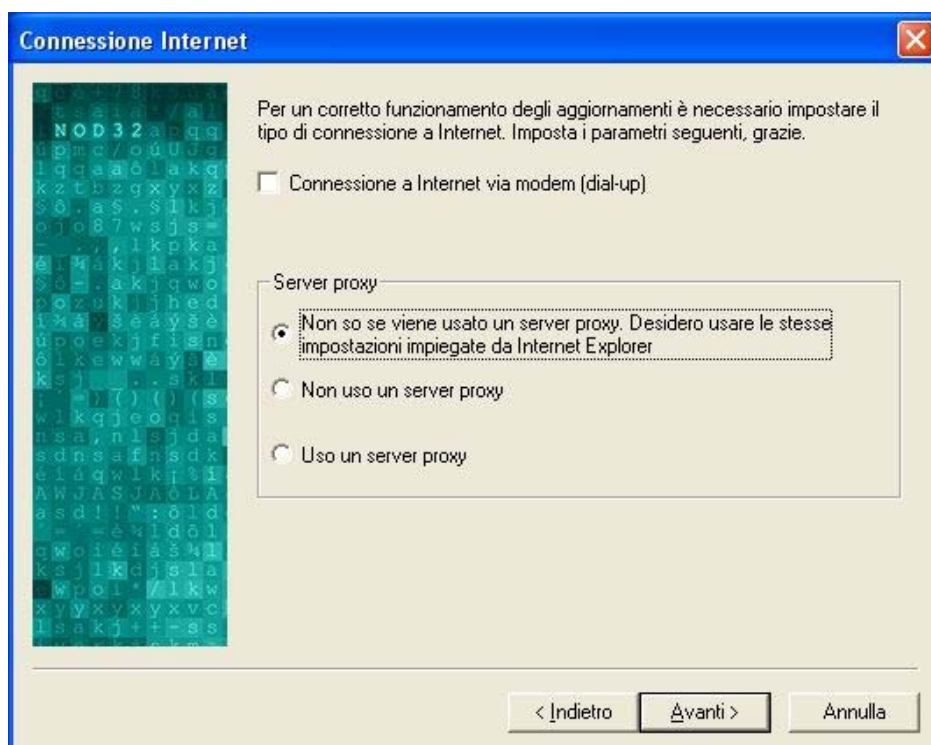
### 1.3 Nome utente e password

Sulla schermata successiva, inserire il nome utente e la password forniti dal proprio rivenditore. Prestare particolare attenzione alle maiuscole e alle minuscole, che devono essere inserite esattamente come sono state fornite (cioè: sia il nome utente che la password sono sensibili alle maiuscole). Non attivare la casella "fornire i parametri in seguito" a meno che non si desideri inserire il nome utente e la password durante l'installazione (questa procedura è sconsigliata, poiché è molto importante che il computer sia in grado di ricevere gli aggiornamenti più recenti dai server di Eset al completamento dell'installazione).



## 1.4 Collegamento Internet

Le impostazioni del collegamento Internet consentono al computer di ricevere gli aggiornamenti nel modo più efficiente, secondo il tipo di connessione di cui si dispone. Gli utenti con modem devono attivare la casella “Connessione a Internet via modem (dial-up)” mentre gli utenti che si connettono a Internet via cavo, ADSL, LAN e a banda larga devono lasciare questa casella disattivata.



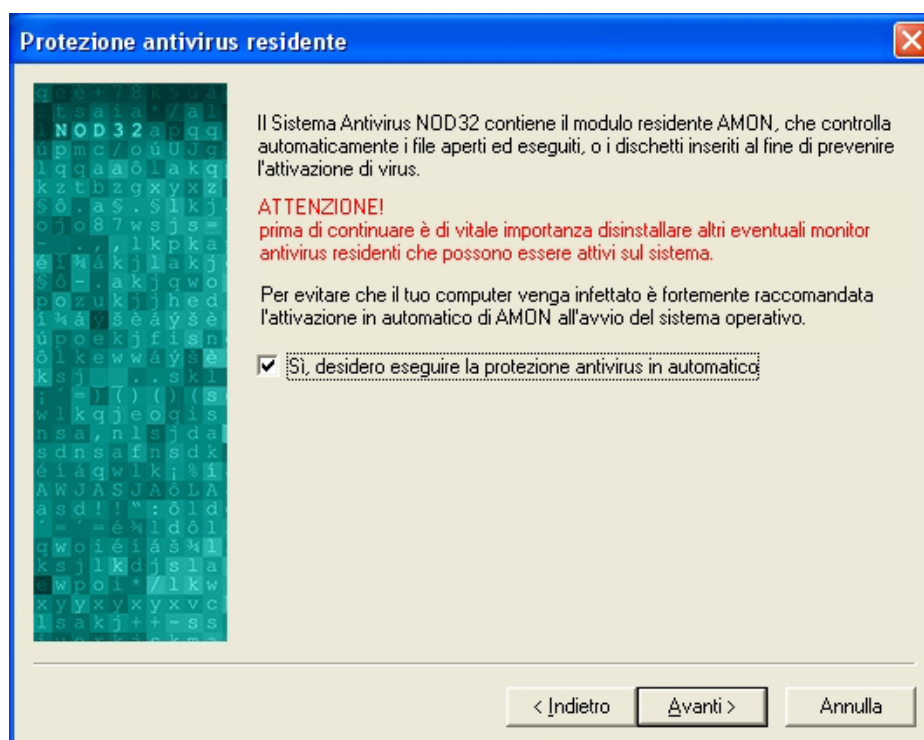


**Nota:** alcuni utenti a banda larga e ADSL devono avviare la connessione Internet manualmente dopo che il computer è acceso e in funzione. Se si dispone di questo tipo di connessione, l'attivazione della casella "Connessione a Internet via modem" istruisce NOD32 a verificare la presenza di aggiornamenti al momento del collegamento a Internet. Comportamento utile se si rimane normalmente collegati a Internet solo per breve tempo. Tuttavia, se di norma si è collegati per almeno due ore, lasciare questa casella disattivata.

Se la connessione a Internet avviene attraverso un server proxy, selezionare questa opzione. In caso di dubbio, l'uso dell'opzione "Non so se viene ....." rappresenta la soluzione più sicura, poiché configura NOD32 per usare le stesse impostazioni di Internet Explorer.

## 1.5 Scanner residente

Nell'installazione *Tipica* la schermata finale è quella relativa alla configurazione dello scanner residente. AMON, lo scanner residente (oppure on-access) costituisce uno dei moduli essenziali del sistema antivirus NOD32. Tuttavia, se nel sistema è stato precedentemente installato un altro software antivirus, il suo scanner residente (o on-access) può creare gravi malfunzionamenti, entrando in conflitto con AMON. Solitamente questi tipi di scanner visualizzano un'icona nella barra di sistema (l'area della barra delle attività accanto all'orologio del sistema). Se è presente, deve essere completamente disinstallato. Il modo più semplice per evitare problemi consiste nel disinstallare qualsiasi altro software antivirus prima di installare NOD32. Se si è certi che nessun altro scanner antivirus sia in funzione attivare la casella "Sì, desidero eseguire la protezione antivirus in automatico".



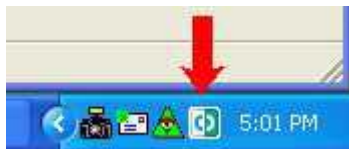
Fare clic su Avanti e, se le impostazioni sono soddisfacenti, fare nuovamente clic su Avanti. L'installazione viene completata con la richiesta di riavvio del computer. Fare clic su Fine per riavviare e iniziare a proteggere il computer con il Sistema Antivirus NOD32.

## 2 Cosa fare dopo l'installazione

---

### 2.1 Verificare che sia in funzione:

Nella barra di sistema deve essere visibile un'icona come questa:



Indica che NOD32 è in funzione. Fare clic una volta sull'icona per aprire la seguente finestra:



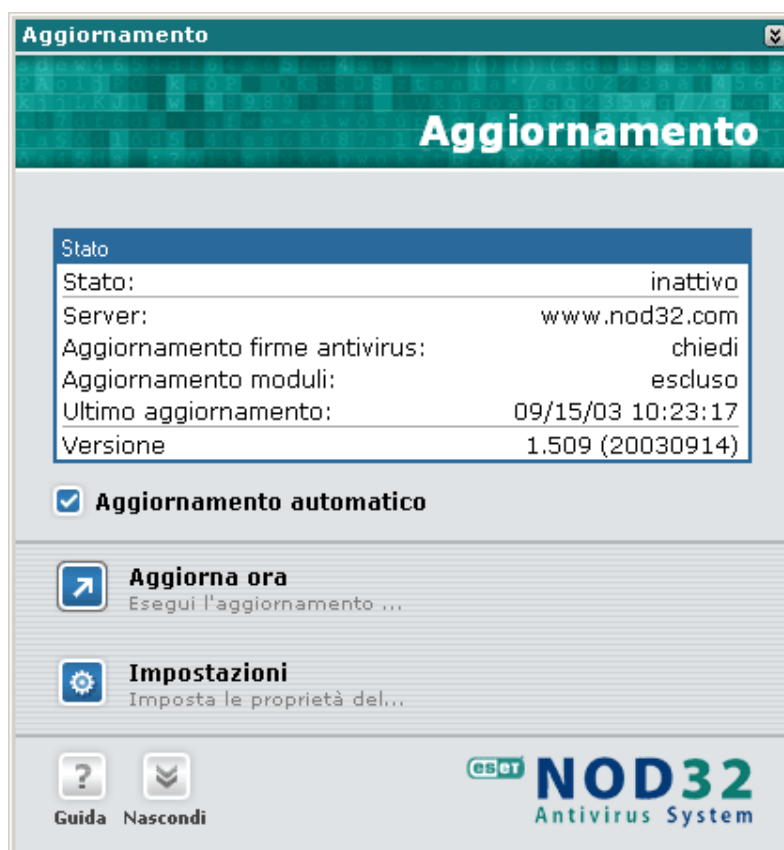
Questo è il Control Center di NOD32

Da qui si controllano tutti gli aspetti dei moduli NOD32.

**Nota:** il modulo EMON (non presente nell'immagine superiore) è progettato per funzionare con Microsoft Outlook installato in Modalità Corporate. Se non si usa Outlook, oppure se è stato installato come client di posta Internet, non è necessario il modulo EMON. In questo caso IMON protegge la posta prelevata attraverso il protocollo POP3.


## 2.1.1 Verificare che il database sia aggiornato

Nel Control Center (pagina precedente) fare clic su “Aggiorna”. La finestra sotto illustrata si apre a destra della finestra del Control Center.



Verificare che la casella di aggiornamento automatico sia attivata e fare clic su *Aggiorna ora*.

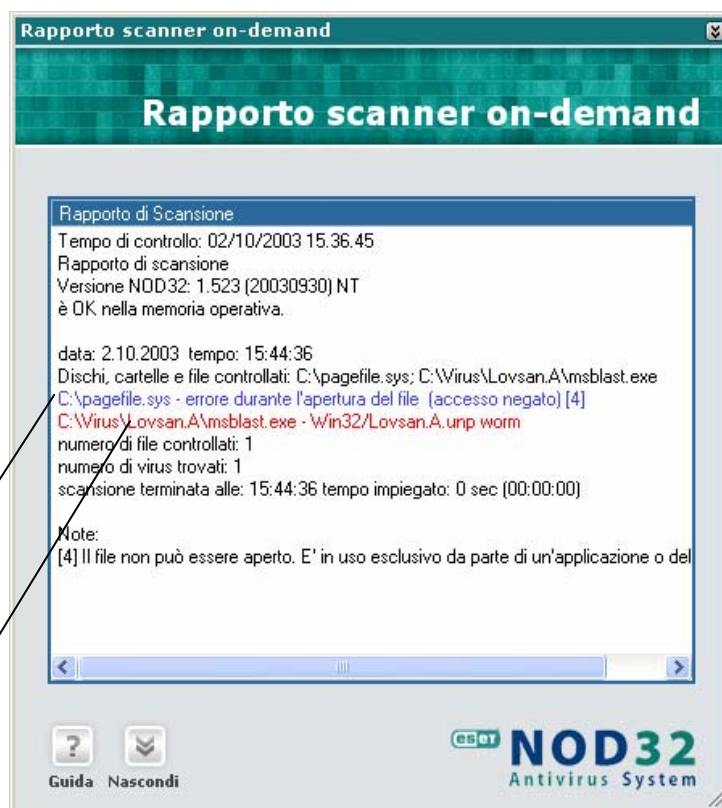
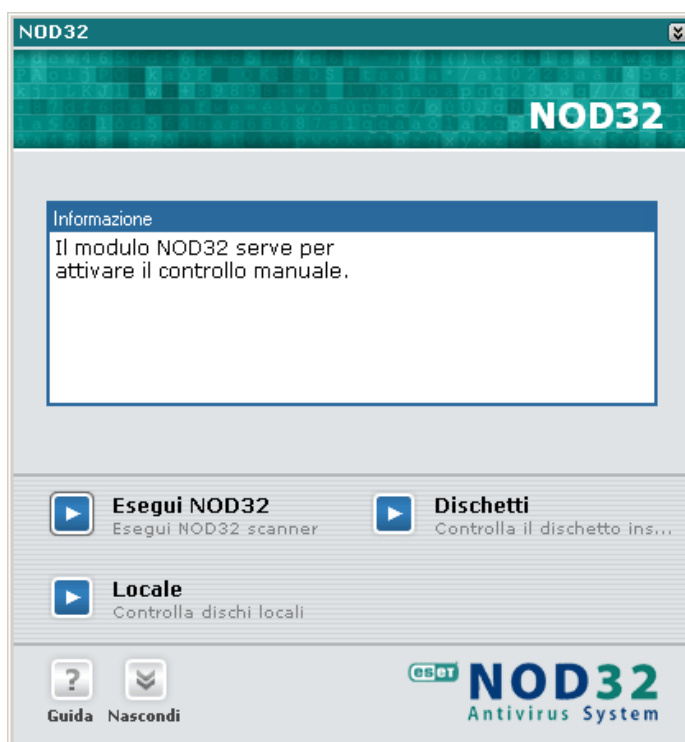
Se compare una finestra di dialogo che richiede nome utente e password, significa che questi sono stati inseriti in modo errato durante l'installazione. Fare clic su *Impostazioni* in questa finestra per inserire nuovamente il nome utente e la password inviati dal proprio fornitore.

 **Nota:** il nome utente e la password sono sensibili alle maiuscole e devono essere inseriti correttamente, compresa la linea “-“ del nome utente.

## 2.1.2 Eseguire la scansione del sistema

Nel pannello sinistro del Control Center, selezionare la sezione "Moduli" e poi "NOD32". Nella finestra che compare sulla destra, fare clic sul pulsante "Locale". Ciò attiva la scansione del sistema per trovare le possibili infezioni esistenti. I metodi avanzati di rilevamento di NOD32 possono trovare infezioni non rilevate dal vecchio scanner.

Se il computer funziona con Windows NT, 2000/2003 oppure XP, è possibile che non si aprano uno o due file durante la scansione. In condizioni normali, *pagefile.sys* e *hiberfil.sys* non possono essere aperti per la scansione poiché vengono usati dal sistema operativo. Il primo file fa parte della memoria di sistema (memoria virtuale) e quindi viene sottoposto a scansione durante il controllo della memoria, che NOD32 esegue automaticamente all'avvio. Il secondo file fa parte del sistema di ibernazione e viene sovrascritto ogni volta che si usa l'opzione di chiusura con ibernazione. Quindi è del tutto normale che NOD32 segnali l'impossibilità di aprire i file menzionati sopra. (Il file *hiberfil.sys* è presente solo sui sistemi 2000/XP che hanno l'ibernazione attivata)



*Non è possibile aprire il file Pagefile.sys. Fatto del tutto normale.*

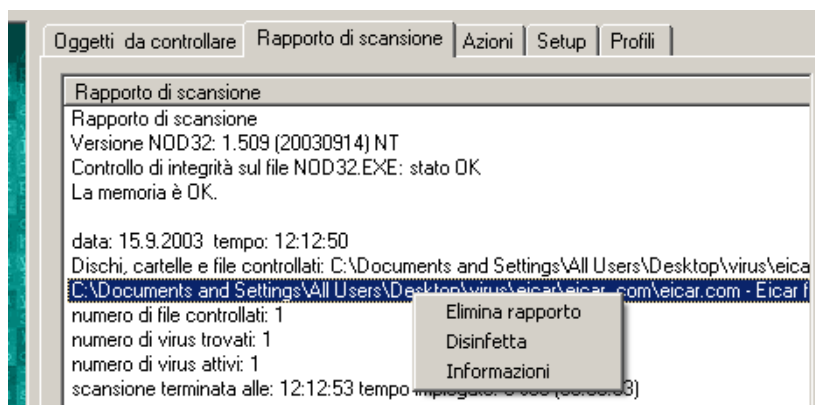
*Questo è un virus rilevato da NOD32!*

Come si deve procedere nel caso in cui venga trovato un virus? Proseguire la lettura del manuale...

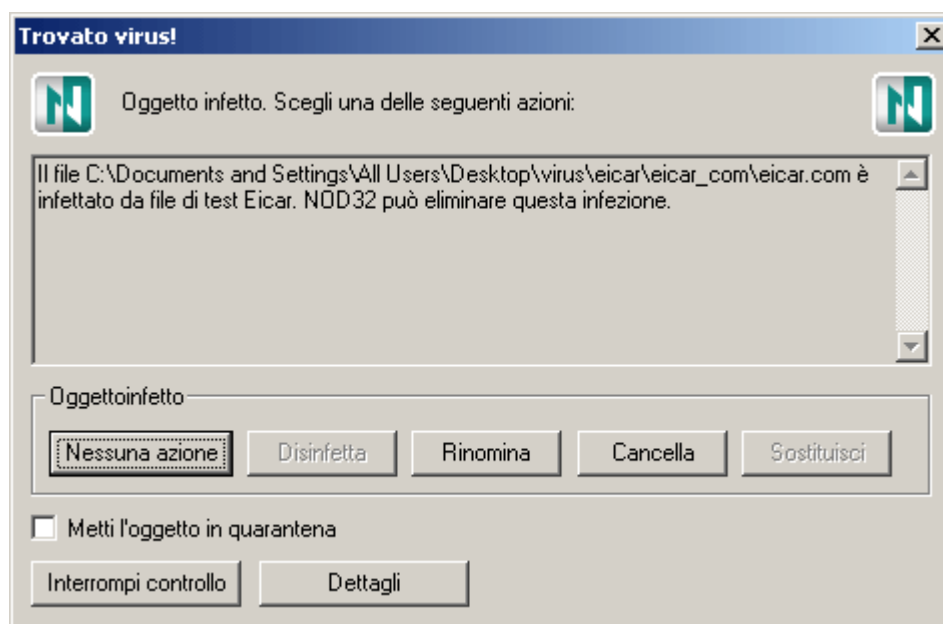
### 3 Che succede se si rileva un virus?

#### 3.1.1 Durante la scansione on-demand (NOD32):


Durante una normale scansione con NOD32 è possibile vedere allarmi di individuazione virus come quello illustrato. Questi appaiono come una voce in rosso nel rapporto di scansione e indicano il nome e il percorso del file e il nome del virus. Per gestirle basta fare clic con il pulsante destro del mouse sulla voce di rapporto e selezionare l'opzione *Disinfetta* dal menu a comparsa:



Compare una schermata come questa:



In questo caso il file infettato non è ripristinabile, oppure non conteneva dati oltre al virus stesso. Questo è un evento abbastanza comune con i "worm" che arrivano via e-mail e la soluzione consiste nella semplice eliminazione del file infetto.

 **Nota:** se il nome dell'infezione contiene le parole "sconosciuto" o "probabile..", attivare la casella di Quarantena prima di pulire o eliminare il file. Quindi è possibile seguire le istruzioni per inviare un campione del virus in quarantena ai nostri laboratori per l'analisi. (vedere l'Appendice C per maggiori informazioni)

### 3.1.2 Durante il normale uso del computer:

Il Sistema Antivirus NOD32 vigila costantemente sulla sicurezza del sistema bloccando eventuali virus che tentano di infettare il computer durante il suo normale utilizzo. Questo tipo di protezione impedisce l'infezione del PC. Gli allarmi di individuazione virus, in momenti diversi dall'esecuzione di una scansione specifica, generalmente provengono da uno dei moduli "on-access" di NOD32: AMON (controllo file), IMON (controllo posta elettronica POP3), o EMON (controllo posta elettronica MAPI, cioè posta ricevuta con Microsoft Outlook installato in modalità *corporate*).

Gli allarmi sono chiaramente visibili sul monitor del computer:



Come per lo scanner on-demand, le opzioni per la gestione di un'infezione sono Disinfetta, Cancella e Rinomina, con l'opzione di mettere prima in quarantena una copia del file infetto. Anche in questo caso, è solitamente possibile cancellare i file che non possono essere puliti poiché non contengono alcun dato utile.

## 4 Appendice A: Risoluzione dei problemi

---

**D:** Il mio nome utente e la mia password non funzionano.

**R:** Se compare una finestra di dialogo che richiede nome utente e password, significa che sono stati inseriti in modo errato durante l'installazione. Fare clic su *Impostazioni* in questa finestra per inserire nuovamente il nome utente e la password inviati dal proprio rivenditore.



**Nota:** il nome utente e la password sono sensibili alle maiuscole e devono essere inseriti correttamente, compresa la linea “-“ del nome utente.

**D:** Ricevo il messaggio: "Microsoft Outlook. Non è presente alcun client di posta predefinito oppure il client di posta corrente non può soddisfare la richiesta del messaggio. Eseguire Microsoft Outlook e impostarlo come client di posta predefinito". Qual è il problema?

**R: Breve descrizione del messaggio di errore:** Questo messaggio è visualizzato da Microsoft Outlook quando NOD32 cerca di accedere a MAPI32.DLL.

### **Soluzioni consigliate:**

Se si utilizza Microsoft Outlook per ricevere la posta elettronica e non è impostato come client di posta predefinito, è possibile impostarlo come client di posta predefinito in questo modo:

- In Internet Explorer>Strumenti>Opzioni Internet>Programmi>Posta elettronica – modificare con Microsoft Outlook (se applicabile).
- Se è installato Microsoft Outlook e non lo si usa: prendere in considerazione la disinstallazione di Microsoft Outlook.
- È anche possibile rinominare MAPI32.DLL in altro modo (come MAPI32.DLL.SAV)
- Infine, è possibile fare in modo che NOD32 non usi l'interfaccia MAPI. Nello scanner di NOD32 andare nella pagina *Setup* e togliere il segno di spunta dalla casella "Usa interfaccia MAPI".

**D:** Posso usare IMON di NOD32 con il client di posta X?

**R:** Se il client di posta usa il protocollo POP3, probabilmente funziona con IMON senza bisogno di ulteriore configurazione. Si osservi che se si utilizza IMAP, o un altro protocollo attualmente non supportato da IMON, si è ancora protetti dall'apertura di allegati non sicuri per mezzo del modulo AMON.


Altre domande?:

Consultare la sezione completa FAQ sul sito <http://www.nod32.it/support/faq.htm>

## 5 Appendice B: Tipi di installazione

---

Opzione	Tipica	Avanzata	Esperti
Modalità silenziosa, impostazioni protette da password		X	X
Tipo GUI, schermata a comparsa			X
Invio avvertenze per posta elettronica o messenger			X
Server di aggiornamento, nome utente e password	X	X	X
Connessione Internet e impostazioni proxy	X	X	X
Configurazione aggiornamento automatico		X	X
Lancio protezione residente all'avvio	X	X	X
Posizionamento icona sul desktop		X	X
Attiva scansione menu di scelta rapida di Explorer		X	X
Attivazione IMON, modifica della posta infetta e allegati avvisi alla posta elettronica		X	X

 **Nota:** la maggior parte di queste impostazioni (e molte altre) possono essere configurate dopo l'installazione di NOD32, a prescindere dal tipo di installazione selezionata. Le eccezioni sono: Attiva scansione del menu contestuale di Explorer e Posiziona l'icona sul desktop.

## 6 Appendice C: Invio dei campioni di virus ai laboratori Eset

---

Talvolta si riceve un allarme virus dove il nome dell'infezione è "sconosciuto" o "probabile...". Ciò accade perché uno dei moduli di NOD32 ha rilevato caratteristiche di tipo virus in un file, ma non possiede una firma corrispondente per verificare il nome del virus. Ciò è molto frequente con le infezioni recenti che non sono state ancora identificate.

NOD32 vanta un incredibile record di rilevamento di nuovi virus e worm ancora sconosciuti, grazie alla sensibilità e alla potenza di queste tecniche di scansione "algoritmica", conosciute anche come *euristica*. Poiché esiste molto spesso del *malware* (software dannoso) ancora sconosciuto, ci interessa ricevere campioni di questi file per analizzarli.

Per inviare un campione a Future Time attivare la casella di Quarantena prima di pulire, rinominare o cancellare il file sospetto. La procedura di quarantena salva una copia del file in forma cifrata e non eseguibile, in modo che nessuno sia accidentalmente infettato spostando il file o inviandolo per posta elettronica.

I file in quarantena vengono salvati (per default) in "C:\Programmi\ESET\infected\". Ciascun file infetto viene memorizzato in due parti, una che termina per .NQF (NOD32 Quarantine File), l'altra per .NQI (NOD32 Quarantine Information). Il nome dei file in quarantena viene generato casualmente – se si dispone di un certo numero di questi file nella cartella "infetti", è possibile che si debba guardare la data di creazione per determinare quali file sono appena stati salvati: fare clic con il pulsante destro sul file e selezionare *Proprietà*. Inviare per posta elettronica entrambe le parti a [supporto@nod32.it](mailto:supporto@nod32.it).

## 7 Glossario

---

### A

**Ankle-biter** individuo che si atteggia o aspira a diventare un hacker/cracker ma che invece possiede una conoscenza limitata dei sistemi informatici e delle tecniche di intrusione. In genere si tratta di persone che usano semplicemente dei programmi dolosi scritti da altri e reperiti attraverso Internet. Vengono anche definiti con il termine script kiddie.

**Antivirus** software scritti per intercettare, prevenire ed eliminare l'azione di virus e di altri tipi di malware. Si dividono in due categorie principali. Gli scanner on demand, che vengono lanciati esplicitamente dall'utente o da uno scheduler al fine di eseguire attivamente la scansione di memoria, file e settori. E i monitor on access, antivirus residenti che effettuano la scansione solo in risposta a particolari eventi: esecuzione di programmi, apertura e creazione di file, lettura/scrittura di settori, ecc.

**Auditing** controllo di un sistema, effettuato in modo tale da permettere di confrontare le attività svolte sul sistema analizzato con le politiche e le procedure stabilite al fine di determinare la loro conformità, suggerendo eventualmente l'opportunità di introdurre delle migliorie.

**Autenticazione** processo attraverso il quale due o più entità separate, ad esempio un client e un server, possono stabilire la reciproca identità in base a delle regole di sicurezza predefinite. I sistemi di autenticazione sono particolarmente rilevanti nelle connessioni di rete.

### B

**Backdoor** in origine, termine usato per identificare delle "porte di servizio" non documentate create dai progettisti di un sistema al fine di garantirsi un accesso privilegiato, in grado di scavalcare il normale processo di autenticazione. Attualmente, designa anche dei particolari cavalli di troia che permettono la gestione abusiva dei sistemi dove gli utenti li hanno incautamente installati. In genere, si tratta di programmi concepiti per consentire accessi indebiti partendo da computer remoti.

**Behavior Blocker** tipo di programma, in genere residente nella memoria del computer, che scherma il sistema da azioni comunemente riscontrate nei virus e in altro tipo di malware: scrittura su file eseguibili o su settori di sistema, tentativi di tracciamento dei gestori di interrupt (tunneling), modifica di chiavi nel Registro di sistema, ecc. A differenza degli scanner e dei monitor antivirus, che identificano i virus analizzandone la struttura, i behavior blocker tentano di prevenirne l'attività in base al comportamento.

**BIOS** acronimo di Basic Input Output System, il microcodice (firmware) presente nelle memorie a sola lettura dei computer, utile per avviare il processo di bootstrap, che inizia all'accensione del computer e termina con il caricamento in memoria del sistema operativo

**Bootstrap** quando viene acceso il computer e il processore è inizializzato, vengono eseguiti il POST (Power On Self Test) e quindi una ricerca del settore di boot sul disco di avvio. Se il settore di boot viene trovato con successo, il suo contenuto è caricato in memoria all'indirizzo di memoria esadecimale 0000:7C00 e il controllo è passato alle istruzioni caricate in tale indirizzo. Se l'avvio è effettuato da un disco rigido, in memoria viene caricato il contenuto del Master Boot Record (MBR), il cui codice ha il compito di trovare e caricare il boot sector della partizione attiva. Il boot sector verifica la presenza di alcuni file di base del sistema operativo, li legge e cede il controllo al loro codice. In tal modo viene avviato l'intero sistema operativo.

**Boot sector/Master Boot Record infector** virus che infettano i settori di sistema, presenti nella struttura di dischetti removibili e dischi rigidi (Boot sector) o soltanto sui dischi rigidi (Master Boot Record). Questi tipi di virus lavorano a basso livello, vengono caricati in memoria durante il processo di bootstrap, prima che il sistema operativo si trovi in memoria, e usano i servizi del BIOS per infettare i settori di dischetti e dischi rigidi.

### C

**Cavallo di troia, trojan horse** programma software che effettua una o più operazioni, in genere nascoste e dolose, diverse da quelle dichiarate. A differenza di un virus, un cavallo di troia non possiede le procedure necessarie per replicare se stesso.

**Crack** programma software usato per modificare un altro programma in modo tale da violarne o scavalcarne le limitazioni impostate, garantendo così privilegi non autorizzati al programma modificato e/o al sistema di cui controlla la sicurezza.

**Crash** blocco delle funzioni svolte da un componente del sistema o interruzione delle operazioni dell'intero sistema.

## D

**DDoS (Distributed Denial of Service)** attacco Denial of Service portato da più persone che collaborano tra loro o da un singolo in grado di pilotare l'azione di più computer zombie.

**DOS (Denial Of Service)** tipo di attacco portato contro sistemi e reti di computer al fine di impedire il normale traffico di informazioni. Gli attacchi DOS possono provocare la saturazione delle risorse dei sistemi o un loro crash, in modo tale da renderli inutilizzabili per i normali utenti. Gli attacchi DOS sono basati su un traffico anomalo di informazioni o sullo sfruttamento di uno o più bug presenti nei protocolli di comunicazione. Alcuni esempi di attacchi DOS sono SYN flood, OOB Nuke, Ping of Death, ICMP Nuke, Land, Smurf e molti altri.

## E

**Euristica** deriva dalla parola greca eurisko, che significa trovare. La scansione euristica degli antivirus fa ricorso a tecniche particolari che permettono di individuare dei virus ancora sconosciuti. In genere, le tecnologie euristiche si basano su firme digitali generiche, automi a stati finiti, sistemi esperti e reti neurali. Sebbene abbia il vantaggio di identificare dei virus in base alla loro struttura piuttosto che attraverso un più classico riconoscimento per firme digitali, che richiede sempre l'analisi preventiva del codice virale, la scansione euristica può facilmente provocare dei falsi positivi.

## F

**Falso positivo** errata segnalazione da parte di un antivirus, che individua un virus in un elemento non infetto (memoria, file, settore). In genere i falsi positivi sono abbastanza comuni quando l'antivirus impiega la scansione euristica.

**File infector** virus che infetta i file, modificandone la struttura interna in modo tale da essere eseguito quando viene lanciata l'applicazione ospite. I file infector possono limitarsi ad alterare il file ospite in maniera tale da preservarne le funzioni (virus parassita) oppure ne sostituiscono completamente il codice, rendendo irrecoverabile il file infettato (overwriting virus). Un particolare tipologia di file infector, i companion virus, non modificano in alcun modo i file infettati: creano dei file che hanno lo stesso nome dei file oggetto dell'attacco, ma estensione diversa. Per garantire l'esecuzione delle copie infette, i companion virus sfruttano la priorità di ricerca che alcuni sistemi operativi assegnano alle estensioni di un file eseguibile, regola che viene applicata quando l'utente esegue un programma specificando soltanto il suo nome. Ad esempio, se nella stessa directory risiedono due file che hanno lo stesso nome, l'uno con estensione .COM e l'altro con .EXE, la shell COMMAND.COM assegnerà sempre una priorità maggiore al primo nel caso in cui l'utente esegua il programma su linea di comando omettendo la sua estensione.

**Firewall** dispositivo hardware e/o software volto a proteggere una rete locale dal traffico di informazioni che transita da e verso reti esterne, in particolar modo Internet. I firewall permettono di intercettare i pacchetti di rete, di analizzarne il contenuto e di filtrarli in modo tale da consentire l'applicazione di una serie di regole di sicurezza, tali da includere o da escludere segmenti del flusso di dati, autorizzando o meno il viaggio verso la loro destinazione.

## G

## H

**Hacker** in origine, il termine veniva usato soltanto per designare persone di eccezionale bravura ed esperienza nel merito dei sistemi informatici. Attualmente, è stato esteso per connotare individui che impiegano le loro conoscenze per penetrare nella sicurezza dei sistemi al fine di accedere a delle informazioni in maniera non autorizzata. Nel gergo informatico, gli hacker vengono distinti in base al colore di un ipotetico cappello: i white, i gray e i black hat. I primi si limitano a violare la sicurezza dei sistemi senza scopi dolosi, avvertendo spesso gli amministratori di sistema delle vulnerabilità presenti nella rete o nel computer dove si sono introdotti; i secondi si comportano in modo diverso a seconda della situazione, mentre gli ultimi hanno sempre intenti dolosi. Gli hacker black hat sono più comunemente noti come cracker.

**Hoax, Internet hoax** in genere, con questo termine si indica un messaggio di posta elettronica che diffonde notizie false su presunti virus dagli effetti devastanti, raccomandando di inviare tale allarme al maggior numero di persone possibili.

## I

**Ingegneria sociale (social engineering)** tecnica di persuasione che mira a carpire informazioni riservate o a forzare i soggetti a compiere certe azioni attraverso l'uso di calcolate pressioni psicologiche. Gli hacker usano spesso questa tecnica quando sono intenti alla violazione di un sistema, sfruttando la propensione delle persone a rispondere a domande dirette e impreviste o ad aiutare qualcuno che sembra in difficoltà.

**In the wild** frase usata per designare dei virus particolarmente diffusi.

## J

**Joke** innocuo programma scherzo che in genere si limita a simulare il payload di un qualche tipo di malware, come la formattazione di un disco o la caduta di lettere sullo schermo.

## K

## L

## M

**Malware** contrazione della frase malicious software (software dannoso). Indica genericamente tutti i tipi di software concepiti volutamente per arrecare danni: virus, cavalli di troia e worm.

**Macro virus** virus che infetta le macro usate da alcuni tipi di file e applicazioni (ad es. i documenti e i modelli di Microsoft Office) per automatizzare l'esecuzione di un certo numero di compiti. I macro virus, in genere scritti in linguaggio Visual Basic for Applications o in WordBasic, sono anch'essi costituiti da macro

**MBR/Master Boot Record** Master Boot Sector di un disco. E' situato sul primo settore di un disco rigido fisico. Il MBR contiene istruzioni e dati che descrivono le partizioni del disco.

**Multipartito** virus concepito per infettare sia i file che i settori di sistema.

## N

**Netstrike** particolare tipo di attacco DDoS, in genere portato come forma di protesta sociale e caratterizzato dal fatto che i potenziali partecipanti vengono pubblicamente avvisati della data in cui si svolgerà l'attacco e invitati a contribuire. Ad esempio, il sito web di Fineco è stato oggetto di un attacco Netstrike.

## O

**Overflow di un buffer** è uno specifico tipo di bug che affligge il software. Si verifica quando un'area di memoria non è dimensionata a sufficienza per ospitare la quantità di dati immessa. Un buffer overflow può provocare un crash, lasciare il sistema in uno stato vulnerabile o essere sfruttato da un hacker per violare la sicurezza di un computer.

## P

**Pacchetto** unità di dati che viaggiano sulle reti di computer.

**Payload** effetto, in genere più o meno distruttivo per i dati, contenuto all'interno del malware.

**Phracker** individuo che usa e combina tecniche di hacking informatico con il phreaking telefonico.

**Phreaker** persona esperta nel funzionamento dei sistemi telefonici, che tenta di violarne la loro sicurezza, in genere allo scopo di assicurarsi telefonate internazionali a costo zero.

**Polimorfo** virus che impiega particolari tecniche per cambiare continuamente alcune parti del suo codice al fine di rendere molto difficile la sua individuazione da parte degli antivirus. I virus polimorfi cifrano gran parte del proprio codice attraverso un algoritmo che produce risultati sempre diversi e mutano di continuo la parte in codice rimasta in chiaro, cioè le istruzioni che hanno il compito di decifrare il corpo principale del virus e subito dopo di cedergli il controllo.

## Q

## R

**Residente in memoria (virus)** virus che rimane attivo nella memoria del sistema, monitorando alcune funzioni che gli permettono di infettare file e/o settori e di attuare contromisure stealth.

**Retrovirus** virus che attacca esplicitamente uno o più antivirus, tentando di neutralizzarli.

**Rootkit** termine con cui si designa genericamente un pacchetto costituito da più programmi, che permettono varie funzioni di hacking: intercettazione del traffico di rete (sniffer), possibilità di installare una backdoor sul sistema, manipolazione dei file di rapporto e di auditing sul computer compromesso al fine di nascondere le tracce di un'intrusione. Il rootkit è disponibile per un'ampia gamma di sistemi operativi.

## S

**Sniffer** programma che in genere viene installato su una rete di computer al fine di intercettarne il traffico e di consentirne l'analisi da parte dell'hacker che lo ha installato. L'analisi dei pacchetti di rete permette di scoprire password che viaggiano in chiaro (cioè non in forma cifrata) e di raccogliere numerose informazioni sulla rete monitorata dallo sniffer.

**Script virus** virus scritto usando un linguaggio di tipo script, non compilato ma interpretato, come il Visual Basic Script per Windows Scripting Host.

**Stealth virus** un virus che sfrutta una serie di tecniche atte a eludere il controllo degli antivirus, in particolar modo dei behavior blocker. Ad esempio, un virus stealth può tentare di infettare un file senza farne aumentare la lunghezza, oppure può usare tecniche di tunneling per accedere direttamente ad alcune funzioni di sistema che interagiscono con il file system (gestori di interrupt e driver), scavalcando così eventuali schermature antivirus.

## T

**Trojan** vedi **Cavallo di troia**

**Tunneling** tecnica usata dagli autori di virus per scavalcare il controllo e la schermatura dei behavior blocker.

## U

## V

**Virus** termine con cui si designano dei programmi software in grado di replicarsi senza autorizzazione da parte dell'utente. L'origine del termine sembra debba essere attribuita a Len Adleman, collega di Fred Cohen, uno dei pionieri nel campo della ricerca antivirus. I virus vengono classificati in base agli oggetti infettati e alle tecniche di infezione.

## W

**Worm** particolare tipo di virus che si diffonde in reti di computer. Nel 2001, sono comparsi i primi worm per Windows in grado di propagarsi senza fare uso di file, transitando esclusivamente nella memoria volatile dei computer (CodeRed, CodeBlue e CodeGreen).

## X

## Y

## Z

**Zombie** computer compromesso da un malintenzionato che, dopo averne violato la sicurezza, possiede un accesso non autorizzato al sistema ed è in grado di pilotarne le funzioni da una postazione remota (ad esempio usando una backdoor).

**Zoo virus** un virus informatico che si trova soltanto nei laboratori di ricerca e che per vari motivi non si è diffuso tra i normali utenti di computer.

## 8 Appunti:

---

Pagina bianca

## 9 Indice

---

Pagina volutamente bianca