

Aggiornamenti di Windows

Microsoft Update è un servizio in linea che consente di scaricare aggiornamenti gratuiti per il software Microsoft. Continuate a leggere per imparare a scaricare gli aggiornamenti gratuiti da Microsoft Update. Troverete inoltre informazioni su Aggiornamenti automatici di Windows, ovvero una funzione che scarica automaticamente gli aggiornamenti disponibili. Quali sono gli scopi di Microsoft Update?

Microsoft Update è una sezione in linea del sito Web Microsoft che fornisce gli ultimi aggiornamenti per Microsoft Windows, Internet Explorer e per altri programmi software Microsoft. Controllate periodicamente la sezione Microsoft Update e attenetevi alle indicazioni riportate di seguito per tenere aggiornato e protetto il vostro computer.

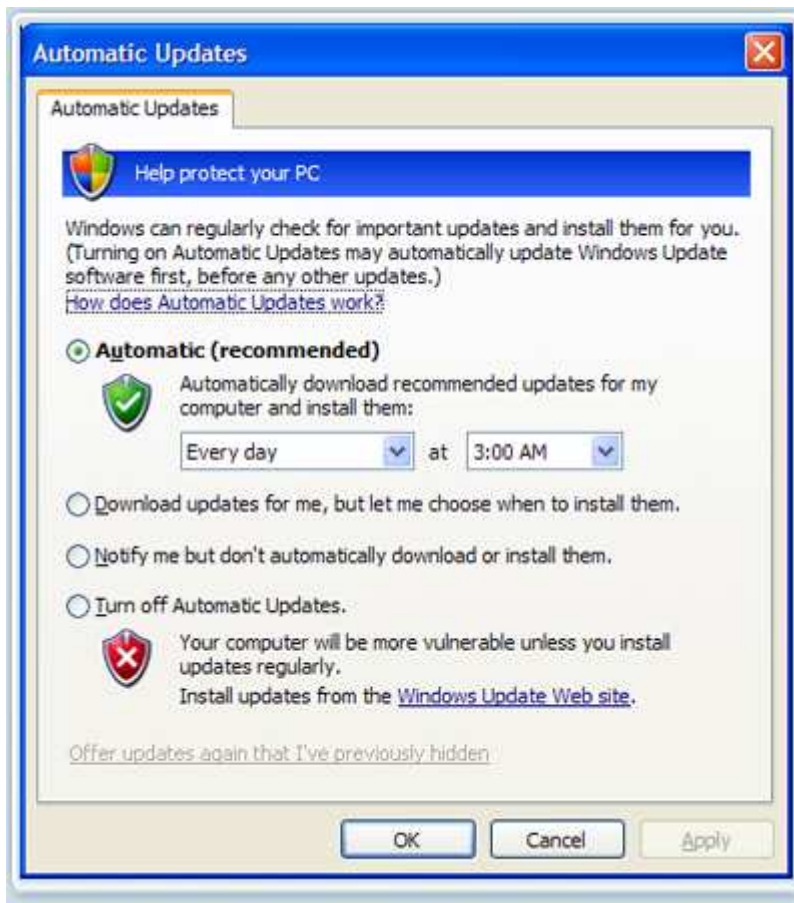
1. Dopo aver eseguito la connessione a Internet, fate clic su Start. Scegliete Tutti i programmi e fate clic su Microsoft Update. Se state utilizzando una vecchia versione di Windows, questa procedura potrebbe essere leggermente differente oppure il servizio [Microsoft Update](#) potrebbe non essere disponibile.
2. È possibile utilizzare Microsoft Update per scaricare aggiornamenti critici alla protezione e aggiornamenti facoltativi non importanti come quelli critici.
Se avete molta fretta, fate clic su Installazione rapida (consigliata).
Se siete interessati a tutti gli aggiornamenti disponibili (inclusi quelli critici e quelli alla protezione), fate clic su Installazione personalizzata.
Nota: se non avete eseguito Microsoft Update da molto tempo, è possibile che venga richiesto di scaricare la versione più recente.
3. Microsoft Update esegue l'analisi del computer e fornisce un elenco degli aggiornamenti consigliati. Questo è valido solo per alcuni prodotti Microsoft. Durante questo processo Microsoft non raccoglie informazioni che possono essere utilizzate per identificare l'utente.
Suggerimento: Per gli aggiornamenti relativi a Microsoft Word, Excel, PowerPoint e per altri programmi Office, utilizzate [Office Update](#).
4. Scorrete l'elenco degli aggiornamenti e fate clic sulla casella relativa all'aggiornamento da installare. Se avete selezionato l'opzione Installazione personalizzata, potete sempre includere tutti gli aggiornamenti critici. Per una descrizione completa di ciascuna voce, fate clic su Ulteriori informazioni.
5. Dopo aver selezionato tutti gli aggiornamenti desiderati, fate clic su Vai all'installazione degli aggiornamenti, quindi su Installa.

Come attivare Aggiornamenti automatici di Windows

Se non visitate Microsoft Update con regolarità, potete scaricare gli aggiornamenti automatici da Microsoft, in tal modo non dovete ricordarvi di controllare la presenza di aggiornamenti critici per mantenere aggiornato e protetto il vostro computer. Se disponete di Windows XP Service Pack 2 (SP2), probabilmente la funzione Aggiornamenti automatici è già attiva. Potete controllare il sito Web [Microsoft Update](#).

Nota: Microsoft non offre il servizio Aggiornamenti automatici per Windows 95, Windows 98 o Windows NT.

1.
 1. Click **Start**, e poi click **Pannello di controllo**.
 2. Click **Aggiornamenti automatici**.
 3. Scegli **Automatic (recommended)**.



2. Ogni volta che è disponibile un nuovo aggiornamento, viene visualizzato un fumetto nell'angolo inferiore destro dello schermo.

Fate clic sul fumetto per avviare il processo di installazione degli aggiornamenti critici che consentono di proteggere il computer dai virus.



Proteggi il tuo PC: altre operazioni possibili

Microsoft Update o Aggiornamenti automatici di Windows rappresentano la prima linea di difesa per i problemi legati alla protezione del computer. È possibile continuare a migliorare la protezione del computer utilizzando un firewall e mantenendo attivo l'abbonamento a un software antivirus.

Gli antivirus

Parti che compongono l'antivirus

Con il termine antivirus in realtà si intendono più parti differenti, alcune indipendenti tra di loro: il file (o i file) delle firme: file che contiene tutte le firme dei virus conosciuti. Questa parte è fondamentale ed essenziale per il funzionamento corretto di qualsiasi altro componente il binario in grado di ricercare il virus all'interno dell'elaboratore. Questo componente è l'antivirus vero e proprio

il binario che rimane residente e richiama l'antivirus ogni qual volta viene creato/modificato un nuovo file o viene modificata una zona di memoria per controllare che il computer non sia stato infettato con questa operazione

il binario che effettua gli update del file delle firme e di tutti i binari dell'antivirus

Nota: alcuni software antivirus possono essere sprovvisti di una o di entrambe le parti 3 e 4

Limiti di un antivirus

Bisogna ricordare che l'antivirus è in grado di eliminare prima di tutto soltanto i virus che riconosce, quindi tutti i nuovi virus (per nuovi si intende sia virus che il proprio antivirus non conosce che quelli che non sono ancora stati scoperti) possono passare completamente inosservati e fare tutto quello che vogliono senza che l'antivirus intervenga. Inoltre l'antivirus riesce ad intercettare il virus soltanto quando questo è entrato all'interno del computer e quindi ha già infettato un file o la memoria; a questo punto, a seconda del virus, può "disinfettare" il file o la memoria eliminando completamente il virus o in alcuni casi è costretto a mettere in "quarantena" il file contagiato ed a eliminarlo per l'impossibilità di recuperare il file originario.

L'antivirus inoltre è un grande utilizzatore delle risorse del computer e se viene [avviato in background](#) ogni volta che viene acceso il computer può comportare un forte rallentamento soprattutto nelle fasi iniziali (perché controlla prima tutta la memoria e poi tutti i file, che rientrano nella ricerca selezionata durante la fase configurazione, su disco); tale rallentamento è presente anche in tutte le fasi in cui si scrive su disco anche se qui può risultare più trascurabile. Per questi motivi l'antivirus affretta l'obsolescenza del proprio computer creando la necessità di aggiornarne alcune parti o prenderne uno nuovo per ottenere delle prestazioni che siano accettabili per l'utente.

Occorre aggiornare continuamente l'antivirus per evitare che virus già riconosciuti dall'antivirus che si è scelto possano infettare il proprio PC. La scelta di un antivirus è una cosa molto complessa anche perché antivirus diversi possono riuscire a rintracciare e quindi a controllare i nuovi virus prima di altri.

La scoperta di un nuovo virus dipende molto da quanto è "infettivo", più un virus si propaga velocemente e più veloce e semplice è individuarlo e quindi aggiornare le firme; se invece il virus tende ad essere molto poco "infettivo" e tende a rimanere localizzato soltanto in una certa area può passare un tempo relativamente lungo prima che venga intercettato e aggiunto alle firme.

È successo più volte che un antivirus considerasse dei file o programmi come virali anche se in realtà non lo erano. Questo è dovuto al fatto che un insieme di istruzioni (od una sua piccola variante) che compongono un virus (od una sua parte) può essere presente anche in programmi e file "normali" o possono essere ottenuti come combinazione casuale in un file di dati salvati non in formato testo. Il problema principale è che si può non riuscire ad eseguire questo programma od aprire il file rilevato come infetto se prima non si disabilita l'antivirus, sempre che l'antivirus non lo abbia cancellato o rovinato in modo irreparabile nel frattempo.

Ci sono numerosi metodi per criptare e compattare codice malevolo rendendolo così non rintracciabile da un antivirus; su questo fronte molti antivirus non sono attrezzati e riescono a fare ben poco, ma anche gli altri possono non essere in grado di rilevare un file infetto se non quando questo entra in esecuzione: il virus viene scompattato in RAM per essere eseguito e solo in questo momento l'antivirus sarà in grado di rintracciarlo.

Infine le compagnie che creano i software antivirus possono avere un incentivo finanziario molto forte a far sì che nuovi virus vengano creati continuamente e che il panico nel pubblico generi un continuo ricorso all'aggiornamento dei loro software. Questa è uno delle accuse che da varie parti vengono rivolte ai produttori di antivirus, anche se in realtà non vi è attualmente nessuna prova che convalidi tale tesi.

Il Firewall

Il firewall: ulteriore protezione contro i virus

Per quello che si è detto si capisce che per avere un sistema sicuro l'antivirus non è affatto sufficiente, occorre una protezione ulteriore: il [firewall](#). Un firewall permette, se ben configurato ed usato correttamente, di bloccare i virus, anche se non conosciuti, prima che questi entrino all'interno del proprio computer e volendo permette anche di bloccare all'interno alcuni virus presenti nel proprio computer evitando così di infettare la rete a cui ci si è collegati. Un firewall quindi può essere uno strumento aggiuntivo che impedisce ad un virus di infettare la macchina prima che possa essere individuato dall'antivirus (con la possibile perdita del file infetto) ed inoltre permette di nascondere parzialmente o totalmente la macchina sulla rete evitando attacchi dei [cracker](#) o degli stessi virus.

Antivirus e sistemi operativi

Con l'avvento di [internet](#) l'antivirus è diventato uno strumento quasi indispensabile per i sistemi operativi rilasciati da [Microsoft](#), mentre altri sistemi risultano quasi immuni da virus; per questo motivo la maggior parte degli antivirus è realizzata per questo sistema operativo. Negli ultimi anni sono stati prodotti antivirus anche per altri sistemi, di solito usati come [server](#), per poter controllare il flusso di dati, soprattutto [e-mail](#), che poi finiranno sui computer desktop degli utenti che usano prodotti Microsoft.

La causa di una così alta diffusione dei virus su questa piattaforma è dovuta principalmente alla sua diffusione, sia per la più facile proliferazione, sia perché chi vuole creare un virus tende a farlo per il sistema operativo più diffuso. Inoltre alcuni sistemi operativi non Microsoft sono visti dalla maggior parte degli utenti come più difficili da usare e quindi tendono ad essere usati da utenti più esperti con maggiore dimestichezza nell'affrontare i possibili problemi.

È vero che sui sistemi operativi derivati da UNIX, come Linux o Mac OS, la diffusione dei virus è in linea teorica molto più ostacolata soprattutto dalla gestione delle utenze che tende a far eseguire programmi da utenti con pochi privilegi, limitando dunque i danni che potrebbero scaturire dall'esecuzione di un codice malevolo; risulta quindi molto più difficile che questa operazione causi una compromissione del sistema operativo come invece accade spesso nei sistemi Microsoft.

Antivirus e programmi

I programmi che maggiormente permettono la diffusione dei virus sono i [client di posta](#) elettronica ed i [browser](#), questo perché questi due programmi sono l'accesso diretto a due funzionalità indispensabili in internet: la posta e la navigazione. Un'altra tipologia di software informatico molto colpito dai virus è quella composta dai file di dati ricavati con [Microsoft Office](#). In questa suite è possibile creare all'interno dei file delle istruzioni ([macro](#)) che eseguono date funzionalità in modo automatico o sulla pressione di una determinata combinazione di tasti. Molti [virus writer](#) sfruttano questa "potenzialità" per allegare delle macro che sono in realtà dei virus.

In generale i virus sfruttano delle vulnerabilità nei sistemi informatici, usando a volte - in modo automatico - tecniche di penetrazione sviluppate dai cracker. Diverse organizzazioni, oltre ai produttori di software antivirus, si occupano di raccogliere le segnalazioni di vulnerabilità o attacchi, e renderle pubblicamente disponibili; tali organizzazioni sono normalmente note con l'acronimo di [CERT](#) ("Computer Emergency Response Team", squadra di risposta alle emergenze informatiche).

I Browser

Anche i browser possono essere un veicolo per l'infezione, basta che vi sia un buco sfruttato da un sito WEB che si visita. Come per i clienti di posta si ha che su tutti i sistemi operativi di [Microsoft](#) l'utente si trova installato [internet explorer](#) e, anche a causa della sua diffusione, risulta proprio questo browser il più soggetto a questi tipi di attacchi, tanto che ultimamente è stato consigliato da più fonti di usare altri browser soprattutto se si fanno delle transazioni a rischio (per esempio se si accede al proprio conto corrente).

I Trojan

Un trojan o trojan horse (dall'[inglese](#) per [Cavallo di Troia](#)), è un tipo di [malware](#). Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un [programma](#) apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice *trojan* nascosto.

L'attribuzione del termine "Cavallo di Troia" ad un programma o, comunque, ad un file eseguibile, è dovuta al fatto che esso nasconde il suo vero fine. È proprio il celare le sue reali "intenzioni" che lo rende un trojan.

In genere col termine Trojan ci si riferisce ai trojan ad accesso remoto (detti anche RAT dall'inglese *Remote Administration Tool*), composti generalmente da 2 file: il file server, che viene installato nella macchina vittima, ed un file client, usato dall'attaccante per inviare istruzioni che il server esegue. In questo modo, come con il [mitico](#) stratagemma adottato da [Ulisse](#), la vittima è indotta a far entrare il programma nella città, ossia, fuor di metafora, ad eseguire il programma. Esistono anche alcuni software legali, come GoToMyPC o PCAnywhere, con funzionalità simili ai *trojan*, ma che non sono dei cavalli di Troia poiché l'utente è consapevole della situazione.

I trojan non si diffondono autonomamente come i [virus](#) o i [worm](#), quindi richiedono un intervento diretto dell'aggressore per far giungere l'eseguibile maligno alla vittima. Spesso è la vittima stessa a ricercare e scaricare un trojan sul proprio [computer](#), dato che i [cracker](#) amano inserire queste "trappole" ad esempio nei [videogiochi](#) piratati, che in genere sono molto richiesti. Vengono in genere riconosciuti da un antivirus aggiornato come tutti i malware. Se il trojan in questione non è ancora stato scoperto dalle software house degli antivirus, è possibile che esso venga rilevato, con la scansione euristica, come probabile malware.

Un trojan può contenere qualsiasi tipo di istruzione maligna. Spesso i trojan sono usati come veicolo alternativo ai [worm](#) e ai [virus](#) per installare delle [backdoor](#) o dei [keylogger](#) sui sistemi bersaglio.

All'incirca negli anni successivi al 2001 o 2002 i *trojan* incominciarono ad essere utilizzati sistematicamente per operazioni criminose; in particolare per inviare messaggi di [spam](#) e per rubare informazioni personali quali numeri di carte di credito e di altri documenti o anche solo indirizzi email.

I peer to peer

Il p2p (o meglio il Peer to Peer che in italiano è "da pari a pari") è uno strumento di scambio file basato su semplicissimo sistema, di seguito spiegato

Una volta installato il programma di file-sharing, inviamo una richiesta, ma a differenza di ciò che accade in un sito internet, nel quale noi client inviamo una richiesta ad un [server](#), nel file-sharing siamo contemporaneamente sia client che server, quando scarichiamo file dalla rete siamo client, mentre quando qualcuno scarica da noi, siamo server, questo sistema risulta essere molto più stabile, e fornisce una quantità superiore di file disponibili

Il primo programma di file-sharing fu Napster, che però aveva un punto debole, infatti Napster si basava su un server centrale al quale noi client inviavamo una nostra richiesta, quest'ultimo ci rimandava indietro una lista degli utenti che possedevano la nostra richiesta, ma se il server centrale per qualche motivo veniva chiuso o si impallava tutto il sistema diventava inutilizzabile. Le case discografiche intrapresero la via legale e obbligarono Napster a chiudere, ma ormai il sistema era stato appreso, e già erano nati nuovi e più efficienti programmi di file-sharing, i quali non si basavano più su un server centrale, ma su un nuovo sistema, quello in cui siamo allo stesso tempo sia client che server

I programmi di peer to peer più diffusi sono:

Overnet e eDonkey: questi due programmi usano suppergiù la stessa metodologia di scambio, infatti si collegano sia alla rete Overnet che a quella Edonkey/Emule, offrendo la possibilità di scaricare da entrambe.

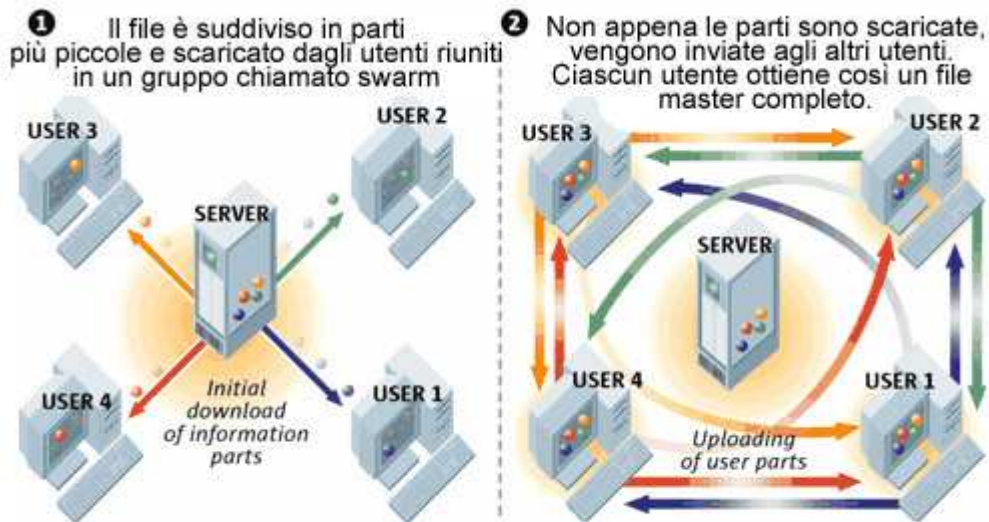
Il vantaggio rispetto ad eMule è che la velocità di download è immediatamente elevata, infatti eMule raggiunge la velocità di download ottimale dopo qualche ora
Lo svantaggio nei confronti di eMule sono svariati, ma quello principale è: che il Mulo è Open-source (questo significa che qualsiasi utente può lavorare sul Mulo per migliorarne il codice originale, e inoltre può creare e distribuire nuovi software derivati dal codice originale)

eMule: è il successore di eDonkey, ma ne migliora alcune caratteristiche: introduce l'aggiornamento automatico dei server, con la possibilità sempre di inserirli anche manualmente, la facilità nel trovare files rari, e infine ma non per questo meno importante, e l'ottimizzazione del rapporto upload/download, questo è possibile grazie ai crediti (il sistema crediti è una caratteristica importante, perché l'utente "x" acquista crediti permettendo ad altri utenti "y" "z" l'upload da esso, così facendo i crediti di "x" aumentano, ed eMule grazie a un sistema di calcolo automatico fa salire nella coda l'utente "x", questo spinge gli utenti a condividere il maggior numero di file per acquistare crediti, con conseguente beneficio per tutta la community). La fregatura (se così si può chiamare) è che gli utenti che hanno una connessione lenta sono decisamente svantaggiati, e non avranno mai il punteggio di un utente che ha una connessione a banda larga (adsl, fibra ottica etc.).

Cosa è un torrent

BitTorrent: non è un vero e proprio programma di file-sharing, infatti in quest'ultimo non troverete il pulsante cerca, come in tutti i programmi di peer to peer, e proprio per questo che risulta più complicato rispetto ai concorrenti.

Per trovare un determinato file, non si effettua una ricerca sul programma, ma prima bisogna trovare e scaricare un file con estensione .torrent (il peso massimo del file deve essere di 2 KB) il quale contiene tutte le informazioni relative al file che vogliamo scaricare. Una volta fatto trovato il file, lo avviamo facendo doppio click su questo, ed è proprio adesso che BitTorrent inizierà il



Fonte: Bit-torrent

download del file.

Il vantaggio di questo programma è che le code sono pressoché inesistenti, e per questo risulta almeno al momento il p2p di file-sharing più veloce in assoluto (questo perché BitTorrent è stato creato proprio per sfruttare al massimo tutta la banda disponibile).

BitTorrent è attualmente considerato il nemico numero uno dalle major cinematografiche, ed il motivo è essenzialmente dovuto alla sua architettura in grado di permettere velocità maggiori rispetto alle altre reti p2p.

Senza mai dimenticare che colpevolizzare uno strumento per l'utilizzo errato che ne si fa è sempre un errore, e puntualizzando che attraverso le reti bit-torrent viene distribuito anche materiale legalissimo, ad esempio molte distribuzioni linux, vediamo di capire meglio come funziona una rete bit-torrent.

Tante reti su misura

A ogni scaricamento viene creata una rete dedicata, con il compito di distribuire i dati di quello specifico download; la vita di questa rete è limitata solo a questo, dopodiché assolto questo compito, essa viene dismessa; a differenza di altre reti peer to peer, i partecipanti si concentrano solamente su pochi download, privilegiando se vogliamo l'aspetto qualitativo a quello quantitativo.

Il Tracker

In ogni rete torrent c'è un programma chiamato tracker che inizializza la rete e che funge da server di distribuzione delle informazioni per tutti i computer che si collegano. Ogni computer per partecipare alla rete deve quindi collegarsi al tracker: per questo deve servirsi di un file torrent, che contiene non solo l'indirizzo Internet del tracker ma anche informazioni sui file che compongono la distribuzione, sulla loro lunghezza e una serie di meccanismi di checksum.

Il tracker è quindi il cuore del torrent e non è un caso che i siti che distribuiscono file torrent siano così avversati dalle major; di fatto bloccando il tracker, il torrent non "decolla"; nel tracker sono indicati in quanti blocchi sono suddivisi i dati e la loro dimensione (256 kb/2 Mb); questi blocchi vengono suddivisi e inviati come singoli pacchetti di dati da 16 kb.

Quando il pc dispone del file torrent può dunque entrare in contatto con il tracker e diventa un nodo (peer) registrato nella rete ad hoc; per questo motivo trasmette al tracker un identificativo di 20 byte autogenerato (chiamato peer-id), lo identifica univocamente nella rete.

I seeders

I seeder sono i nodi che offrono il download completo, mentre i leecher sono quelli che offrono solo download parziali; queste informazioni vengono veicolate a ciascun nodo dal tracker che invia anche un elenco di 50 peer-id a cui potersi collegare.

Ovviato a questo compito di starter, il tracker non è più necessario, la rete dedicata è costituita e comincia a funzionare, in quanto con l'upload e il download dei pacchetti di dati i peer scambiano i file solamente tra di loro.

Ogni nuovo peer interroga gli altri nodi per sapere se gli è permesso scaricare qualcosa; dopo una prima fase, chiamata handshake, avviene poi lo scambio di un bitfield, ossia le informazioni su quali blocchi ciascun nodo ha già scaricato. Tramite il bitfield il peer può gradualmente rendersi conto di quali blocchi siano facili da reperire nella rete e quali siano invece poco distribuiti. Queste informazioni vengono elaborate per scaricare inizialmente i blocchi meno richiesti, in modo da minimizzare il rischio di formare colli d'i bottiglia in rete. L'unica eccezione a questa regola è il primo download di un peer: in quel caso ogni nodo richiede un blocco qualsiasi, per poter a sua volta mettere a disposizione qualche dato verso gli altri nodi della rete.

Il singolo nodo cerca di scaricare da quanti più peer gli riesce ma anche di fornire dati solo ai peer che offrono un'alta velocità di download. Questo significa che i nodi veloci vengono preferiti, a scapito di quelli lenti scartati (chocking).

Con questo meccanismo premiante per i più performanti, chi offre pochi upload, entro breve tempo non riceverà più alcun download. Il chocking funziona unilateralmente, ossia il partecipante cerca di fare in modo che il peer lento non riceva più da lui alcun download. Può però scaricare da quel peer.

Per l'upload ciascun nodo nella configurazione base dispone di quattro posti liberi per connessioni "unchocked". Per non dover effettuare continuamente chocking e unchocking, ogni dieci secondi dev'essere ricevuto un nuovo peer, bloccandone uno precedente.

I peer migliori

Ciascun nodo tuttavia non si affida soltanto ai collegamenti noti ma cerca di trovare connessioni nuove e migliori; per questo dispone di un unchocking: ogni 30 secondi si fida ed apre una connessione di upload a un nuovo peer; se le velocità di upload e download sono adatte, il collegamento viene mantenuto, altrimenti si passa al successivo. C'è anche un'altra forma di unchocking: se un partecipante non riceve per un minuto alcun blocco da un altro peer, ne deduce che questo lo ha bloccato; in questo caso passa quindi all'anti-snobbing, ossia elimina quel peer ed effettua un nuovo unchocking ottimistico separato nel posto reso libero, aumentando la velocità di download.

Nero

I formati standard per la creazione di CD gestiti da Nero Burning Rom sono:



CD DATI ISO9660

Con questo formato possono essere scritti CD-ROM contenenti dati, leggibili da parecchi sistemi operativi; l'unica limitazione potrebbe essere rappresentata dalla lunghezza dei nomi assegnati ai file.



CD DATI Joliet

Con questo formato possono essere scritti CD-ROM contenenti dati con nomi di file più lunghi rispetto all'ISO9660. In generale, però, un CD in questo formato non è leggibile sui sistemi Unix e Apple.



CD Audio

I CD in questo formato contengono soltanto dati audio; possono essere ascoltati da tutti i lettori CD audio disponibili in commercio, e con un programma adeguato, anche sui computer.

N.B. Nella creazione di un CD audio, ricorda che soltanto pochi lettori CD presenti sul mercato supportano la lettura di CD riscrivibili, pertanto per una sicura compatibilità usa CD-R.

Nero supporta vari formati audio:

- **File WAVE** (con estensione .wav)

I file Audio sono salvati sul disco rigido nel formato wave. Questo formato è parte dello standard generale RIFF (Resource Interchange File Format). Questo formato supporta varie frequenze di campionamento e risoluzioni.

- **File CD-DA** (con estensione .cda)

Il primo standard del CD è il CD audio ed è conosciuto come CD-DA (CD Digital Audio). Un CD audio comprende varie tracce, dove di solito ogni traccia corrisponde ad una canzone. Ogni traccia è a sua volta suddivisa in settori. I CD musicali di solito fanno parte di questa categoria.

- **File MP3** (con estensione .mp3)

Il formato audio MPEG3 è diventato di recente il formato più utilizzato per trasferire dati audio attraverso Internet. MP3 sta per MPEG-1 Audio Layer 3. Utilizzando l'MP3, le dimensioni dei file audio vengono ridotte notevolmente (fattore 1 a 10), senza perdita di qualità.

- **File TwinVQ** (con estensione .vqf)

Il formato TwinVQ è simile al formato MP3. Si distingue per il maggior grado di compressione. Di solito, i file sono più piccoli del 30% rispetto agli MP3, ma con la stessa qualità.



CD Mixed-Mode

Questo formato comprende una traccia dati, seguita da varie tracce audio.



CD Extra/Enhanced Music-CD

Il CD Extra è il più recente standard per i CD audio con componenti multimediali.

Un CD in questo formato contiene sempre due sessioni:

La prima contiene soltanto tracce audio, che possono essere ascoltate con un lettore CD, mentre la seconda contiene dati leggibili dai computer, in qualsiasi formato.



Copia CD

Selezionando questo formato verrà creato un cd copia dell'originale

Video CD

Basato su un file system ISO, questo formato permette di creare CD contenenti film in formato digitale. I Video CD possono essere riprodotti con speciali lettori o con appositi programmi dai computer stessi.

N.B. Un Video-CD non deve essere scritto con il sistema Joliet, poichè i file MPEG devono essere contrassegnati come mode 2, form 2 per poter poi essere leggibili. Questo non può essere fatto con la struttura delle directory [Joliet](#) ma solo con la struttura [ISO9660](#), in caso contrario Windows non troverà le informazioni necessarie.



Super Video CD

Questo formato permette la creazione di Super Video CD, con dati sorgente codificati in MPEG-2 e parametrici adatti per i Super Video CD. Per creare Super Video CD si deve utilizzare un encoder, che deve comprendere le opzioni necessarie



CD-ROM Boot

Un CD-ROM Boot contiene caricato all'interno il sistema operativo, infatti è composto da una traccia d'avvio ed una ISO 9660. Speciali CD bootable devono essere creati per poter avviare il computer da CD.



CD Ibrido

Un CD ibrido contiene dati nei formati HFS e ISO9660. Se il CD viene inserito in un Macintosh, verranno visualizzati solo i dati HFS, mentre in un PC verranno mostrati soltanto i dati ISO.



CD-ROM UDF

L'UDF è stato creato per sfruttare appieno le potenzialità dei CD-RW e dei DVD. Esso è ottimizzato per gestire enormi quantità di dati e per minimizzare le modifiche nel caso in cui sia necessario aggiungere o eliminare alcuni file.

Il file system UDF può essere scritto e letto senza alcun driver speciale da Windows 98 e Windows 2000. Da

ricordare, tuttavia, che Nero non supporta la multisessione per i CD UDF, per cui bisogna utilizzare necessariamente dei CD-R vergini.



CD-ROM UDF/ISO

In questo formato Nero è in grado di creare un CD contenente sia dati ISO 9660 che UDF. Da ricordare che attualmente Nero non supporta i CD UDF multi-sessione, per cui le sessioni UDF o UDF Bridge devono essere scritte su un CD vergine.



CD-ROM HFS

In questo formato Nero è in grado di creare un CD contenente dati in HFS, file system leggibile dai computer Apple Macintosh.

Per creare un CD HFS è necessario connettere al PC un disco rigido SCSI che contenga una o più partizioni HFS. Queste partizioni HFS possono essere create o modificate soltanto da un computer Apple Macintosh. Ricordatevi, inoltre, che il disco rigido SCSI deve essere connesso al PC prima di accendere il PC, altrimenti Nero non potrà trovare nessuna partizione HFS.

Track-At-Once

Con questo metodo, ogni traccia viene scritta singolarmente sul CD e l'operazione di scrittura viene, quindi, brevemente interrotta dopo ogni traccia. Questo vuol dire che un CD-R o un CD-RW può essere scritto come un normale disco.

| | |
|---------------------|-------------------------------|
| Metodo di Scrittura | Track-At-Once |
| Numero di Copie | Track-At-Once Disc-At-Once |

Disc-At-Once

Con questo metodo, tutte le tracce vengono scritte in una sola operazione sul CD, senza spegnere mai il laser.

| | |
|---------------------|-------------------------------|
| Metodo di Scrittura | Track-At-Once |
| Numero di Copie | Track-At-Once Disc-At-Once |

Copia Immagine

Con questo metodo Nero legge i file da scrivere sul CD e li salva in un file immagine sul disco rigido per eliminare gli errori di copia. Errori che possono essere causati da un disco rigido lento o un lettore CD/DVD lento o dal fatto che i file nascosti non vengono salvati. Il metodo copia immagine richiede 800 MB di spazio sul disco rigido