bitdefender
free antivirus 2010

Manuale dell'utente

BitDefender Free Antivirus 2010
Manuale dell'utente

Pubblicato 2010.04.22

Avvertimenti Legali


bitdefender

Indice

Accettamento della Licenza per utenti finali

SE NON SI ACCETTANO I TERMINI E LE CONDIZIONI NON INSTALLARE IL SOFTWARE. SELEZIONANDO "ACCETTO", "OK", "CONTINUA", "SI", OPPURE INSTALLANDO O UTILIZZANDO IN OGNI CASO IL SOFTWARE, STATE INDICANDO IL VOSTRO COMPLETO BENESTARE E ACCETTANDO I TERMINI DI QUESTO ACCORDO.

Questi termini ricoprono le Soluzioni e i Servizi BitDefender per gli utilizzatori Home, incluse le documentazioni relative e qualsiasi aggiornamento e rinnovo delle applicazioni rese disponibili dalla licenza installata o qualsiasi servizio in accordo a quanto definito nella documentazione e ogni copia di questa.

Questo accordo di Licenza è un contratto legale tra te (utente finale o individuale o entità singola) e BITDEFENDER, per l'utilizzo dei prodotti Software BITDEFENDER identificati sopra, che include il software e può includere supporti digitali, materiale stampato, e documentazione "online" oppure elettronica (qui di seguito designata come "BitDefender"), tutti protetti dalle leggi degli Stati Uniti ed internazionali sul copyright, e trattati di protezione internazionali. Mediante l'installazione, copia, o qualsiasi uso di BitDefender, accetti di essere vincolato ai termini di questo accordo.

Se non si è d'accordo con i termini che determinano il contratto di utilizzo della licenza, non installare o utilizzare BitDefender.

Licenza BitDefender. BitDefender è protetto da leggi e trattati internazionali su copyright, così come da altre leggi e trattati sulla proprietà intellettuale. BitDefender è autorizzato, non venduto.

CONCESSIONE DI LICENZA. BITDEFENDER concede,solamente all'utente che l'ha acquistata e non a terzi, la presente licenza non esclusiva, limitata e non trasferibile, a utilizzare BitDefender.

APPLICAZIONE DEL SOFTWARE. Si può installare e usare BitDefender, su quanti computers è necessario ma limitatamente al numero totale di utenti autorizzati dalla licenza. E' possibile fare una copia addizionale di back-up.

LICENZA UTENTE DESKTOP. Questa licenza si applica al software BitDefender che può essere installato su un computer singolo e che non fornisce servizi di rete. Ogni utente principale può installare questo software su un computer singolo e può eseguire una copia aggiuntiva per il backup su un dispositivo diverso. Il numero di utenti principali consentito è il numero di utenti della licenza.

PERIODO DI LICENZA. La licenza distribuita sarà considerata in funzione a partire dal giorno di installazione di BitDefender e terminerà alla fine del periodo per il quale la licenza è installata – 1 anno.

AGGIORNAMENTI Se il prodotto BitDefender è presentato come aggiornamento, l'utente deve essere in possesso di una licenza di un prodotto identificato come BITDEFENDER al fine di poter giovare degli aggiornamenti disponibili. Un aggiornamento BitDefender sostituisce e/o integra il prodotto alla base dell'elegibilità

dell'utente per il suddetto aggiornamento. L'utente potrà utilizzare l'aggiornamento solo secondo i termini di utilizzo presenti nell'accordo per la licenza. Se BitDefender è un aggiornamento di un componente di un pacchetto software che l'utente ha in licenza come singolo prodotto, BitDefender potrà essere utilizzato e trasferito solo come parte di quel singolo prodotto, e non potrà essere separato per un numero superiore al totale degli utenti con licenza. I termini e le condizioni di questa licenza sostituiscono e prendono il posto di ogni accordo precedente in corso fra l'utente e BITDEFENDER, per quanto riguarda il prodotto originale o gli aggiornamenti derivati del prodotto.

COPYRIGHT. Tutti i diritti, titoli, e interessi derivati da o verso BitDefender e tutti i diritti di copyright derivati da o verso BitDefender (includendo ma non limitando qualsiasi immagine, fotografia, logo, animazione, video, audio, musica, testo e "applets" incorporati nel BitDefender) il materiale stampato allegato e qualsiasi copia di BitDefender sono proprietà della BITDEFENDER. BitDefender è protetto dalle leggi di copyright e da quanto previsto dai trattati internazionali. Di conseguenza, BitDefender deve essere considerato come qualunque altro materiale protetto da copyright ad eccezione del fatto che è possibile installare BitDefender su un singolo computer conservando l'originale esclusivamente per scopi di backup o archiviazione. Non è permessa la copia o riproduzione del materiale stampato e allegato al prodotto o supporto BitDefender. In tutte le copie create indipendentemente dal supporto o formato in cui vi sia BitDefender, è necessario riprodurre ed includere tutte le note copyright in formato originale. Non è permesso noleggiare a terzi, vendere, dare in leasing, la licenza di BitDefender. Non è permesso smontare, raggruppare, disassemblare, creare lavori derivati, modificare, tradurre né fare alcun tentativo per scoprire, individuare, il codice fonte di BitDefender.

GARANZIA LIMITATA. BITDEFENDER garantisce che il supporto con il quale viene distribuito BitDefender è esente da difetti per un periodo di trenta giorni dalla data in cui viene consegnato. In caso di difettosità riscontrate, BITDEFENDER, a sua discrezione, potrà sostituire il supporto, oppure rimborsare l'importo pagato per l'acquisto, a fronte di una ricevuta. BITDEFENDER non garantisce che BitDefender sarà sempre privo di errori o che gli errori verranno comunque corretti. BITDEFENDER non garantisce che BitDefender soddisferà le necessità dell'utilizzatore.

ECCETTO PER QUANTO CHIARAMENTE SOTTOLINEATO IN QUESTO ACCORDO, ESPRESSAMENTE O IMPLICITAMENTE, RISPETTO AI PRODOTTI, AI MIGLIORAMENTI, ALLA MANUTENZIONE O AL SUPPORTO AD ESSI RELATIVI, O A QUALSIASI ALTRO MATERIALE (TANGIBILE O INTANGIBILE) O SERVIZIO FORNITO DA QUESTI. BITDEFENDER QUI DISCONOSCE ESPRESSAMENTE QUALSIASI GARANZIA E CONDIZIONE IMPLICITA, INCLUSO, SENZA LIMITAZIONE, LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, APPROPRIATEZZA PER UNO SCOPO PARTICOLARE, TITOLO, NON INTERFERENZA, ACCURATEZZA DEI DATI, ACCURATEZZA DEL CONTENUTO INFORMATIVO, INTEGRAZIONE DEL SISTEMA, E NON VIOLAZIONE DEI DIRITTI DI TERZE PARTI ATTRAVERSO IL FILTRO, LA DISABILITAZIONE, O LA RIMOZIONE DI TALE SOFTWARE, SPYWARE, ADWARE, COOKIE, E-MAIL, DOCUMENTI, PUBBLICITÀ

O SIMILI, DI TERZE PARTI, CHE SI ORIGININO DA STATUTO, LEGGE, CORSO DI TRATTATIVE, COSTUMI E PRATICA, O USI DEL COMMERCIO.

DECLINAZIONE DELLE RESPONSABILITA' DI DANNI. Chiunque utilizzi, provi oppure valuti BitDefender, si assume tutto il rischio della qualità e delle prestazioni di BitDefender. In nessun caso BITDEFENDER sarà ritenuta responsabile di qualunque danno di qualsiasi tipo, inclusi senza limitazioni, danni diretti o indiretti derivati dall' utilizzo, o la consegna di BitDefender, anche nel caso in cui BITDEFENDER sia informata dell'esistenza o la possibilità che tali danni possano verificarsi. ALCUNI STATI NON CONSENTONO LA LIMITAZIONE O L' ESCLUSIONE DI RESPONSABILITA' PER DANNI ACCIDENTALI O CONSEGUENTI, IN QUEL CASO LA LIMITAZIONE O ESCLUSIONE SOPRA INDICATA NON POTRA' ESSERE APPLICATA. Le restrizioni e limitazioni fissate saranno applicate indipendentemente dal modo in cui si accetta di usare, valutare o provare BitDefender.

AVVISO IMPORTANTE AGLI UTENTI. AVVISO IMPORTANTE AGLI UTENTI. QUESTO SOFTWARE NON E ESENTE DA EVENTUALI DIFETTI PROVOCATI ANCHE DALL'UTILIZZO DELLO STESSO, E NON E' STATO PROGETTATO NE' DESTINATO ALL'USO IN AMBIENTI PERICOLOSI CHE RICHIEDANO OPERAZIONI O ATTIVITA' IN MANCANZA DI SICUREZZA. QUESTO SOFTWARE NON E' ADATTO ALL'USO IN OPERAZIONI DI NAVIGAZIONE AEREA, NELLE ISTALLAZIONI NUCLEARI, NEI SISTEMI DI COMUNICAZIONE, SISTEMI DI ARMAMENTO, SISTEMI DI RESPIRAZIONE ASSISTITA DIRETTA O INDIRETTA, CONTROLLO DEL TRAFFICO AEREO O QUALUNQUE APPLICAZIONE, ISTALLAZIONE, DOVE L'ERRORE POSSA PROVOCARE MORTE, LESIONI FISICHE GRAVI, O DANNI ALLA PROPRIETA'.

AGGIORNAMENTI: accettando questo accordo, lei riconosce e accetta che il suo sistema sia utlizzato per ricevere e utilizzare aggiornamenti attraverso un protocollo peer to peer. Il protocollo non verrà utilizzato per niente altro che trasmettere e ricevere signature degli aggiornamenti BitDefender.

Accettando questo accordo, lei riconosce e accetta che la tecnologia per la sicurezza scannerizzi il suo traffico al fine di individuare eventuali malware e di prevenire i danni che questi potrebbero produrre.

GENERALE. Questo accordo sarà regolato dalle leggi della Romania e dai regolamenti e trattati internazionali sul diritto d'autore. La giurisdizione esclusiva e la sede di decisione per qualsiasi disputa che sorga al di fuori di questi Termini di Licenza sarà in capo ai tribunali della Romania.

La licenza per l'utilizzo del prodotto BitDefender è soggetta a cambiamenti senza necessità di avvisi prioritari nei confronti dell'utente.

Nel caso di invalidità di qualsiasi previsione di questo Accordo, l'invalidità non avrà effetto sulla validità delle porzioni residue di questo Accordo.

BitDefender e i loghi BitDefender sono marchi registrati di BITDEFENDER. Tutti gli altri marchi registrati utilizzati nel prodotto o nei materiali associati sono di proprietà dei rispettivi titolari.

La licenza terminerà immediatamente senza notifica se si infrange uno qualsiasi dei suoi termini e condizioni. Non si ha diritto ad alcun rimborso da BITDEFENDER o da qualsiasi rivenditore di BitDefender come risultato della cessazione. I termini e le condizioni che riguardano la riservatezza e le restrizioni d'uso resteranno in vigore anche dopo qualsiasi cessazione.

BITDEFENDER può revisionare questi Termini in qualsiasi momento e i termini revisionati si applicheranno automaticamente alle versioni corrispondenti del Software distribuito con i termini revisionati. Se qualsiasi parte di questi Termini è giudicata nulla o non applicabile, ciò non avrà effetto sulla validità del resto dei Termini, che resteranno validi ed applicabili.

In caso di controversia o inconsistenza tra le traduzioni di questi Termini nelle altre lingue, prevarrà la versione inglese emessa da BITDEFENDER.

BITDEFENDER SRL, Preciziei Boulevard, n.24, West Gate Building H2, ground floor, distretto 6, Bucarest, Romania

Prefazione

La presente guida è destinata a tutti gli utenti che hanno scelto **BitDefender Free Antivirus 2010** come soluzione di sicurezza per i loro PC. L'informazione presentata in questo libro è indicata non solo per esperti di computer ma è inoltre accessibile a chiunque sia capace di utilizzare Windows.

Questo manuale illustra BitDefender Free Antivirus 2010, e il processo di installazione e configurazione. Sarà possibile imparare ad utilizzare BitDefender Free Antivirus 2010, ad aggiornarlo, testarlo e personalizzarlo, in pratica come sfruttare al meglio BitDefender.

Ti auguriamo una lettura gradevole e utile.

1. Convenzioni usate in questo manuale

1.1. Convenzioni tipografiche

Nel libro vengono usati diversi stili di testo per una leggibilità migliorata. Il loro aspetto e significato vengono presentati nella tabella sottostante.

Aspetto	Descrizione
`sample syntax`	Gli esempi sintattici vengono scritte con caratteri `monospazio`.
http://www.bitdefender.it	I link URL puntano su alcuna ubicazione esterna, su server http o ftp.
documentation@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo per informazioni sui contatti.
«Prefazione» (p. x)	Questo è un link interno, verso qualche ubicazione nel documento.
`filename`	File e directory (cartelle) vengono scritte con fonti `monospazio`.
option	Tutte le opzioni del prodotto vengono scritte usando caratteri in **grassetto**.

1.2. Avvertenze

Le avvertenze appaiono in note di testo, segnalate graficamente, offrendo alla tua attenzione informazione addizionale relativa al paragrafo corrente.

Nota

La nota è solo una piccola osservazione. Anche se la puoi omettere, la nota può provvedere informazione di valore come una caratteristica specifica o un link verso temi relazionati.

Importante

Questa richiede la tua attenzione e non è consigliato saltarla. Solitamente facilita informazione non critica ma significante.

Avvertimento

Questa è un'informazione critica che dovresti trattare con crescente cautela. Niente di male accadrà se segui le istruzioni. Dovresti leggerlo e capirlo, perché descrive qualcosa di estremamente rischioso.

2. Struttura del manuale

Il manuale è composto da diverse parti contenenti gli argomenti importanti. Inoltre, viene anche fornito un glossario per chiarire alcuni termini tecnici.

Installazione e rimozione. Istruzioni passo passo per l'installazione di BitDefender su un personal computer. Partendo dai prerequisiti per una installazione valida, l'utente viene guidato lungo l'intero processo di installazione. Infine la procedura di rimozione viene descritta nel caso si abbia bisogno di disinstallare BitDefender.

Configurazione e Gestione. Vi spieghiamo come configurare ed utilizzare tutti i moduli di BitDefender in modo da proteggere efficacemente il vostro computer da ogni tipo di minaccia malware (virus, spyware, rootkit ed altro).

Integrazione in Software Windows e di terzi . Mostra come utilizzare le opzioni di BitDefender dal menu contestuale di Windows e dalla barra degli strumenti BitDefender integrata in programmi supportati di terze parti.

Risoluzione dei problemi e aiuto. Dove cercare e ottenere un aiuto in caso di difficoltà.

Glossario. Il glossario cerca di spiegare alcuni termini tecnici e poco comuni che troverai tra le pagine di questo documento.

3. Richiesta di commenti

Ti invitiamo ad aiutarci a migliorare questo manuale. Abbiamo provato e verificato tutta l'informazione con la nostra massima capacità, ma potresti trovare che le caratteristiche siano cambiate (o persino che abbiamo commesso degli errori). Per favore scrivi per parlarci su qualsiasi errore trovi in questo libro o come credi che possa essere migliorato, per aiutarci a fornirti la migliore documentazione possibile.

Facci sapere inviando una e-mail a documentation@bitdefender.com.

Importante

Per una comunicazione efficiente, vi invitiamo a scrivere i vostri documenti e le e-mails in lingua Inglese.

Installazione e rimozione

1. Requisiti del sistema

È possibile installare BitDefender Free Antivirus 2010 solo su computer con i seguenti sistemi operativi:

- Windows XP (32/64 bit) con Service Pack 2 o superiore
- Windows Vista (32/64 bit) o Windows Vista con Service Pack 1 o successivo
- Windows 7 (32/64 bit)

Prima dell'installazione, assicurarsi che il computer soddisfa i prerequisiti hardware e software minimi.

Nota

Per verificare il sistema operativo sul computer e l'informazione hardware, fare clic con il pulsante destro del mouse su **Risorse del computer** sul desktop e quindi selezionare **Proprietà** dal menu.

1.1. Requisiti minimi di sistema

- 450 MB di spazio disponibile su disco rigido
- Processore da 800 MHz
- RAM:
  - 512 MB per Windows XP
  - 1 GB per Windows Vista/Windows 7
- Internet Explorer 6.0
- .NET Framework 1.1 (disponibile anche nel kit d'installazione)

1.2. Requisiti di sistema consigliati

- 600 MB di spazio disponibile su disco rigido
- Intel CORE Duo (1.66 GHz) o processore equivalente
- RAM:
  - 1 GB per Windows Vista/Windows 7
  - 1,5 GB per Windows Vista
- Internet Explorer 7 (o superiore)
- .NET Framework 1.1 (disponibile anche nel kit d'installazione)

1.3. Software supportato

La protezione antiphishing viene fornita solo per:

- Internet Explorer 6.0 o superiore
- Mozilla Firefox 2.5
- Yahoo Messenger 8.5
- Windows Live Messenger 8

2. Preparazione all'Installazione

Prima di installare BitDefender Free Antivirus 2010, completare questi passi preliminari per assicurarsi che l'installazione funzioni senza problemi:

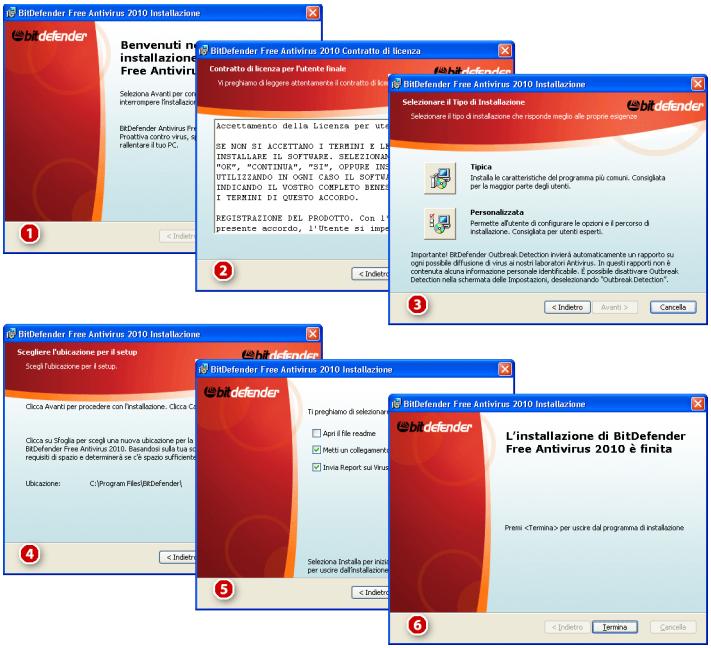
- Assicurarsi che il computer su cui si desidera installare BitDefender risponda ai requisiti minimi di sistema. Se il computer non risponde ai requisiti minimi di sistema, BitDefender non verrà installato o se installato non funzionerà correttamente e causerà rallentamenti e instabilità del sistema. Per un elenco completo dei requisiti di sistema, fare riferimento a «*Requisiti del sistema*» (p. 2).
- Accedere al computer utilizzando un account Amministratore.
- Rimuovere qualsiasi altro software di sicurezza dal computer. L'esecuzione simultanea di due programmi di sicurezza può influenzarne il funzionamento e causare problemi seri al sistema. Windows Defender sarà disabilitato per default prima dell'avvio dell'installazione.

3. Installazione di BitDefender

Il file di installazione può essere scaricato dal sito web di BitDefender al seguente indirizzo: http://www.bitdefender.it.

Individuare il file di setup e cliccare due volte. Verrà lanciato l'assistente che vi guiderà attraverso il processo di setup:

Il programma di installazione controllerà innanzitutto il sistema per convalidare l'installazione. Se l'installazione viene convalidata, apparirà l'assistente di setup. L'immagine seguente illustra i passaggi dell'assistente di setup.



Fasi per l'installazione

Seguire questi passi per installare BitDefender Free Antivirus 2010:

1. Selezionare **Avanti**. E' possibile annullare l'installazione in qualsiasi momento facendo clic su **Annulla**.

   BitDefender Free Antivirus 2010 avvisa se vi sono altri prodotti antivirus installati sul computer. Selezionare **Rimuovi** per disinstallare il corrispondente prodotto. Se si desidera continuare senza rimuovere i prodotti rilevati, selezionare **Avanti**.

Avvertimento
Si raccomanda di disinstallare qualsiasi altro prodotto antivirus precedentemente installato. Infatti due o più antivirus sulla stessa macchina potrebbero rendere il sistema inutilizzabile.

2. Vi preghiamo di leggere il Contratto di Licenza, e selezionare **Accetto**

Importante
Se non siete d'accordo con le condizioni del contratto, selezionare **Cancella**. Il processo di installazione verrà abbandonato ed uscirete dal setup.

3. Selezionare il tipo di installazione da eseguire.
   - **Tipica** - per installare il programma immediatamente, utilizzando le opzioni di installazione di default. Se si seleziona questa opzione, passare al Passo 6.
   - **Personalizzata** - per configurare le opzioni di installazione e quindi installare il programma. Questa opzione permette di modificare il percorso di installazione.
4. Per default, BitDefender Free Antivirus 2010 verrà installato in `C:\Program Files\BitDefender\BitDefender 2010`. Se si desidera modificare il percorso d'installazione, fare clic su **Sfoglia**, quindi selezionare, la cartella dove si desidera installare Antivirus BitDefender 2010.

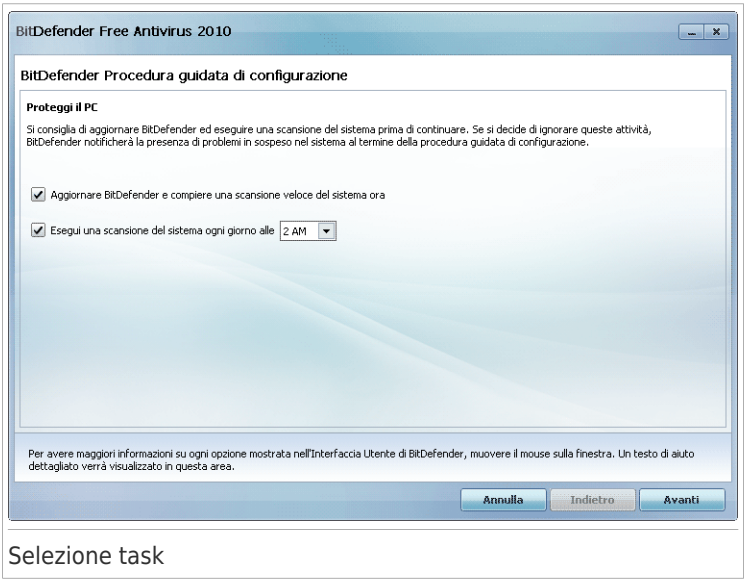
   Selezionare **Avanti**.
5. Selezionare le opzioni relative al processo di installazione. Le opzioni consigliate sono selezionate per default:
   - **Apri il file readme** - per aprire il file leggimi al termine dell'installazione.
   - **Metti un collegamento sul desktop** - per mettere un collegamento a BitDefender Free Antivirus 2010 sul desktop al termine dell'installazione.
   - **Invia Rapporti Virus** - per inviare rapporti sulla scansione antivirus al Laboratorio BitDefender per l'analisi. I report non conterranno dati confidenziali, come il vostro nome o indirizzo IP, e non verranno utilizzati per scopi commerciali.
   - **Disattiva Windows Defender** - per disattivare Windows Defender; questa opzione compare slo su Windows Vista.

   Fare clic su **Installa** per avviare l'installazione. Se non è stato ancora installato, BitDefender installerà per prima .NET Framework 1.1.
6. Attendere che l'installazione sia completata e fare clic su **Termina**. Vi verrà richiesto di riavviare il sistema in modo che l'assistente di setup completi il processo di installazione. Si raccomanda di farlo al più presto.

3.1. Procedura guidata di Configurazione

La prima volta che avviarete il computer dopo l'installazione, comparirà l'assistente di configurazione. Questo assistente permette di aggiornare i file del prodotto e le firme dei malware ed effettuare una scansione dei file di sistema e delle applicazioni per assicurarsi che non siano infetti. Se non si desidera seguire questo assitente, fare click su **Annulla**.

3.1.1. Passo 1 - Selezionare le Attività da eseguire



Selezione task

Impostare BitDefender per l'esecuzione di attività importanti per la sicurezza del sistema. Sono disponibili le seguenti opzioni:

- **Aggiorna BitDefender ed esegui una scansione veloce del sistema ora** - al passaggio successivo le firme dei virus e i file di prodotto di BitDefender verranno aggiornati per proteggere il computer contro le minacce più recenti. Inoltre, immediatamente al termine dell'aggiornamento, BitDefender effettuerà una scansione dei file nelle cartelle `Windows` e `Programmi` per assicurarsi che non siano infetti. Queste cartelle contengono file del sistema operativo e delle applicazioni installate e sono di norma le prime ad essere infettate.
- **Esegui una scansione del sistema ogni giorno alle 2** - imposta BitDefender in modo da eseguire una scansione standard del computer ogni giorno alle 2. Per modificare l'orario di esecuzione della scansione, fare clic sul menu e selezionare

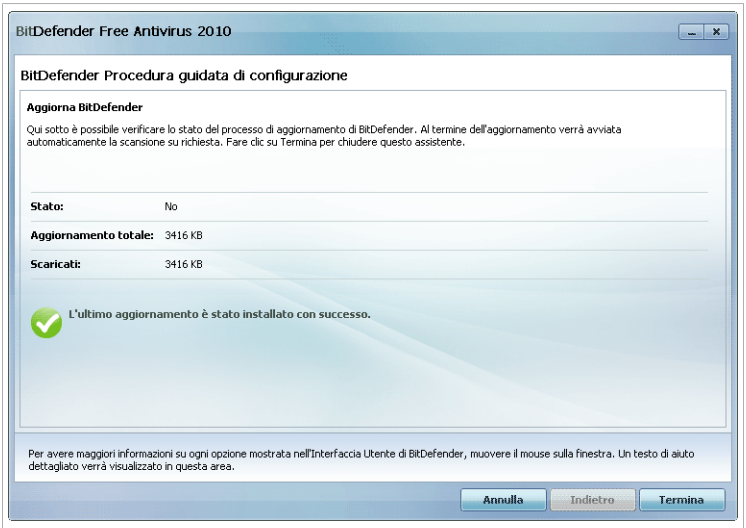
l'orario di inizio desiderato. Se il computer è spento quando deve essere eseguita la programmazione, l'attività verrà eseguita appena si avvia il computer.

Nota
In seguito non potrai disattivare o riconfigurare la scansione programmata.

Vi raccomandiamo di abilitare queste opzioni prima di passare al passo successivo per assicurare la sicurezza del vostro sistema. Selezionare **Successivo** per continuare.

Se viene deselezionata la prima casella di controllo, non vi sono attività da eseguire nell'ultimo passaggio dell'assistente. Fare clic su **Termina** per completare l'assistente.

3.1.2. Passo 2 - Fine



Stato dei Task

Attendere che BitDefender aggiorni le firme del malware e i motori di scansione. Non appena l'aggiornamento è completato, verrà avviata una scansione rapida del sistema. La scansione avverrà in modo silenzioso, in background. E' possibile seguire l'icona di avanzamento della scansione nell'area di notifica. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

Fare clic su **Termina** per completare l'assistente. Non devi attendere il termine della scansione

Nota

La scansione impiegherà alcuni minuti. Quando è terminata, aprire la finestra di scansione per controllare i risultati e assicurarsi che il sistema sia pulito. Se un virus è rilevato durante una scansione, dovresti aprire immediatamente BitDefender ed avviare una scansione completa

4. L'aggiornamento alla versione a pagamento

Le versioni a pagamento di BitDefender aggiornano automaticamente ogni ora le signature contro i malware. Oltre alla protezione in tempo reale, questi prodotti garantiscono diverse funzioni con l'obiettivo di proteggere il computer e la sua indentità in rete.

Per poter aggiornare BitDefender Free Antivirus 2010 ad una versione a pagamento, la preghiamo di seguire i seguenti passi:

1. Acquista un prodotto BitDefender che soddisfi le tue necessità. Clicchi sul link **Acquista adesso** situato al fondo dell'interfaccia BitDefender per poter essere ridiretto alla pagina web dove potrà acquistare i prodotti BitDefender.
2. Installa la versione acquistata di BitDefender: clicca due volte sul file eseguibile e segui le istruzioni d’installazione. Non è necessario prima rimuovere BitDefender Free Antivirus 2010.

5. Riparare o Rimuovere BitDefender

Se si desidera riparare o rimuovere BitDefender Free Antivirus 2010, seguire questo percorso dal menu di avvio di Windows: **Start → Programmi → BitDefender 2010 → Ripara o Rimuovi**.

Vi verrà richiesto di confermare la vostra scelta selezionando **Avanti**. Apparirà una nuova finestra dove potrete selezionare:

- **Riparare** - per re-installare tutte le componenti del programma installate dal setup precedente.

  Scegliendo di riparare BitDefender, la seguente nuova finestra comparirà. Selezionare **Riparare** per iniziare il processo di riparazione.

  Riavviare il computer quando venga richiesto, e quindi selezionare **Installare** per reinstallare BitDefender Free Antivirus 2010.

  Una volta completato il processo di installazione, apparirà una nuova finestra. Selezionare **Termina**.

- **Rimuovi** - per rimuovere tutte le componenti installate.

  Nota
  Vi consigliamo di scegliere **Rimuovere** per una reinstallazione pulita.

  Scegliendo di rimuovere BitDefender, apparirà una nuova finestra.

  Importante

  Solo Windows Vista! Rimuovendo BitDefender, non sarete più protetti contro le minacce malware come virus e spyware. Se desiderate che Windows Defender venga attivato dopo aver disinstallato BitDefender, selezionare la casella di controllo corrispondente.

  Selezionare**Rimuovere** per iniziare la rimozione di BitDefender Free Antivirus 2010 dal computer.

  Una volta completato il processo di rimozione, apparirà una nuova finestra. Selezionare **Termina**.

  Nota
  Al termine del processo di disinstallazione, consigliamo di cancellare la cartella `BitDefender` dei `Program Files`.

Configurazione e Gestione

6. Iniziando

BitDefender Free Antivirus 2010 offre una protezione di base contro virus, spyware, rootkits e altri malware. Poichè il suo obiettivo è quello di rispondere ai bisogni di protezione antivirus di base, viene aggiornato meno frequentemente e non scannerizza il web e il traffico e-mail.

BitDefender Free Antivirus 2010 è preregistrato con una licenza che le permette di utilizzare il prodotto per un anno dalla data di istallazione. Non appena la chiave di licenza scade, BitDefender cessa di eseguire le sue funzioni.

6.1. Apertura di BitDefender in corso

Per accedere all'interfaccia principale di BitDefender Free Antivirus 2010, usare il menu Avvio di Windows, seguendo il percorso: **Start → Programmi → BitDefender 2010 → BitDefender Free Antivirus 2010** o più rapidamente facendo doppio clic sull'icona BitDefender presente nella barra delle applicazioni.

6.2. Panoramica interfaccia utente

BitDefender Free Antivirus 2010 soddisfa le necessità di persone esperte e di principianti. L'interfaccia grafica dell'utente è quindi stata progettata per essere adatta a qualsiasi categoria di utenti.

Modalità intermedia

La seguente tabella descrive brevemente ogni scheda dell'interfaccia utente.

Tab	Descrizione
Dashboard	Indica lo stato della sicurezza del sistema.
Antivirus	Mostra lo stato del modulo antivirus, il quale vi aiuta a mantenere il vostro BitDefender aggiornato ed il vostro computer libero di virus.
Antiphishing	Mostra lo stato dei moduli che ti proteggono contro il phishing (furto di informazioni personali) mntre sei online

Nell'angolo in alto a destra della finestra è possibile vedere il pulsante **Impostazioni**. Apre una finestra in cui è possibile abilitare o disabilitare le impostazioni principali di BitDefender. Per ulteriori informazioni, ti preghiamo di far riferimento a «*Configurazione delle Impostazioni di base*» (p. 33).

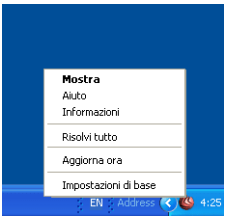
Nell'angolo in basso a destra della finestra è possibile trovare diversi link utili.

Link	Descrizione
Acquista adesso	Apre una pagina web dove è possibile acquistare un prodotto BitDefender. Le versioni a pagamento di BitDefender aggiornano automaticamente ogni ora le signature contro i malware. Oltre alla protezione in tempo reale, questi prodotti garantiscono diverse funzioni con l'obiettivo di proteggere il computer e la sua indentità in rete.
Supporto (FAQ)	Apre una pagina web che fornisce utili informazioni di supporto tecnico.
Inviare Feedback	Apre una pagina web dove è possibile inviare il feedback.
Aiuto	Ti da accesso ad un file di aiuto che ti insegna ad usare BitDefender.
Visualizza Registri	Vi permette di visualizzare una cronologia dettagliata di tutti i task eseguiti da BitDefender nel vostro sistema.

6.3. Icona barra delle applicazioni

Per gestire tutto il prodotto più velocemente, è possibile utilizzare l'icona BitDefender nella barra delle applicazioni. Se si fa doppio clic su questa icona, BitDefender si aprirà. Inoltre, facendo clic con il pulsante destro sull'icona, apparirà un menu contestuale che consentirà una rapida gestione del prodotto BitDefender.

- **Mostra** - apre l'interfaccia di BitDefender.
- **Help** - apre il file di aiuto, che spiega nel dettaglio come configurare e usare BitDefender Free Antivirus 2010.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su BitDefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.



Icona della barra delle applicazioni

- **Risolvi tutto** - aiuta a rimuovere tutte le vulnerabilità di sicurezza correnti. Se l'opzione non è disponibile, non ci sono errori da riolvere. Per ulteriori informazioni, far riferimento a *«Risolvi i Problemi»* (p. 19).
- **Aggiorna adesso** - inizia un aggiornamento immediato. Apparirà una nuova finestra, dove potrete visualizzare lo stato dell'aggiornamento.
- **Impostazioni di base** - apre una finestra dove è possibile abilitare e disabilitare le impostazioni principali del prodotto. Per ulteriori informazioni, far riferimento a *«Configurazione delle Impostazioni di base»* (p. 33).

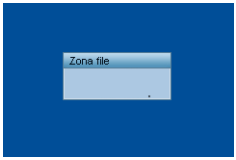
Se ci fossero problemi critici che colpicono il vostro sistema, un punto esclamativo verrà mostrato sull'icona BitDefender.

Se BitDefender non è in funzione, l'icona nell'area di notifica è disattivata. Questo si verifica normalmente quando la licenza è scaduta. Può anche verificarsi quando i servizi di BitDefender non rispondono o quando altri errori interferiscono con il normale funzionamento di BitDefender.

6.4. Barra di Attività della Scansione

La **Barra delle attività di scansione** è una visualizzazione grafica dell'attività di scansione sul vostro sistema. Questa piccola finestra è disabilitata per default.

Le barre grigie (**Zona File**) indicano il numero di file esaminati al secondo, in una scala da 0 a 50.

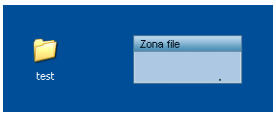


Barra di Attività della Scansione

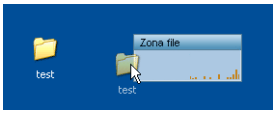
Nota
La Barra delle attività di scansione vi informerà quando la protezione in tempo reale sia disattivata mostrando una croce rossa sulla **Zona File**.

6.4.1. Scansiona File e Cartelle

Puoi usare la barra di scansione per scansionare velocemente files e cartelle (trascinandoli sopra alla barra) Selezionare il file o la cartella che si desidera esaminare e trascinarla sulla **Barra delle Attività di Scansione**, come nella figura seguente.



Trascinare il file



Abbandonare il file

Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 37).

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti. Le opzioni di scansione sono standard e non è possibile modificarle.

6.4.2. Attiva/Disattiva Scan attività di bar

Per attivare la barra delle attività di scansione, seguire questi passi:

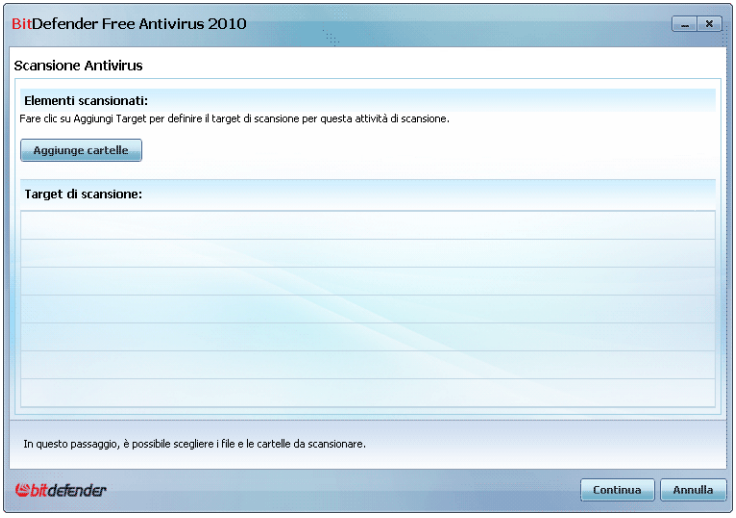
1. Apri BitDefender.
2. Fare clic sul pulsante **Impostazioni** in alto a destra.
3. Nella categoria Impostazioni generali, selezionare la casella di controllo corrispondente a **Barra Attività di Scansione**.
4. Fare clic su **OK** per salvare e applicare i cambiamenti.

Quando non si vuole più vedere la visualizzazione grafica, si deve semplicemente premere sulla stessa con il pulsante destro e selezionare **Nascondi**.

6.5. Scansione Manuale di BitDefender

La scansione Manuale BitDefender consente di scansionare cartelle o partizioni di disco rigido specifiche senza dover creare una attività di scansione. Questa funzionalità è stata progettata per essere utilizzata quando Windows è in Modalità provvisoria. Se il sistema è infettato con un virus resistente, si può provare a rimuovere il virus avviando Windows nella Modalità provvisoria e eseguendo la scansione di ogni partizione di disco rigido usando BitDefender Manual Scan.

Per accedere alla Scansione Manuale BitDefender utilizzare il menu Avvio di Windows, seguendo il percorso **Avvio → Programmi → BitDefender 2010 → Scansione Manuale di BitDefender** Apparirà la finestra seguente:



Scansione Manuale di BitDefender

Fare clic su **Aggiungi Cartella**, selezionare la posizione per cui si desidera eseguire la scansione e fare clic su **OK**. Se si desidera eseguire la scansione di cartelle multiple, ripetere questa azione per ciascuna posizione aggiuntiva.

I percorsi alle posizioni selezionate appariranno nella colonna **Target di Scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutti i Percorsi** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si ha concluso la selezione delle posizioni, fare clic su **Continua**. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori

informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 37).

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti. Le opzioni di scansione sono standard e non è possibile modificarle.

Cos'è la Modalità provvisoria?
La modalità provvisoria è un modo speciale di avviare Windows, usato principalmente per risolvere problemi che influenzano il normale funzionamento di Windows. Tali problemi vanno da driver in conflitto a virus che impediscono a Windows di avviarsi normalmente. Nella Modalità provvisoria, Windows carica solo una parte minima di componenti del sistema operativo e dei driver fondamentali. Solo alcune applicazioni funzionano nella Modalità provvisoria. Ecco perché la maggior parte del virus sono inattivi quando si utilizza Windows nella Modalità provvisoria e perché possono essere facilmente rimossi.
Per avviare Windows nella Modalità provvisoria, riavviare il computer e premere il tasto F8 fino a quando appare il Menu opzioni avanzate di Windows. È possibile scegliere tra varie opzioni di Windows nella Modalità provvisoria. Si può selezionare **Modalità provvisoria con Networking** per abilitare l'accesso a Internet.

Nota

Per ulteriori informazioni sulla Modalità provvisoria, fare clic su Guida e Supporto tecnico di Windows (nel menu Start, fare clic su **Guida e Supporto tecnico**). È inoltre possibile trovare informazioni utili cercando su Internet.

6.6. Rilevamento dispositivo automatico

BitDefender rileva automaticamente quando si collega un dispositivo rimovibile al computer e chiede di eseguirne la scansione prima che si acceda ai suoi file. Questa operazione è consigliata per impedire che virus e altri malware infettino il computer.

I dispositivi rilevati rientrano in una di queste categorie:

- CD/DVD
- Dispositivi di archiviazione USB, ad esempio chiavette e dischi rigidi esterni
- unità di rete (remote) mappate

Quando un tale dispositivo viene rilevato, viene visualizzata una finestra di avviso.

Allarme Rilevamento Dispositivi

Per scansionare il dispositivo di archiviazione, è sufficiente fare clic su **Sì**. Appare la procedura guidata Antivirus Scan che illustra il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 37).

Se non si desidera scansionare il dispositivo, si deve fare clic su **No**. In questo caso, si possono ritenere utili una di queste opzioni:

- **Non farmi più domande su questo tipo di dispositivo** - BitDefender non chiederà più di eseguire la scansione di dispositivi di questo tipo quando sono collegati al tuo computer.
- **Disabilita rilevamento automatico dispositivi** - Non verrà più chiesto di eseguire la scansione di nuovi dispositivi di archiviazione quando sono collegati al computer.

Importante
La informiamo che nel caso in cui utilizzi queste opzioni, non potrà abilitare di nuovo la detenzione automatica.

7. Risolvi i Problemi

BitDefender utilizza un sistema di identificazione dei problemi per rilevare e fornireinformazioni relative ai problemi che potrebbero avere effetto sulla sicurezza delcomputer e dei dati. I problemi in sospeso vengono notificati nel modo seguente:

- Viene visualizzato un simbolo speciale sull'icona BitDefender nell'area di notifica ad indicare la presenza di problemi in sospeso.

  Triangolo rosso con un punto esclamativo: Si sono verificati dei problemi critici per la sicurezza del sistema. Tali problemi richiedono immediata attenzione e devono essere risolti il più presto possibile.

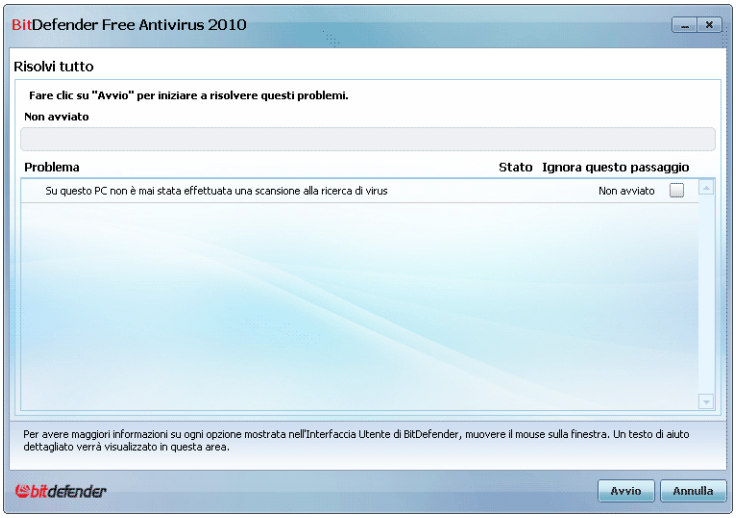
  Inoltre muovendo il cursore sull'icona un pop-up confermerà l'esistenza di problemi in sospeso.

- Quando viene aperto BitDefender, l'area Stato della Sicurezza indicherà il numero di problemi del sistema.

7.1. Assistente Risolti Tutti i Problemi

Il modo più semplice di risolvere i problemi esistenti è di seguire le istruzioni passo-passo dell'assistente **Risolvi tutto**. L'assistente aiuta a rimuovere con facilità qualsiasi minaccia per la sicurezza del computer e dei dati. Per aprire l'assistente, compiere una delle seguenti operazioni:

- Fare clic on il pulsante di destra sull icona BitDefender nell'area di notifica e selezionare **Risolvi tutto**.
- Apri BitDefender, andare alla scheda **Dashboard** e fare clic su **Risolvi tutto**.



Assistente Risolti Tutti i Problemi

L'assistente visualizza l'elenco delle vulnerabilità di sicurezza esistenti sul computer.

Tutti i problemi attuali sono stati selezionati per essere risolti. Se vi è un problema che non si desidera risolvere, selezionare la casella di controllo corrispondente. In questo modo lo stato cambierà su **Ignora**.

Nota
Se non si desidera ricevere notifiche relative a particolari problemi è necessario configurare di conseguenza il sistema di controllo, come descritto alla sezione successiva.

Per risolvere i problemi selezionati, fare clic su **Avvia**. Alcuni problemi vengono risolti immediatamente. Per altri problemi verrà eseguito un assistente per poterli risolvere.

I problemi che l'assistente permette di risolvere possono essere raggruppati nelle seguenti categorie principali:

- **Impostazioni di sicurezza disabilitate.** Tali problemi vengono risolti immediatamente abilitando le rispettive impostazioni di sicurezza.
- **Attività di sicurezza preventiva che è necessario eseguire.** Un esempio di tali attività è la scansione del computer. Si consiglia di eseguire la scansione del compuer almeno una volta alla settimana. BitDefender compirà questa attività automaticamente nella maggior parte dei casi. Tuttavia se il programma di

scansione è stato modificato o non è stato completato, si riceverà un avviso relativo a questo problema.

Nel risolvere tali problemi, un assistente permette di completare con successo l'attività.

7.2. Configurazione del monitoraggio problemi

E' possibile configurare il sistema di controllo per rispondere al meglio alle proprieesigenze di sicurezza, selezionando di quali problemi specifici si desidera essereinformati. Attenersi alla seguente procedura:

1. Andare alle schede **Antivirus** o **Antiphishing**.
2. Fare clic su **Configura Status Alerts**.
3. Selezionare le caselle di controllo corrispondenti agli elementi che si desidera monitorare.

8. Dashboard

La scheda Dashboard fornisce informazioni sullo stato di sicurezza del computer e permette di risolvere i problemi in sospeso.

Dashboard

La Dashboard è costituita dalle seguenti sezioni:

- **Stato di sicurezza** - Indica il numero di problemi che influiscono sul computer ed aiuta a risolverli. Se vi sono problemi in sospeso verrà visualizzato un **cerchio rosso con un punto esclamativo** e il pulsante **Risolvi tutto**. Fare clic sul pulsante per avviare l'assistente Risolvi tutto.
- **Dettagli Stato** - Indica lo stato di ciascun modulo principale utilizzando frasi esplicite e una delle seguenti icone:

  Cerchio verde con un segno di spunta: Non vi sono problemi che influenzano lo stato di sicurezza. Il computer e i dati sono protetti.

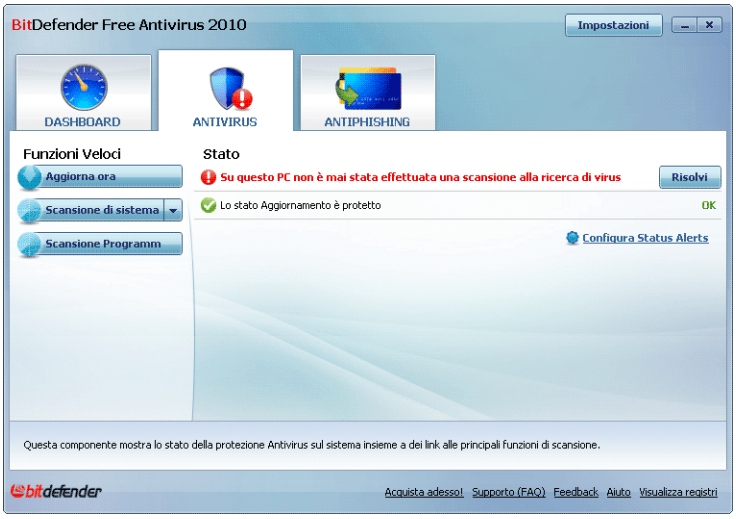
  Cerchio grigio con un punto esclamativo: L'attività dei componenti di questo modulo non viene monitorata. Di conseguenza non vi sono informazioni disponibili sullo stato di sicurezza di tali componenti. Potrebbero esservi problemi specifici relativi a questo modulo.

  Cerchio rosso con un punto esclamativo: Vi sono problemi che influiscono sulla sicurezza del sistema. I problemi critici richiedono immediata attenzione. Anche i problemi non critici dovrebbero essere affrontati il più presto possibile.

Fare clic sul nome di un modulo per visualizzare ulteriori dettagli sul suo stato e per configurare il monitoraggio dello stato dei suoi componenti.

9. Antivirus

BitDefender contiene un modulo di Antivirus che vi aiuta a mantenere il vostro BitDefender aggiornato ed il vostro computer libero di virus. Per accedere al modulo Antivirus, cliccare sul tab **Antivirus**.



Antivirus

Il modulo Antivirus ha due sezioni:

- **Area di Stato** - Visualizza lo stato attuale di tutti i componenti di sicurezza monitorati e permette di selezionare quali componenti monitorare.
- **Attività Veloci** - Qui si trovano i link alle attività di sicurezza più importanti: aggiornamento immediato, scansione del sistema e scansione personalizzata.

9.1. Area di Stato

L'area di stato visualizza l'elenco completo dei componenti del modulo di sicurezza e il loro stato attuale. Monitorando ogni modulo di sicurezza, BitDefender vi comunicherà non solo quando vengono configurate delle impostazioni che potrebbero influenzare la sicurezza del vostro computer, ma anche quando viene dimenticata l'esecuzione di attività importanti.

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** corrispondente ad una frase per risolvere il problema riportato. Se un problema non viene risolto subito seguire l'assistente per risolverlo.

9.1.1. Configurazione del Monitoraggio Stato

Per selezionare i componenti che BitDefender deve monitorare, fare clic su **Configura Status Alerts** e selezionare la casella di controllo **Abilita allarmi** corrispondente alle caratteristiche che si desidera monitorare.

Importante

Per assicurarsi che il sistema sia completamente protetto abilitare il monitoraggio per tutti i componenti e risolvere tutti i problemi riportati.

BitDefender può monitorare lo stato dei seguenti componenti di sicurezza:

- **Antivirus** - BitDefender controlla lo stato dei due componenti della funzione Antivirus: protezione in tempo reale e scansione a richiesta. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
La protezione in tempo reale è disabilitata	I file non vengono controllati quando viene effettuato l'accesso da parte vostra o da parte di un'applicazione in esecuzione sul sistema.
Questo PC non è stato mai controllato alla ricerca di virus	Non è mai stata compiuta una scansione del sistema su richiesta per controllare che i file contenuti sul computer siano esenti da malware.
L'ultima scansione di sistema avviata è stata annullata prima della sua conclusione	È stata avviata, ma non completata, una scansione completa del sistema.
L'Antivirus è in uno stato critico	La protezione in tempo reale del sistema è disabilitata e la scansione del sistema è ormai necessaria da lungo tempo.

- **Aggiornamento** - BitDefender controlla se le firme del malware sono aggiornate. I problemi più comuni riportati per questo componente vengono elencati nella seguente tabella.

Problema	Descrizione
L'Aggiornamento Automatico è disabilitato	Le firme del malware del prodotto BitDefender non vengono aggiornate automaticamente e regolarmente.
L'aggiornamento non è stato compiuto per x giorni	Le firme del malware del prodotto BitDefender sono obsolete.

9.2. Funzioni Veloci

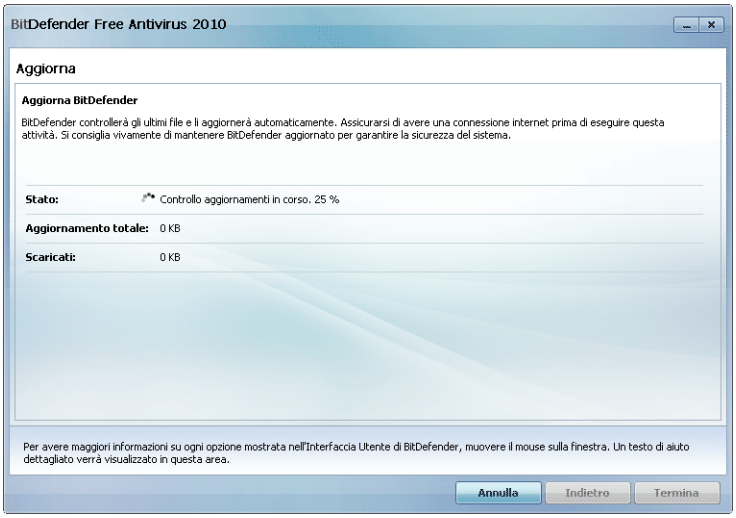
In questo elenco è possibile trovare dei link alle attività di sicurezza più importanti:

- **Aggiorna adesso** - inizia un aggiornamento immediato.
- **Scansione del Sistema** - inizia una scansione completa del computer (archivi esclusi).
- **Scansione Programmata** - avvia un assistente che permette di creare ed eseguire un'attività di scansione personalizzata.

9.2.1. Aggiornamento di BitDefender

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

BitDefender controlla automaticamente se ci sono aggiornamenti quando accendete il computer ed in seguito **ogni 24 ore** dopo. Ad ogni modo, se si vuole aggiornare BitDefender, cliccare semplicemente su **Aggiorna adesso**. Il processo di aggiornamento verrà iniziato ed apparirà immediatamente la seguente finestra:



Aggiornamento di BitDefender

In questa finestra potete visualizzare lo stato del processo di aggiornamento.

Il processo di aggiornamento viene eseguito in volo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Se si desidera chiudere questa finestra, cliccare semplicemente su **Annulla**. Ad ogni modo, questo non fermerà il processo di aggiornamento.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di BitDefender su richiesta dell'utente.

Riavviare il computer se richiesto. In caso di un aggiornamento importante, verrà chiesto di riavviare il computer. Cliccare su **Riavviare** per riavviare il sistema immediatamente.

Se si desidera riavviare il sistema più tardi, cliccare semplicemente su **OK**. Si consiglia di riavviare il sistema al più presto.

9.2.2. Scansione con BitDefender

Per avviare la scansione del vostro computer alla ricerca di malware, eseguire un task particolare di scansione cliccando sul tasto corrispondente. La seguente tabella elenca i task di scansione disponibili, assieme alla loro descrizione:

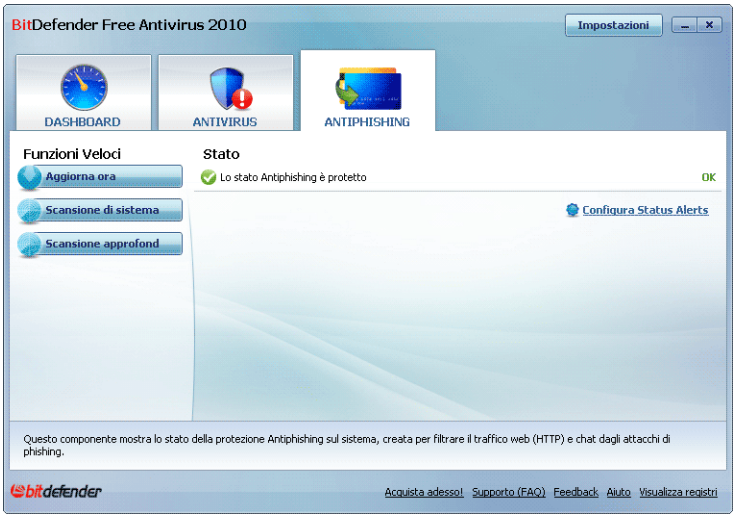
Task	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi, per tutti i tipi di malware ad eccezione dei rootkit.
Scansione Programmata	Usare questa funzione per scegliere file e cartelle specifici da esaminare.

Quando si esegue una Scansione sistema, apparirà l'assistente Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 37).

Quando si esegue una Scansione Personalizzata, l'assistente Scansione Personalizzata vi condurrà lungo il processo di scansione. Seguire i sei passi della procedura guidata per effettuare la scansione di file o cartelle specifiche. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Assistente Scansione Programmata*» (p. 41).

10. Antiphishing

BitDefender contiene un modulo Antiphishing che assicura che tutte le pagine web a cui si accede tramite Internet Explorer o Firefox siano sicure. Per accedere al modulo Antiphishing, cliccare sul tasto **Antiphishing**.



Antiphishing

Il modulo Antiphishing ha due sezioni:

- **Area di Stato** - Visualizza lo stato attuale del modulo antiphishing e permette di abilitare/disabilitare il monitoraggio dell'attività di tale modulo.
- **Attività Veloci** - Qui si trovano i link alle attività di sicurezza più importanti: aggiornamento immediato, scansione del sistema e scansione approfondita del sistema.

10.1. Area di Stato

Lo stato attuale di un componente è indicato utilizzando frasi esplicite e una delle icone seguenti:

Cerchio verde con un segno di spunta: Nessun problema riscontrato sul componente.

Cerchio rosso con un punto esclamativo: Alcuni problemi riscontrati sul componente.

Le frasi di descrizione dei problemi sono visualizzate in rosso. Fare clic sul pulsante **Risolvi** corrispondente ad una frase per risolvere il problema riportato.

Il problema più comune riportato per questo modulo è **Antiphishing disabilitato**. Questo indica che l'Antiphishing non è abilitato per una o più delle seguenti applicazioni supportate: Internet Explorer, Mozilla Firefox, Yahoo! Messenger o Windows Live Messenger.

10.2. Funzioni Veloci

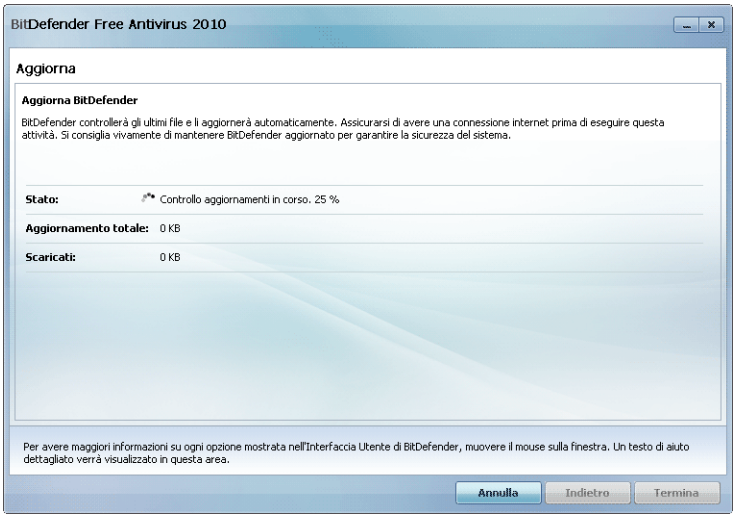
In questo elenco è possibile trovare dei link alle attività di sicurezza più importanti:

- **Aggiorna adesso** - inizia un aggiornamento immediato.
- **Scansione del Sistema** - inizia una scansione completa del computer (archivi esclusi).
- **Scansione approfondita** - avvia una scansione completa del computer (archivi inclusi).

10.2.1. Aggiornamento di BitDefender

Tutti giorni vengono trovati ed identificati nuovi malware. E' quindi molto importante mantenere aggiornato il vostro BitDefender con le impronte più recenti del malware.

BitDefender controlla automaticamente se ci sono aggiornamenti quando accendete il computer ed in seguito **ogni 24 ore** dopo. Ad ogni modo, se si vuole aggiornare BitDefender, cliccare semplicemente su **Aggiorna adesso**. Il processo di aggiornamento verrà iniziato ed apparirà immediatamente la seguente finestra:



Aggiornamento di BitDefender

In questa finestra potete visualizzare lo stato del processo di aggiornamento.

Il processo di aggiornamento viene eseguito in volo, il chè vuol dire che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Se si desidera chiudere questa finestra, cliccare semplicemente su **Annulla**. Ad ogni modo, questo non fermerà il processo di aggiornamento.

Nota
Se siete connessi a Internet mediante una connessione telefonica, è consigliato l'aggiornamento periodico di BitDefender su richiesta dell'utente.

Riavviare il computer se richiesto. In caso di un aggiornamento importante, verrà chiesto di riavviare il computer. Cliccare su **Riavviare** per riavviare il sistema immediatamente.

Se si desidera riavviare il sistema più tardi, cliccare semplicemente su **OK**. Si consiglia di riavviare il sistema al più presto.

10.2.2. Scansione con BitDefender

Per avviare la scansione del vostro computer alla ricerca di malware, eseguire un task particolare di scansione cliccando sul tasto corrispondente. La seguente tabella elenca i task di scansione disponibili, assieme alla loro descrizione:

Task	Descrizione
Scansione sistema	Esamina l'intero sistema, esclusi gli archivi, per tutti i tipi di malware ad eccezione dei rootkit.
Scansione approfondita	Esamina l'intero sistema,per tutti i tipi di malware che minacciano la sicurezza del vostro sistema, come virus, spyware, adware, rootkits ed altri.

Nota

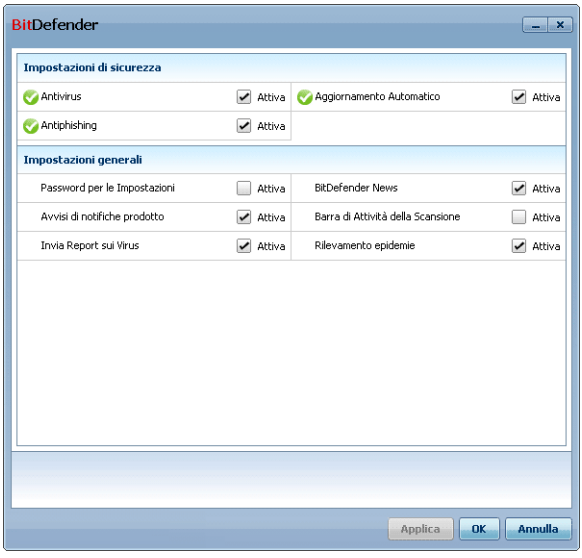
Poiché le funzioni **Scansione approfondita** e **Scansione sistema** analizzano l'intero sistema, la scansione può richiedere un po' di tempo.

Quando si esegue una Scansione del Sistema o una Scansione Approfondita del Sistema apparirà l'assistente Scansione Antivirus. Seguire la procedura di tre passi per completare il processo di scansione. Per ulteriori informazioni sulla procedura guidata, far riferimento a «*Procedura guidata scansione antivirus*» (p. 37).

11. Configurazione delle Impostazioni di base

È possibile configurare le impostazioni principali del prodotto dalla finestra delle impostazioni fondamentali. Per aprirla, seguire una delle seguenti procedure:

- Aprire BitDefender e fare clic sul pulsante **Impostazioni** in alto a destra.
- Fare clic con i pulsante di destra sulla icona BitDefender nella barra delel applicazioni e selezionare **Impostazioni fondamentali**.



Impostazioni di base

Le impostazioni sono suddivise in due categorie:

- Impostazioni sulla sicurezza
- Impostazioni generali

Per applicare e salvare le modifiche apportate alla configurazione, fare clic su **OK**. Per chiudere la finestra senza salvare i cambiamenti, fare clic su **Elimina**.

11.1. Impostazioni di sicurezza

In questa area, è possibile abilitare o disabilitare le impostazioni del prodotto che riguardano vari aspetti della sicurezza del computer e dei dati. Lo stato attuale delle impostazioni è indicato usando una di queste icone:

Cerchio verde con un segno di spunta: L'impostazione è abilitata.

Cerchio rosso con un punto esclamativo: L'impostazione è disabilitata.

Per abilitare / disabilitare una impostazione, selezionare / deselezionare la casella di controllo **Abilita** corrispondente.

Avvertimento

Prestare molta attenzione prima di disabilitare la protezione antivirus in tempo reale o aggiornamenti automatici. Disabilitare queste funzionalità potrebbe compromettere la sicurezza del proprio computer. Se è davvero necessario disabilitarle, ricordarsi di riabilitarle appena possibile.

È possibile trovare tutto l'elenco delle impostazioni e la relativa descrizione nella seguente tabella:

Impostazione	Descrizione
Antivirus	La protezione in tempo reale assicura che tutti i file vengano scansionati quando l'utente o un'applicazione eseguita nel sistema vi accede.
Aggiornamento automatico	L'aggiornamento automatico assicura che la versione più recente del prodotto BitDefender e i file di firma vengano scaricati ed installati automaticamente e regolarmente.
Antiphishing	L'Antiphishing rileva se una pagina web è impostata per rubare informazioni personali e avverte in tempo reale.

11.2. Impostazioni generali

In questa area, è possibile abilitare o disabilitare impostazioni che influenzano il comportamento del prodotto e l'esperienza utente. Per abilitare / disabilitare una impostazione, selezionare / deselezionare la casella di controllo **Abilita** corrispondente.

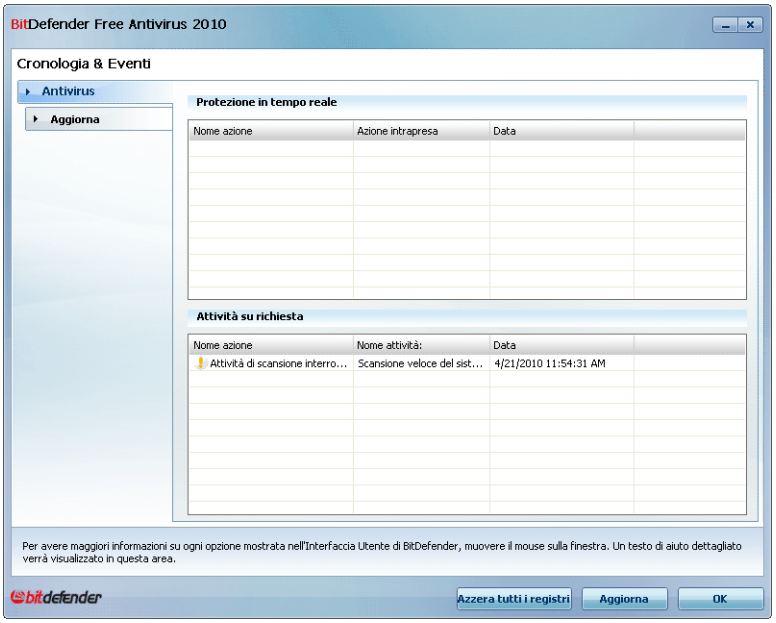
È possibile trovare tutto l'elenco delle impostazioni e la relativa descrizione nella seguente tabella:

Impostazione	Descrizione
Password delle impostazioni	Questo assicura che le impostazioni di BitDefender possano essere modificate solo da una persona che conosca questa password. Quando viene abilitata questa opzione verrà richiesto di configurare la password impostazioni. Digitare la

Impostazione	Descrizione
	password desiderata in entrambi i campi e fare clic su **OK** per impostare la password.
Notizie BitDefender	Abilitando questa opzione, riceverete da BitDefender importanti notizie sull'azienda, aggiornamenti del prodotto e notizie sulle nuove minacce per la sicurezza.
Avvisi notifiche prodotto	Abilitando questa opzione riceverete informazioni sugli allarmi.
Barra dell'Attività di scansione	La Barra dell'attività di scansione è una piccola finestra trasparente che indica l'avanzamento dell'attività dell'attività di scansione di BitDefender. Per ulteriori informazioni, far riferimento a *«Barra di Attività della Scansione»* (p. 14).
Inviare report sui Virus	Abilitando questa opzione i report sulle scansioni antivirus verranno inviati ai Laboratori BitDefender per analisi. Questi report non contengono dati confidenziali, come il vostro nome o indirizzo IP, e non verranno usati a fini commerciali.
Rilevamento di Outbreak	Abilitando questa opzione i report riguardanti potenziali outbreak di virus verranno inviati ai Laboratori BitDefender per analisi. Questi report non contengono dati confidenziali, come il vostro nome o indirizzo IP, e non verranno usati a fini commerciali.

12. Cronologia ed Eventi

Il link **Visualizza Registri** nella parte inferiore della finestra principale di BitDefender apre un'altra finestra che visualizza la cronologia e gli eventi di BitDefender. Tale finestra offre una panoramica di tutti gli eventi relativi alla sicurezza. Per esempio, potete potete controllare facilmente se l'aggiornamento è stato eseguito con successo, se è stato rilevato del malware sul vostro computer, etc.



Eventi

Per aiutarvi a filtrare la cronologia ed eventi di BitDefender, sulla sinistra sono disponibili le seguenti categorie:

- **Antivirus**
- **Aggiornamento**

Per ogni categoria c'è una lista di eventi disponibile. Ogni evento viene con la seguente informazione: una breve descrizione, l'azione intrapresa da BitDefender quando è successo, e la data ed ora in cui è successo. Se volete trovare ulteriori informazioni su un particolare evento della lista, cliccateci due volte sopra.

Fare clic su **Cancella tutti i registri** se si desidera rimuovere tutti i vecchi registri, oppure **Aggiorna** per assicurarsi di visualizzare i registri più recenti.

13. Procedure guidate

Questa capitolo descrive le procedure guidate potrebbero apparire quando si risolvono problemi o svolgono attività specifiche con BitDefender.

13.1. Procedura guidata scansione antivirus

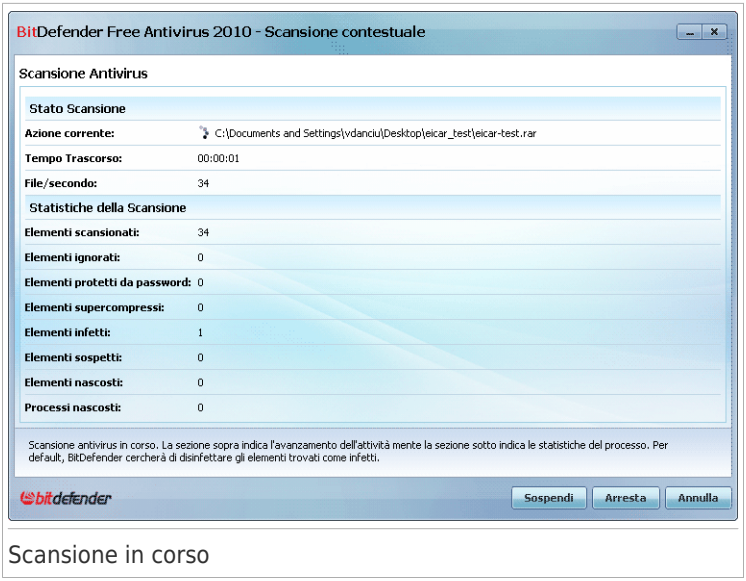
Ogni volta che si inizia una scansione su richiesta (ad esempio, facendo clic con il tasto destro su una cartella e selezionando **Scansiona con BitDefender**), apparirà l'assistente Scansione Antivirus BitDefender. Seguire la procedura di tre passi per completare il processo di scansione.

Nota

Se non appare la procedura guidata di scansione, potrebbe darsi che la procedura guidata sia configurata per una esecuzione sullo sfondo. Cercare l'icona di avanzamento della scansione nella barra delle applicazioni. Clicca su questa icona per aprire un processo di scansione e visualizzarne il progresso.

13.1.1. Passo 1/3 – Scansione

BitDefender inizierà la scansione degli oggetti selezionati.



Scansione in corso

Potete visualizzare lo stato della scansione e le statistiche (velocità di scansione, tempo trascorso, numero di oggetti esaminati / infetti / sospetti / nascosti ed altro).

Attendere che BitDefender finisca la scansione.

Nota
La durata del processo dipende dalla complessità della scansione.

Archivi protetti da password. Se BitDefender rileva un archivio protetto da password durante la scansione e l'azione predefinita è **Richiedi la password**, verrà chiesto di inserire la password. Gli archivi protetti da password non possono essere esaminati a meno che non forniate la password. Sono disponibili le seguenti opzioni:

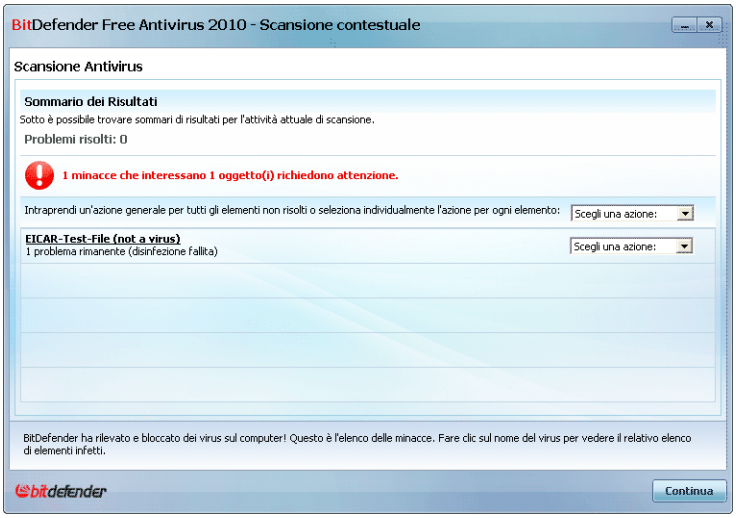
- **Desidero inserire la password per questo oggetto.** Se si desidera che BitDefender scansioni l'archivio, selezionare questa opzione e digitare la password. Se non si conosce la password, scegliere un'altra opzione.
- **Non desidero inserire la password per questo oggetto (ignora questo oggetto).** Selezionare questa opzione per non scansionare questo archivio.
- **Non desidero inserire la password per questi oggetti (ignora tutti gli oggetti protetti da password).** Selezionare questa opzione se non si vuole ricevere ulteriore domande sugli archivi protetti da password. BitDefender non sarà in grado di scansionarli, ma verranno annotati nel registro della scansione.

Fare clic su **OK** per continuare la scansione.

Arresto o messa in pausa della scansione. Potete fermare la scansione in qualsiasi momento, cliccando su **Fermare**. Verrete portati all'ultimo passo dell'assistente. Per interrompere temporaneamente il processo di scansione, cliccare semplicemente su **Pausa**. Per riprendere la scansione dovrete cliccare su **Continuare**.

13.1.2. Passo 2/3 – Selezionare Azioni

Una volta completato il processo di scansione, apparirà una nuova finestra, dove potrete visualizzare i risultati della scansione.



Azioni

Si potrà vedere il numero di problemi che colpiscono il vs. sistema.

Gli oggetti infetti vengono mostrati in gruppi in base al malware con il quale sono stati infettati. Cliccare sul link corrispondente alla minaccia per trovare più informazioni sugli oggetti infetti.

Potete scegliere di intraprendere un'azione globale per tutti i problemi oppure selezionare azioni separate per ogni gruppo di problemi.

Una o più delle seguenti opzioni possono apparire nel menu:

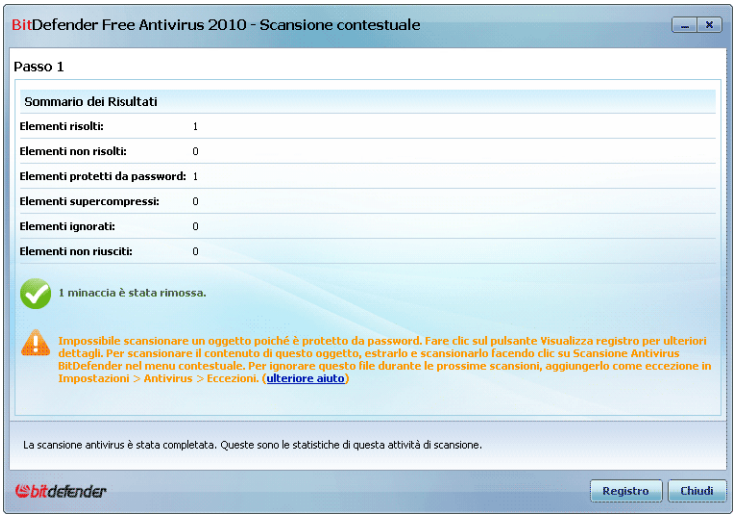
Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file rilevati. Dopo che la scansione sia stata completata, potrete aprire il log di scansione per visualizzare le informazioni su questi file.
Disinfettare	Rimuove il codice malware da file infetti.
Eliminare	Elimina i file infetti.
Sposta in quarantena	Sposta i file infetti nella quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

Azione	Descrizione
Rinomina i files	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono. Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

Cliccare su **Continuare** per applicare le azioni specificate.

13.1.3. Passo 3/3 – Visualizzare risultati

Quando BitDefender completa la risoluzione dei problemi, i risultati della scansione appariranno in una nuova finestra.



Riassunto

E' possibile visualizzare il sommario dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza registro** per visualizzare il registro di scansione.

Importante
Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

13.2. Assistente Scansione Programmata

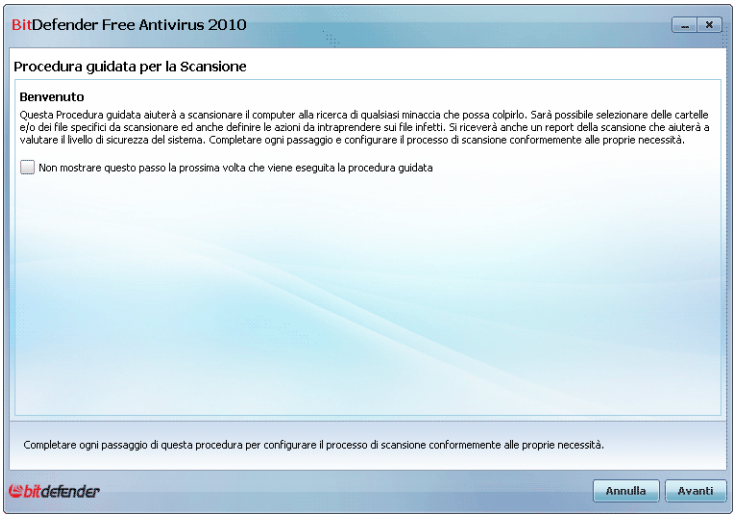
L'Assistente Scansione Programmata vi permette di creare ed eseguire un'attivitàdi scansione personalizzata e di salvarla opzionamente come Attività Veloce.

Per eseguire un'attività di scansione personalizzata utilizzando l'Assistente Scansione Programmata, è necessario seguire questi passi:

1. Apri BitDefender.
2. Andare alla scheda **Antivirus**.
3. Nell'area Funzioni Rapide, clicca **Scansione Programmata**.
4. Seguire i sei passi della procedura guidata per completare il processo di scansione.

13.2.1. Passo 1/6 - Finestra di Benvenuto

Questa è una finestra di benvenuto.



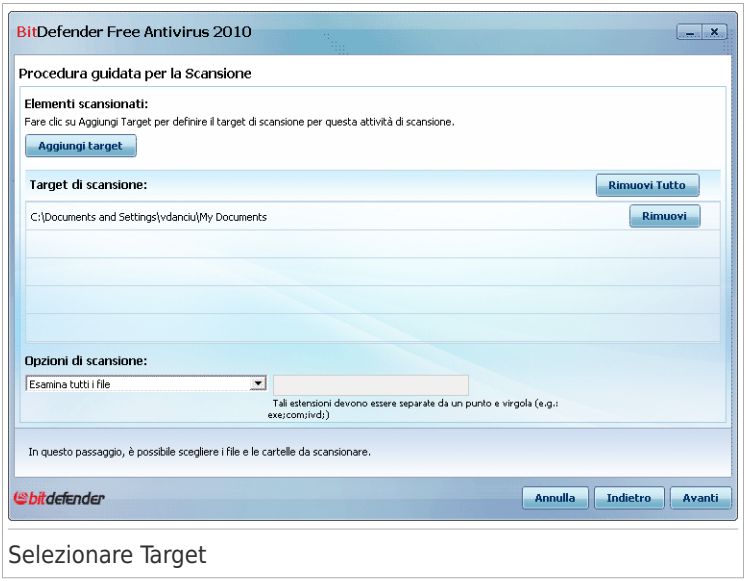
Finestra di benvenuto

Se si desidera ignorare questa finestra quando si esegue di nuovo l'assistente in futuro, selezionare la casella di controllo **Non mostrare questo passo la prossima volta che viene eseguito l'assistente**.

Selezionare **Avanti**.

13.2.2. Passo 2/6 - Selezionare Target

Qui è possibile specificare i file o le cartelle da scansionare, nonché le opzioni di scansione.



Selezionare Target

Fare clic su **Aggiungere Target**, selezionare i file o le cartelle che si desidera scansionare e fare clic su **OK**. I percorsi alle posizioni selezionate appariranno nella colonna **Target di scansione**. Se si cambia idea circa la locazione, sarà sufficiente fare clic sul pulsante **Rimuovere** vicino. Fare clic sul pulsante **Rimuovi Tutto** per rimuovere tutte le posizioni aggiunte all'elenco.

Quando si è conclusa la selezione delle posizioni, impostare le **Opzioni di Scansione**. Sono disponibili le seguenti opzioni:

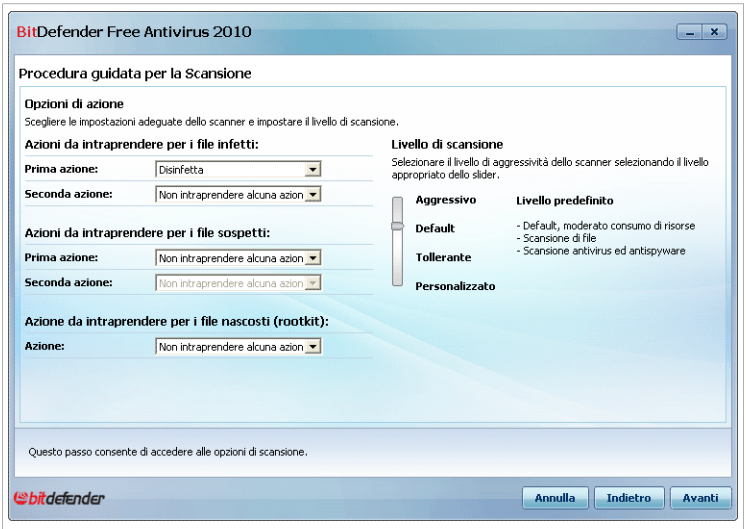
Opzione	Descrizione
Tutti i file	Selezionare questa opzione per esaminare tutti i file nelle cartelle desiderate.

Opzione	Descrizione
Scansiona solo i file con estensioni di applicazione	Verranno esaminati solo i file di programma. Questo significa solo i file con le seguenti estensioni: .exe; .bat; .com; .dll; .ocx; .scr; .bin; .dat; .386; .vxd; .sys; .wdm; .cla; .class; .ovl; .ole; .exe; .hlp; .doc; .dot; .xls; .ppt; .wbk; .wiz; .pot; .ppa; .xla; .xlt; .vbs; .vbe; .mdb; .rtf; .htm; .hta; .html; .xml; .xtp; .php; .asp; .js; .shs; .chm; .lnk; .pif; .prc; .url; .smm; .pdf; .msi; .ini; .csc; .cmd; .bas; .eml e .nws.
Esamina solo le estensioni definite dall'utente	Verranno esaminati soltanto i file con le estensioni specificate dall'utente. Le varie estensioni devono essere separate da ";".

Selezionare **Avanti**.

13.2.3. Passo 3/6 - Selezionare Azioni

Qui è possibile specificare le impostazioni dello scanner e il livello di scansione.



Selezionare Azioni

- Selezionare le azioni da intraprendere sui file infetti e sospetti rilevati. Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file infetti. Questi file appariranno nel file di rapporto.
Disinfetta i file	Rimuovere il codice malware dai file infetti rilevati.
Cancella i file	Cancella immediatamente i file infetti, senza alcun avviso.
Muova i files in Quarantena	Sposta i file infetti nella zona di quarantena. I file in quarantena non possono essere eseguiti nè aperti; così il rischio di infezione sparisce.

- Selezionare l'azione da intraprendere sui file nascosti (rootkit). Sono disponibili le seguenti opzioni:

Azione	Descrizione
Non eseguire alcuna Azione	Nessuna azione verrà eseguita sui file nascosti. Questi file appariranno nel file di report.
Rinomina	Cambia il nome di file nascosti aggiungendo `.bd.ren` al loro nome. Come risultato, si potrà cercare tali file sul computer, se ve ne sono. Notare che i file nascosti non sono i file che l'utente ha nascosto in modo deliberato da Windows. Sono file nascosti da programmi speciali, noti come rootkit. I rootkit non sono file di tipo nocivo. Tuttavia sono utilizzati per rendere introvabili virus o spyware per normali programmi antivirus.

- Configurare l'aggessività dello scanner. Vi sono 3 livelli da cui scegliere. Trascinare il selettore lungo la scala per impostare il livello di protezione più adeguato:

Livello di scansione	Descrizione
Permissiva	Vengono esaminate solo le applicazioni e solo alla ricerca di virus. Il livello di consumo delle risorse è basso.
Default	Il livello di consumo delle risorse è moderato. Vengono analizzati tutti i file alla ricerca di virus e spyware.
Aggressiva	Vengono esaminati tutti i file (inclusi gli archivi) alla ricerca di virus e spyware. I file nascosti e i processi

Livello di scansione	Descrizione
	sono inclusi nella scansione. Il livello di consumo delle risorse è elevato.

Gli utenti più esperti possono trarre vantaggio dalle impostazioni di scansione offerte da BitDefender. Lo scanner può essere impostato per la ricerca di minacce malware specifiche. Questo può ridurre considerevolmente i tempi di scansione e migliorare i tempi di risposta del computer durante la scansione.

Trascinare il selettore per selezionare **Personalizzazione** quindi fare clic sul pulsante **Livello di Personalizzazione**. Apparirà una finestra. Specificare il tipo di malware per cui si desidera che BitDefender compia una scansione selezionando le opzioni appropriate:

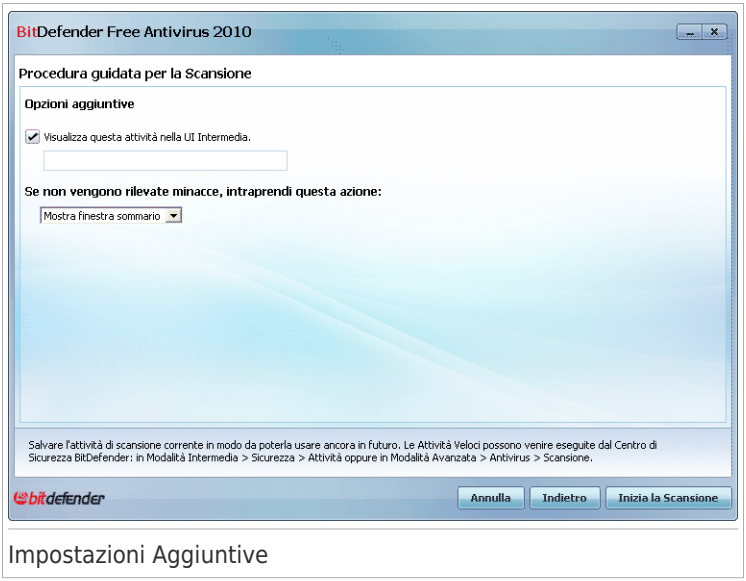
Opzione	Descrizione
Scansione Virus	Esamina per virus conosciuti. BitDefender rileva anche virus incompleti, rimuovendo ogni possibile minaccia che possa colpire la sicurezza del vostro sistema.
Scansione adware	Esegue la scansione per minacce adware. Questi file verranno trattati come file infetti. Software che includono componenti adware potrebbero bloccarsi se questa opzione è attiva.
Scansione spyware	Esegue la scansione per minacce spyware conosciuti. Questi file verranno trattati come file infetti.
Scansiona alla ricerca di applicazioni	Cerca applicazioni legittime che possono essere usate come strumenti per spiare, per nascondere applicazioni maligne o per altri intenti maligni.
Scansione dialers	Esegue la scansione per applicazioni che utilizzano numeri di telefono a costo elevato. Questi file verranno trattati come file infetti. Software che includono componenti dialer potrebbero bloccarsi se questa opzione fosse attiva.
Scansione per i Rootkits	Esegue la scansione per oggetti nascosti (file e processi), generalmente conosciuti come rootkits.
Scansiona alla ricerca di keylogger	Scansiona applicazioni malevole che registrano i tasti premuti.

Selezionare **OK** per chiudere la finestra.

Selezionare **Avanti**.

13.2.4. Passo 4/6 - Impostazioni Aggiuntive

Prima dell'avvio della scansione sono disponibili alcune opzioni aggiuntive:



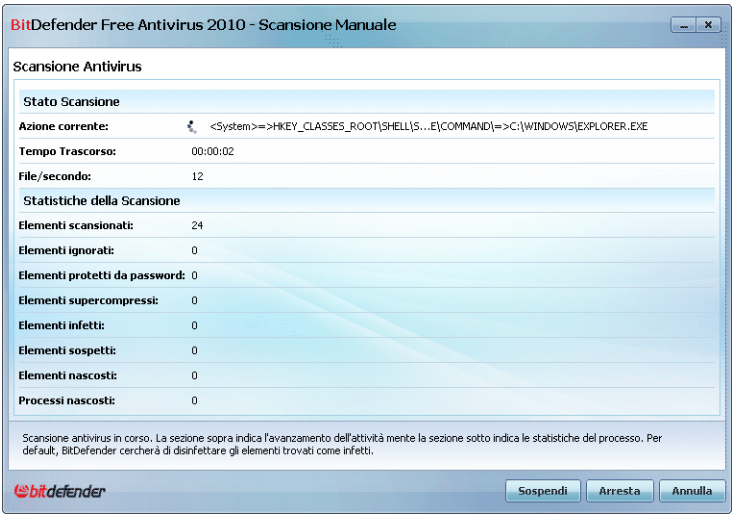
Impostazioni Aggiuntive

- Per salvare l'attività personalizzata che si sta creando per l'uso in futuro, selezionare la casella di controllo **Mostra questa attività nell'Interfaccia Utente Intermedia** ed inserire il nome dell'attività nel campo di immissione fornito.
- Dal menù corrispondente, selezioni l'azione da intraprendere nel caso non siano state riscontrate minacce.

Fare clic su **Avvia Scansione**.

13.2.5. Passo 5/6 - Scansione

BitDefender inizierà la scansione degli oggetti selezionati:



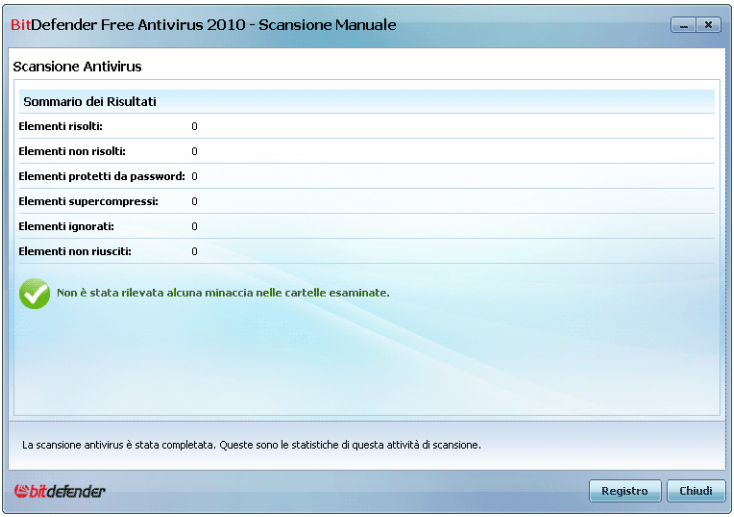
Scansione in corso

Nota

La durata del processo dipende dalla complessità della scansione. Facendo clic sull'icona di avanzamento della scansione nell'area di notifica si aprirà la finestra di scansione e sarà possibile osservare l'avanzamento della scansione.

13.2.6. Passo 6/6 – Visualizzare Risultati

Quando BitDefender completa il processo di scansione, i risultati della scansione verranno visualizzati in una nuova finestra:



Riassunto

Viene visualizzato il riepilogo dei risultati. Se si desiderano informazioni esaurienti sul processo di scansione, fare clic su **Visualizza Registro** per visualizzare il registro di scansione.

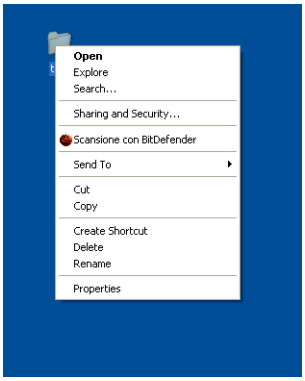
Importante
Se richiesto, vi preghiamo di riavviare il sistema per completare il processo di pulizia.

Cliccare su **Chiudere** per chiudere la finestra.

Integrazione in Software Windows e di terzi

14. Integrazione nel Menu Contestuale Windows

Il menu contestuale Windows appare ogni volta che si fa clic con il pulsante destro su un file o una cartella del computer o un oggetto sul desktop. BitDefender si integra nel menu contestuale Windows per aiutare a scansionare file in cerca di virus. È possibile individuare una opzione BitDefender sul menu contestuale cercando l'icona BitDefender.



Menu Contestuale Windows

È semplice eseguire la scansione di file, cartelle e persino dischi rigidi interi utilizzando il menu contestuale Windows. Fare clic con il pulsante destro del mouse sull'oggetto che si desidera scansionare e selezionare dal menu **Scansiona con BitDefender**. La procedura guidata di Scansione apparirà e vi guiderà attraverso il processo di scansione.

Opzioni di scansione. Le opzioni di scansione sono preconfigurate per i migliori risultati di scansione. Se vengono individuati fili infetti, BitDefender cercherà di disinfettarli (rimuovere il codice malware). Se la disinfettazione non riesce, la procedura guidata Antivirus Scan consentirà di specificare altre azioni da intraprendere sui file infetti.

Nota
Le opzioni di scansione sono standard e non è possibile modificarle.

15. Integrazione nei Web Browser

BitDefender vi protegge da tentativi di phishing mentre navigate in Internet. Esamina i siti web visitati e vi allerta se ci sono minacce di phishing. Può essere configurata una White List di siti web che non vogliate vengano esaminati da BitDefender.

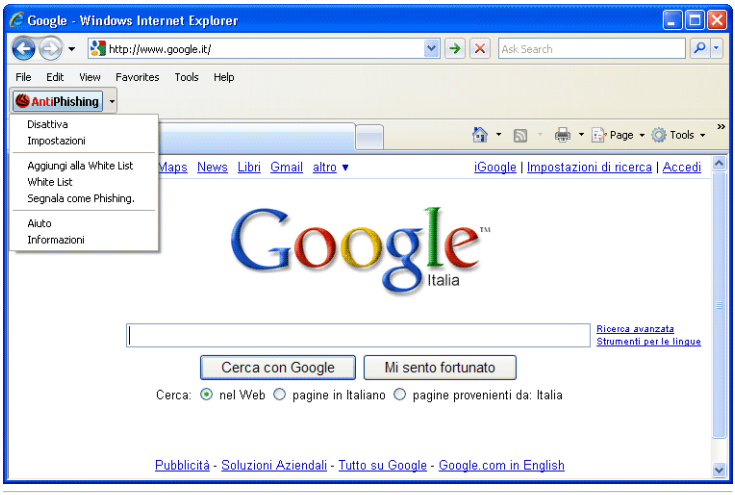
BitDefender si integra direttamente attraverso una barra degli strumenti intuitiva e di facile uso nei seguenti web browser:

- Internet Explorer
- Mozilla Firefox

Potete gestire facilmente ed efficacemente la protezione antiphishing e la White List utilizzando la barra degli strumenti Antiphishing BitDefender integrata nei web browser citati sopra.

La barra degli strumenti antiphishing, rappresentata dall'icona BitDefender, si trova nella parte superiore del browser. Cliccare sopra per aprire il menu della barra degli strumenti.

Nota
Se non potete visualizzare la barra degli strumenti, aprire il menu **Visualizzare**, puntare su **Barre degli strumenti** e selezionare **Barra degli strumenti BitDefender**.



Barra degli Strumenti Antiphishing

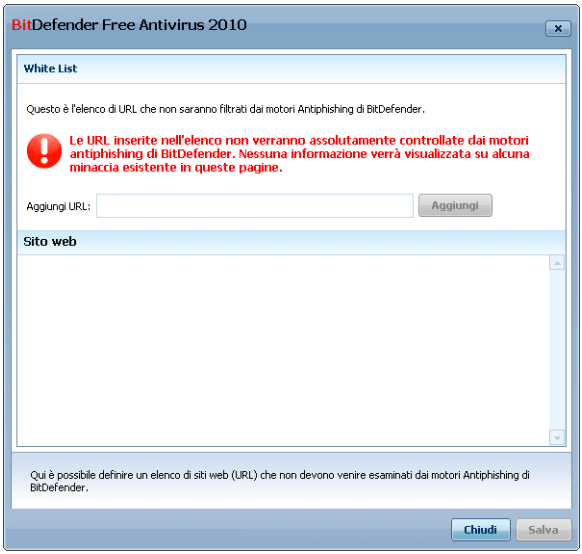
Nella barra degli strumenti sono disponibili i seguenti comandi:

- **Attivare / Disattivare** - attiva / disattiva la protezione Antiphishing di BitDefender nel browser web attuale.
- **Impostazioni** - apre una finestra dove potete specificare le impostazioni della barra degli strumenti Antiphishing. Sono disponibili le seguenti opzioni:
  - **La protezione Web Antiphishing in tempo reale** - individua e avverte in tempo reale se un sito web è oggetto di phishing (impostato per rubare informazioni personali). Questa opzione controlla la protezione antiphishing BitDefender solo nel browser web attuale.
  - **Chiedere prima di aggiungere alla White List** - vi viene chiesto prima di aggiungere un sito web alla White List.
- **Aggiungere alla White List** - aggiunge il sito web corrente alla White List.

Nota

Aggiungere un sito alla White List significa che BitDefender non esaminerà più il sito per tentativi di phishing. Vi consigliamo di aggiungere alla White List solo siti di cui vi fidate pienamente.

- **White List** - apre la White List.



White List Antiphishing

Potete vedere la lista di tutti i siti web che non vengono controllati dai motori di antiphishing BitDefender. Se si vuole rimuovere un sito dalla White List in modo

che sia notificata qualsiasi minaccia di phishing su quella pagina, fare clic sul pulsante **Rimuovi** a fianco.

Potete aggiungere i siti di cui vi fidate pienamente alla White List, in modo che non verranno più esaminati dai motori antiphishing. Per aggiungere un sito alla White List, inserire il suo indirizzo nel campo corrispondente e quindi cliccare **Aggiungere**.

- **Segnala come phishing** - informa il Laboratorio BitDefender che si considera il relativo sito web come sito usato per phishing. Segnalando siti web di phishing si aiuta a proteggere altri da furti di identità.
- **Aiuto** - apre la documentazione elettronica.
- **Informazioni** - apre una finestra nella quale è possibile visualizzare delle informazioni su BitDefender e cercare aiuto nel caso in cui accada qualcosa di inaspettato.

Risoluzione dei problemi e aiuto

16. Risoluzione dei problemi

In questo capitolo vengono spiegati alcuni problemi che si possono incontrare utilizzando BitDefender e vengono inoltre fornite possibili soluzioni per questi problemi.

16.1. Problemi di installazione

Quest'articolo permette di risolvere i problemi di installazione più comuni di BitDefender. Tali problemi possono essere raggruppati nelle seguenti categorie:

- Errori di convalida dell'installazione: non è possibile eseguire l'assistente di setup a causa di condizioni specifiche del sistema.
- Installazione non riuscita: l'installazione è stata avviata dall'assistente di setup ma non è stata completata con successo.

16.1.1. Errori di convalida dell'installazione

Quando viene avviato l'assistente di setup vengono verificate diverse condizioni al fine di convalidare la possibilità di avviare l'installazione. La tabella seguente presenta gli errori di convalida dell'installazione più comuni e le soluzioni per superarli.

Errore	Descrizione e soluzione
Non si dispone di privilegi sufficienti per installare il programma.	Per eseguire l'assistente di setup e installare BitDefender è necessario avere privilegi di amministratore. Eseguire una delle seguenti azioni: ● Accedere ad un account di amministratore di Windows ed eseguire di nuovo l'assistente di setup. ● Fare clic con il pulsante destro sul file di installazione e selezionare **Esegui come**. Digitare il nome utente e la password di un account di amministratore di Windows sul sistema.
Il programma di installazione ha individuato una versione precedente di BitDefender che non è stata disinstallata correttamente.	BitDefender era precedentemente installato sul sistema, ma l'installazione non è stata rimossa completamente. Questa condizione blocca la nuova installazione di BitDefender.

Errore	Descrizione e soluzione
	Per risolvere questo errore ed installare BitDefender, seguire questi passi: 1. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer. 2. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore. 3. Riavviare il computer. 4. Avviare di nuovo l'assistente setup per installare BitDefender.
Il prodotto BitDefender non è compatibile con il sistema operativo.	Si sta cercando di installare BitDefender su un sistema operativo non supportato. Controllare i *«Requisiti del sistema» (p. 2)* per scoprire su quali sistemi operativi è possibile installare BitDefender. Se il sistema operativo è Windows XP con Service Pack 1 o senza alcun service pack, è possibile installare il Service Pack 2 o superiore e quindi eseguire di nuovo l'assistente di setup.
Il file di installazione è progettato per un tipo diverso di processore.	Se viene ricevuto tale errore, significa che si sta tentando di eseguire una versione non corretta del file di installazione. Esistono due versioni del file di installazione di BitDefender: una per processori a 32 bit e l'altra per processori a 64 bit. Per assicurarsi di avere la versione corretta per il proprio sistema, scaricare il file di installazione direttamente da www.bitdefender.it.

16.1.2. Installazione non riuscita

Vi sono diverse possibilità di installazione non riuscita:

- Durante l'installazione appare una schermata di errore. Potrebbe essere richiesto di annullare l'installazione oppure potrebbe esservi un pulsante per avviare lo strumento di disinstallazione in modo da pulire il sistema.

Nota
Immediatamente dopo aver avviato l'installazione si potrebbe ricevere una notifica di spazio libero insufficiente su disco per l'installazione di BitDefender. In tal caso liberare lo spazio richiesto sulla partizione dove si desidera installare BitDefender e quindi riprendere o riavviare l'installazione.

- L'installazione si blocca e il sistema potrebbe congelarsi. Solo un riavvio ripristina la capacità di rispondere del sistema.
- L'installazione è stata completata ma è impossibile utilizzare alcune o tutte le funzioni di BitDefender.

Per risolvere un'installazione non riuscita ed installare BitDefender, seguire questi passi:

1. **Ripulire il sistema dopo l'installazione non riuscita.** Se l'installazione non riesce, alcuni file e alcune chiavi di registro di BitDefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di BitDefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema. Per questa ragione è necessario rimuoverle prima di tentare nuovamente di installare il prodotto.

   Se la schermata di errore fornisce un pulsante per avviare lo strumento di disinstallazione, fare clic su tale pulsante per ripulire il sistema. Altrimenti procedere nel modo seguente:

   a. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer.

   b. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore.

   c. Riavviare il computer.

2. **Controllare le possibili cause per il fallimento dell'installazione.** Prima di procedere con la disinstallazione del prodotto, controllare e rimuovere le possibili condizioni che potrebbero aver causato il fallimento dell'installazione:

   a. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di BitDefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente BitDefender.

   b. È anche necessario controllare che il sistema non sia infetto. Aprire Internet Explorer, andare su www.bitdefender.it ed eseguire una scansione on-line (fare clic sul pulsante **scansiona ora**).

3. Riprovare ad installare BitDefender. Si raccomanda di scaricare ed eseguire la versione più recente del file di installazione da www.bitdefender.it.

16.2. I servizi BitDefender non rispondono

Questo articolo aiuta a risolvere i problemi nel caso in cui *I servizi BitDefender non funzionano*. Si potrebbe trovare questo errore:

- L'icona BitDefender nell'area di notifica è grigia e un pop-up informa che i servizi BitDefender non rispondono.
- La finestra BitDefender mostra che i servizi BitDefender non stanno rispondendo.

L'errore potrebbe essere causato da una delle seguenti condizioni:

- Si sta installando un aggiornamento importante.
- errori temporanei di comunicazione tra i servizi di BitDefender.
- alcuni servizi di BitDefender sono arrestati.
- altri programmi di sicurezza sono in esecuzione sul computer contemporaneamente a BitDefender.
- virus presenti nel sistema stanno interferendo con il normale funzionamento di BitDefender.

Per risolvere questo errore, provare queste soluzione:

1. Aspettare alcuni momenti e vedere se qualcosa cambia. L'errore potrebbe essere temporaneo.
2. Riavviare il computer e aspettare alcuni attimi fino a quando BitDefender è caricato. Aprire BitDefender per vedere se l'errore persiste. Riavviare il computer di solito risolve il problema.
3. Controllare che non vi siano altri programmi di sicurezza installati che potrebbero interferire con il normale funzionamento di BitDefender. Se è così si raccomanda di rimuovere tutti gli altri programmi di sicurezza e quindi installare nuovamente BitDefender.
4. È anche necessario controllare che il sistema non sia infetto. Aprire Internet Explorer, andare su www.bitdefender.it ed eseguire una scansione on-line (fare clic sul pulsante **scansiona ora**).

16.3. Rimozione di BitDefender non riuscita

Questo articolo permette di risolvere gli errori che potrebbero verificarsi nella rimozione di BitDefender. Vi sono due possibili situazioni:

- Durante la rimozione appare una schermata di errore. La schermata fornisce un pulsante per avviare uno strumento di disinstallazione che pulirà il sistema.
- La rimozione si blocca e il sistema potrebbe congelarsi. Fare clic su **Annulla** per annullare la rimozione. Se questo non dovesse funzionare, riavviare il sistema.

Se la rimozione non riesce, alcuni file e alcune chiavi di registro di BitDefender potrebbero rimanere sul sistema. Tali rimanenze potrebbero impedire una nuova installazione di BitDefender. Potrebbero inoltre influenzare le prestazioni e la stabilità del sistema. Per rimuovere completamente BitDefender dal sistema è necessario avviare lo strumento di disinstallazione.

Se la rimozione non riesce con una schermata di errore, fare clic sul pulsante per avviare lo strumento di disinstallazione e ripulire il sistema. Altrimenti procedere nel modo seguente:

1. Andare su www.bitdefender.it/uninstall e scaricare il programma di disinstallazione sul computer.
2. Eseguire il programma di disinstallazione utilizzando privilegi di amministratore. Il tool di disinstallazione rimuoverà tutti i file e chiavi di registro che non siano stati rimossi durante il processo automatico di rimozione.
3. Riavviare il computer.

17. Supporto

Per supporto o ulteriori informazioni su BitDefender, utilizzi le informazioni di contatto presenti di seguito.

Compra: http://www.bitdefender.com/links/it/buy/free.html

Supporto: http://www.bitdefender.com/links/it/support/free.html

Web: http://www.bitdefender.it

Glossario

ActiveX

ActiveX è una modalità di scrittura dei Programmi affinché possano essere invocati da altri Programmi e sistemi operativi. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per generare pagine Web interattive che sembrino e si comportino come applicazioni e non come semplici pagine statiche. Con gli elementi ActiveX, gli utenti possono chiedere o rispondere a domande, adoperare dei pulsanti ed interagire in altri modi con la pagina Web. I controlli ActiveX vengono spesso scritti utilizzando il linguaggio Visual Basic.

Gli ActiveX sono noti per una totale mancanza di controlli di sicurezza; gli esperti di sicurezza dei computer scoraggiano il loro utilizzo attraverso Internet.

Adware

L' adware è spesso combinato con un' applicazione Host offerta senza spese quando l'utente accetta l'adware. Le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove si spiega il proposito della applicazione. Non viene commesa quindi alcuna offesa o scortesia.

Comunque, i pop-up di avvertimento possono rappresentare un fastidio, ed in alcuni casi degrada il funzionamento del sistema. Inoltre, l'informazione che viene raccolta da queste applicazioni può causare inconvenienti riguardo alla privacy degli utenti non completamente ben informati sui termini del'accordo di licenza.

Archivia

Disco, nastro o cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Backdoor

Breccia nella sicurezza di un programma deliberatamente implementata dal costruttore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del venditore a scopo di manutenzione.

Settore di boot

Settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Virus di boot

Virus che infetta il settore di boot di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infetto con un virus di boot, farà sì che il virus venga attivato nella memoria. Da quel momento in

poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo nella memoria.

Browser

Abbreviazione di Web browser, un'applicazione software utilizzata per localizzare e visualizzare pagine Web. I due browser più noti sono Netscape Navigator e Microsoft Internet Explorer. Entrambi sono Browser grafici, ovvero in grado di visualizzare sia grafici che testo. Inoltre, i browser più moderni possono presentare informazioni multimediali, incluso suoni e animazione, nonostante richiedano i plug-in per alcuni formati.

Linea di commando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di commando.

Cookies

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia dei vostri interessi e gusti online. In questo regno, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire direttamente ciò che si dichiara essere il proprio interesse. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Dall'altra parte, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. Comprensibilmente in questo modo nascerà un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un " SKU number" (il codice a barre sul retro delle confezioni che vengono passati alla scansione della cassa). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Disk drive

È un dispositivo che legge e scrive dei dati su un disco.

Un drive di disco rigido legge e scrive dischi rigidi.

Un drive di floppy accede i dischi floppy.

I drive di disco possono essere interni (incorporati all'interno di un computer) oppure esterni (collocati in un meccanismo separato e connesso al computer).

Download

Per copiare dati (solitamente un file intero) da un'origine principale su un dispositivo periferico. Il termine viene spesso utilizzato per descrivere un processo di copia di un documento da un servizio on-line sul computer di un utente. Si può inoltre riferire al processo di copiatura di un file da un file server di rete su un computer della rete.

E-mail

Posta elettronica. Servizio che invia messaggi ai computer attraverso reti locali o globali.

Eventi

Azione oppure avvenimento rilevato da un programma. Gli eventi possono rappresentare azioni dell'utente, come fare un clic con il mouse o premere un tasto sulla tastiera oppure avvenimenti del sistema, ad esempio memoria insufficiente.

Falso positivo

Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

Estensione del nome di un file

Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni del nome del file, come Unix, VMS e MS-DOS. Sono normalmente composti da uno a tre lettere (alcuni vecchi supporti OS non più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScipt, "txt" per testi arbitrari.

Euristico

Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche impronte dei virus. Il vantaggio della scansione euristica è di non venire ingannata dalle nuove varianti dei virus esistenti. Può comunque occasionalmente segnalare codici sospetti in programmi normali, generando "falsi positivi".

IP

Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Applet Java

Programma Java concepito per funzionare solo su pagine web. Per utilizzare un applet su una pagina web, bisognerà specificare il nome dell'applet e la dimensione (lunghezza e larghezza -in pixel) che l'applet può utilizzare. Quando si accede alla pagina web, il browser scarica l'applet dal server e lo esegue sulla macchina dell'utente (il client). Gli Applet differiscono dalle applicazioni in quanto sono governati da un rigido protocollo di sicurezza.

Ad esempio, nonostante gli applet vengano lanciati sul client, essi non possono leggere o scrivere dati nella macchina dell'utente. Inoltre, gli applet sono ulteriormente limitati in modo che possano leggere e scrivere dati solo dallo stesso dominio dai quali provengono.

Macro virus

Tipo di virus del computer codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Client mail

Un client e-mail è un'applicazione che vi consente di inviare e ricevere e-mail.

Memoria

Aree di immagazzinaggio interne nel computer. Il termine memoria identifica l'immagazzinaggio dati sotto forma di chip; la parola storage viene utilizzata per la memoria su nastri o su dischi. Ogni computer dispone di un certo quantitativo di memoria fisica, solitamente chiamata memoria principale oppure RAM.

Non euristico

Questo metodo di scansione si basa su specifiche impronte di virus. Il vantaggio della scansione non-euristica è di non essere ingannato da ciò che potrebbe sembrare un virus e non genera falsi allarmi.

Programmi impaccati

File in formato compresso. Molti sistemi operativi e molte applicazioni contengono comandi che vi consentono di impaccare un file in modo da occupare meno memoria. Ad esempio, supponiamo che abbiate un file di testo che contenga dieci caratteri spazio consecutivi. Normalmente occuperebbe dieci byte di memoria.

Un programma che impacca i file sostituirebbe gli spazi con un carattere speciale serie_di_spazi seguito dal numero di spazi sostituiti. In questo caso i dieci spazi occuperebbero solo due byte. Questa è solo una tecnica di impaccaggio – ce ne sono molte altre.

Percorso

Le esatte direzioni per raggiungere un file su un computer. Queste direzioni vengono solitamente descritte attraverso il sistema di casellario gerarchico dall'alto al basso.

La strada tra due punti qualsiasi, come ad esempio il canale di comunicazioni tra due computer.

Phishing

L'atto d'inviare una mail ad un utente fingendo di essere una ditta legittima ed affermata, nel tentativo di truffare l'utente, facendole cedere informazione privata che verrà usata per furti d'identità. La e-mail indirizza gli utenti a visitare una pagina Web, dove gli viene chiesto di aggiornare informazioni personali, come password e carte di credito, numero della previdenza sociale e del conto

in banca, che questa legittima organizzazione ha già. In ogni caso, la pagina Web è finta, e organizzata soltanto per rubare l'informazione del utente.

Virus polimorfico

Virus che modifica la propria forma con ogni file che infetta. In quanto non dispongono di caratteristiche binarie costanti, tali virus sono difficili da identificare.

Porta

Interfaccia su un computer alla quale è possibile connettere un supporto. I Personal Computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente i Personal Computer hanno porte per la connessione dei modem, delle stampanti, dei mouse e altri supporti periferici.

Nelle reti TCP/IP e UDP, un punto di arrivo ad una connessione logica. Il numero della porta identifica di che tipo di porta si tratta. Ad esempio, la porta 80 viene usata per il traffico HTTP.

File di report

File che elenca le azioni avvenute. BitDefender mantiene un file di rapporto che elenca i percorsi esaminati, le cartelle, il numero di archivi e file esaminati, quanti file infetti e sospetti sono stati trovati.

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore ad un sistema. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la loro presenza in modo da non dover essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, i login e i log. Possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche, se incorporano il software adeguato.

I rootkit non sono maligni per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando rootkit. Comunque, essi vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati al malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e log ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Spam

Posta elettronica pubblicitaria. Generalmente conosciuto come qualsiasi e-mail non richiesta.

Spyware

Accede alla connessione internet dell'utente senza che l'utente se ne accorga, normalmente a scopo pubblicitario. Le applicazioni Spyware vengono tipicamente come un componente nascosto di programmi freeware o shareware che possono essere scaricati da Internet. Tuttavia, deve essere segnalato che la maggioranza delle applicazioni shareware o freeware non arrivano con spyware. Una volta installato, lo spyware esegue il monitoraggio dell'attività dell' utente su Internet e trasmette questa informazione di nascosto a qualcun altro. Lo spyware può anche raccogliere informazione su indirizzi mail e addirittura passwords e numeri di carta di credito.

Lo spyware è simile a un Cavallo di Troia che gli utenti installano senza volere quando installano qualcos'altro. Un modo comune di diventare una vittima dello spyware è scaricare certi file peer-to-peer scambiando prodotti che sono disponibili oggi.

A parte delle questioni dell'etica e la privacy, lo spyware approfitta dell' utente usando risorse di memoria del computer "mangiandosi" larghezza di banda dal momento in cui invia informazione alla sua "casa" usando l' internet dell' utente. Dato che lo spyware sta usando memoria e risorse del sistema, le applicazioni eseguite in sottofondo (background) possono portare alla caduta del sistema o alla instabilità.

Elementi di startup

Qualsiasi file posizionato in questa cartella si aprirà quando il computer viene avviato. Ad esempio, una schermata di avvio, un file sonoro da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure programmi applicativi che possono essere elementi di startup. Normalmente in questa cartella viene posizionato un alias di un file, anziché il file stesso.

Barra di sistema

Introdotta con Windows 95, la barra delle applicazioni è situata nella barra degli strumenti di Windows (solitamente in basso vicino all'orologio) e contiene icone miniaturizzate per un semplice accesso alle funzioni di sistema, ad esempio il fax, la stampante, il modem, il volume ed altro. Fare doppio clic o fare clic con il pulsante destro su un'icona per vedere ed accedere ai dettagli e ai controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di networking largamente utilizzati su Internet che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il traffico di instradamento.

Trojan

Programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia particolarmente insidioso è un programma che dichiara di pulire i virus del vostro computer ma che al contrario introduce i virus nel vostro computer.

Il termine deriva dalla storia dell'Iliade di Omero, dove i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e catturare Troia.

Aggiorna

La nuova versione di un prodotto software o hardware creato per sostituire una versione precedente dello stesso prodotto. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul vostro computer; diversamente non sarà possibile installare l'aggiornamento.

BitDefender dispone del proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Virus

Programma o parte di codice caricato sul vostro computer senza che voi lo sappiate e che viene eseguito contro la vostra volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus del computer sono creati dall'uomo. E' relativamente facile produrre un semplice virus in grado di copiare sé stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere sé stesso attraverso le reti superando i sistemi di sicurezza.

Definizione di virus

Caratteristica binaria di un virus, utilizzata dal programma antivirus alfine di rilevare ed eliminare il virus stesso.

Worm(baco)

Programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.