MANUALE D'USO

Bitdefender CONSUMER SOLUTIONS

VPN

Bitdefender VPN

Manuale d'uso

Publication date 02/07/2024

Avvertenze legali

Bitdefender

Indice

INFORMAZIONI SU QUESTA GUIDA

Finalità e destinatari

Questa guida è intesa per tutti gli utenti di Bitdefender che hanno scelto Bitdefender VPN come proprio servizio di riferimento per garantire il proprio anonimato online cifrando tutto il traffico in entrata e in uscita sui propri PC, Mac o dispositivi mobili.

Scoprirai come configurare e utilizzare Bitdefender VPN per mantenere la tua identità e le tue attività online al sicuro da hacker, ISP e utenti malintenzionati. Apprenderai anche come ottenere il meglio da Bitdefender.

Buona lettura e speriamo che lo troverai utile.

Come usare questo manuale

Questo manuale presenta alcuni argomenti principali:

Cos'è Bitdefender VPN (pagina 4)

Iniziamo con Bitdefender VPN apprendendo di cosa si tratta e come può aiutarti a proteggerti garantendoti un completo anonimato online.

Utilizzare Bitdefender VPN (pagina 13)

Scopri come interagire con Bitdefender VPN e la sua interfaccia utente.

Bitdefender VPN Impostazioni e funzionalità (pagina 17)

Scopri maggiori informazioni sulle funzionalità e impostazioni di Bitdefender VPN.

Ottenere aiuto (pagina 30)

Dove cercare e ottenere aiuto in caso di difficoltà o problemi.

Convenzioni usate in questo manuale

Convenzioni tipografiche

Nel manuale vengono usati diversi stili di testo per migliorare la leggibilità. L'aspetto e il significato sono illustrati nella tabella sottostante.

Aspetto	Descrizione
sample syntax	Gli esempi di sintassi vengono stampati con monospaced caratteri.
https://www.bitdefender.com	I link URL indirizzano a una qualche ubicazione esterna, su server http o ftp.
documentation@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo come informazioni di contatto.
A proposito di questa guida (pagina 1)	Questo è un link interno, verso una qualche ubicazione nel documento.
filename	File e directory vengono stampati utilizzando monospaced font.
opzione	Tutte le opzioni del prodotto vengono stampate utilizzando **grassetto** caratteri.
parola chiave	Le parole chiave o le frasi importanti vengono evidenziate utilizzando **grassetto** caratteri.

Avvertenze

Le avvertenze appaiono sotto forma di note di testo, segnalate graficamente, portando alla tua attenzione ulteriori informazioni relative al paragrafo attuale.

Nota

Le note sono solo piccole osservazioni. Anche se si possono omettere, le note potrebbe fornire informazioni preziose, come una determinata caratteristica o un link verso eventuali temi collegati.

Importante

Richiede la tua attenzione e non è consigliato ignorarla. Solitamente, fornisce informazioni non critiche ma importanti.

Avvertimento

Si tratta di un'informazione critica che dovresti trattare con maggiore cautela. Se segui le istruzioni, non accadrà nulla di male. Dovresti leggerla e comprenderla, perché descrive qualcosa di estremamente rischioso.

Richiesta di commenti

Ti invitiamo ad aiutarci a migliorare il presente manuale. Abbiamo provato e verificato tutte le informazioni con la massima attenzione. Ti preghiamo di scriverci per indicarci eventuali errori che dovessi riscontrare nel manuale o suggerirci come poterlo migliorare, per aiutarci a fornirti la migliore documentazione possibile.

Segnalacelo inviando una mail a documentation@bitdefender.com. Scrivi tutte le tue e-mail relative alla documentazione in inglese in modo che possiamo elaborarle in modo efficiente.

1. COS'È BITDEFENDER VPN

La VPN funge da tunnel tra il tuo dispositivo e la rete a cui ti connetti per proteggere la tua connessione, crittografare i dati utilizzando una crittografia di livello militare e nascondere il tuo indirizzo IP ovunque tu sia. Il tuo traffico viene reindirizzato attraverso un server separato; rendendo così impossibile l'identificazione del tuo dispositivo da parte del tuo ISP, attraverso la miriade di altri dispositivi che utilizzano i nostri servizi. Inoltre, mentre sei connesso a Internet tramite Bitdefender VPN, puoi accedere a contenuti che normalmente sono limitati in aree specifiche.

> **Nota**
> Alcuni paesi censurano Internet e quindi l'utilizzo di una VPN sul loro territorio è vietato per legge. Per evitare conseguenze legali, potrebbe comparire un messaggio di avviso quando provi a utilizzare la funzionalità di Bitdefender VPN per la prima volta. Continuando a utilizzare tale funzionalità, confermi di essere a conoscenza dei regolamenti applicabili nel paese in cui ti trovi e dei rischi in cui potresti incorrere.

1.1. Protocolli di cifratura

I set di pacchetti di cifratura predefiniti abilitati sul server e sul client Hydra sono indicati di seguito. Tutti gli altri pacchetti di cifratura sono disabilitati.

Pacchetti di cifratura del client Hydra:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Nota

Il set lato server è molto più restrittivo e sia il server che il client Hydra rifiuteranno modalità diverse da GCM tramite AES. Il server Hydra assegna una priorità lato server a pacchetti di cifratura più severi e rifiuterà handshake TLS in caso di richieste di suite meno restrittive da parte di un client. L'elenco può anche essere configurato in runtime lato server.

2. ABBONAMENTI A VPN

Con Bitdefender VPN, puoi scegliere tra due tipi di abbonamento:

- Abbonamento base
- Abbonamento Premium

2.1. Abbonamento base

Bitdefender VPN ti offre 200 MB di traffico giornaliero gratuito per dispositivo per proteggere la tua connessione ogni volta che ti serve, permettendoti di connetterti da una singola località, che non può essere modificata.

L'abbonamento base è disponibile per tutti gli utenti che scaricano Bitdefender VPN.

2.2. Abbonamento Premium

Per avere accesso illimitato a tutte le funzionalità incluse in Bitdefender VPN, effettua l'upgrade alla versione Premium. Gli utenti con un abbonamento a Premium VPN attivo hanno una quantità illimitata di traffico protetto e possono connettersi a ogni nostro server in tutto il mondo.

Ci sono due piani disponibili per l'abbonamento Premium: mensile e annuale.

- Piano mensile: con questo piano, paghi i servizi Premium VPN su base mensile. Puoi interromperlo quando vuoi.
- Piano annuale: paghi in un'unica soluzione e hai accesso ai nostri servizi Premium per un anno intero.

2.3. Come passare a Premium VPN

Il modo più facile di effettuare l'upgrade alla versione Premium di Bitdefender VPN è fare clic sul pulsante **Aggiorna** nel lato inferiore dell'interfaccia principale. Scegli il modello di abbonamento che preferisci e segui le istruzioni a schermo.

Se già possiedi un codice di attivazione, segui queste istruzioni:

- **Per gli utenti Windows**
  1. Clicca sull'icona Il mio account sulla sinistra dell'interfaccia VPN.
  2. Clicca su **Aggiungi qui**.
  3. Digita il codice che hai ricevuto via e-mail, poi clicca sul pulsante **Attiva codice**.

- **Per gli utenti macOS**
  1. Clicca sull'ingranaggio nell'angolo in alto a destra dell'interfaccia VPN e seleziona **Il mio Account**.
  2. Clic **Aggiungilo qui**.
  3. Digita il codice ricevuto via e-mail, quindi fai clic su **Attiva codice** pulsante.

- **Per gli utenti Android**
  1. Tocca l'ingranaggio nell'angolo in alto a destra dell'interfaccia VPN e seleziona **Il mio Account**.
  2. Tocca **Aggiungi codice**.
  3. Digita il codice ricevuto via e-mail, quindi fai clic su **Attiva codice** pulsante.

- **Per gli utenti iOS**
  1. Tocca la ruota dentata nell'angolo in alto a destra dell'interfaccia VPN e seleziona **Il mio conto**.
  2. Rubinetto **Aggiungi codice**.
  3. Digita il codice ricevuto via e-mail, quindi fai clic su **Attiva codice** pulsante.

3. INSTALLAZIONE

3.1. Prepararsi all'installazione

Prima di installare Bitdefender VPN, completa questi passaggi preliminari per assicurarti che l'installazione funzioni senza problemi:

- Assicurati che il dispositivo su cui desideri installare Bitdefender soddisfi i requisiti di sistema. Se il dispositivo non soddisfa tutti i requisiti di sistema, Bitdefender non sarà installato, o, nel caso venisse installato, non funzionerà correttamente e causerà rallentamenti e instabilità.
  Per un elenco completo di tutti i requisiti di sistema, fai riferimento a Requisiti di sistema (pagina 8)
- Accedi al dispositivo utilizzando un account Amministratore.
- Assicurati che il dispositivo sia connesso a Internet durante l'installazione, anche se l'hai avviata da un CD/DVD. Se sono disponibili versioni più recenti dei file dell'applicazione inclusi nel pacchetto d'installazione, Bitdefender può scaricarli e installarli.

3.2. Requisiti di sistema

- **Per utenti Windows**
  - **Sistemi operativi:** Windows 7 con Service Pack 1, Windows 8, Windows 8.1 Windows 10 e Windows 11
  - **Memoria (RAM):** 1 GB
  - **Spazio disponibile su disco fisso:** 500 MB
  - **Net Framework:** versione minima 4.5.2

    Importante
    Le prestazioni del sistema potrebbero essere influenzate su dispositivi dotati di CPU di vecchia generazione.

- **Per utenti macOS**
  - **Sistema operativo:** macOS Sierra (10.12) o versione successiva
  - **Spazio disponibile su disco fisso:** 100 MB

- **Per utenti Android**
  - **Sistema operativo:** Android 5.0 o versione successiva
  - **Spazio di archiviazione:** 100 MB
  - Una connessione Internet attiva
- **Per utenti iOS**
  - **Sistema operativo:** iOS 12 o versione successiva
  - **Spazio su archiviazione su iPhone:** 50 MB
  - **Spazio di archiviazione su iPad:** 100 MB
  - Una connessione Internet attiva

3.3. Installazione di Bitdefender VPN

Per avviare l'installazione, segui le istruzioni relative al sistema operativo in uso:

- **Per utenti Windows**
  1. Per avviare l'installazione di Bitdefender VPN su un PC Windows, inizia a scaricare il kit di installazione da https://www.bitdefender.com/solutions/vpn/download o dall'e-mail ricevuta dopo il tuo acquisto.
  2. Clicca due volte sul programma d'installazione scaricato per eseguirlo.
  3. Se appare la finestra di dialogo Controllo dell'account utente, seleziona Sì.
  4. Attendi il completamento del download.
  5. Tramite il menu a discesa del programma di installazione, seleziona la lingua per il prodotto.
  6. Seleziona la casella "Confermo di aver letto e di accettare l'Accordo di abbonamento e l'Informativa sulla privacy, poi clicca su **INIZIA L'INSTALLAZIONE**.
  7. Attendi il completamento dell'installazione.
  8. **ACCEDI** con il tuo account Bitdefender Central. Se non hai un account Central, clicca sul pulsante **CREA UN ACCOUNT**.

9. Seleziona **Ho un codice di attivazione** se hai acquistato un abbonamento a Premium VPN.
   In alternativa, puoi selezionare **AVVIA PROVA** per provare il prodotto gratuitamente per 7 giorni prima di decidere di pagarlo.
10. Digita il codice che hai ricevuto via e-mail, poi clicca sul pulsante **ATTIVA PREMIUM**.
11. Dopo una breve attesa, Bitdefender VPN sarà installato e pronto per essere utilizzato sul tuo computer.

❍ **Per utenti macOS**

1. Per avviare l'installazione di Bitdefender VPN su macOS, inizia a scaricare il kit di installazione da https://www.bitdefender.com/solutions/vpn/download o dall'e-mail ricevuta dopo il tuo acquisto.
2. Il programma di installazione viene salvato sul Mac. Nella cartella dei download, fai doppio clic sul file del pacchetto .
3. Segui le istruzioni a schermo. Scegli **Continua**.
4. Ti guiderà attraverso i passaggi necessari per installare Bitdefender VPN sul tuo Mac. Clicca due volte sul pulsante **Continua**.
5. Dopo aver letto e accettato i termini del contratto di licenza del software, clicca su **Accetto**.
6. Clicca su **Installa**.
7. Inserisci un nome utente e una password amministratore, poi clicca su **Installa software**.
8. Riceverai una notifica con l'informazione che un'estensione di sistema firmata da Bitdefender è stata bloccata. Non si tratta di un errore, solo di un controllo di sicurezza. Clicca su **Apri preferenze di sicurezza**.
9. Clicca sull'icona a forma di lucchetto per sbloccarla.
   Inserisci un nome e una password amministratore, poi premi **Sblocca**.
10. Clicca su **Consenti** per caricare l'estensione di sistema di Bitdefender Bitdefender. Poi chiudi la finestra Sicurezza e privacy e il programma di installazione.

11. Accedi all'icona a forma di scudo sulla barra dei menu, poi **effettua l'accesso** con il tuo account Bitdefender Central. Se non hai un account Central, creane uno.

12. Se hai acquistato un abbonamento a Premium VPN, seleziona Ho un **codice di attivazione**.
    Altrimenti puoi scegliere **INIZIA LA PROVA** per testare il prodotto gratuitamente per 7 giorni prima di impegnarsi a pagarlo.

13. Digita il codice ricevuto via e-mail, quindi fai clic su **Attiva codice** pulsante.

14. Dopo una breve attesa, Bitdefender VPN sarà installato e pronto per essere utilizzato sul tuo Mac.

- **Per utenti Android**

  1. Per installare Bitdefender VPN su Android, apri l'app **Google Play Store** sul tuo smartphone o tablet.
  2. Cerca {1}{2} e seleziona questa app.
  3. Tocca il pulsante **Installa** e attendi il completamento del download.
  4. Tocca {1}Apri{2} per eseguire l'app.
  5. Seleziona la casella "Accetto l'Accordo di abbonamento e l'Informativa sulla privacy" e poi tocca **CONTINUA**.
  6. **Accedi** con il tuo account Bitdefender Central. Se non hai un account Central, tocca **Crea un account** per crearne uno.
  7. Se hai acquistato un abbonamento a Premium VPN, seleziona {1}Ho un codice di attivazione{2}.
     In alternativa, puoi selezionare Inizia la prova di 7 giorni per provare il prodotto gratuitamente per 7 giorni prima di decidere di pagarlo.
  8. Digita il codice che hai ricevuto via e-mail, poi tocca {1}Attiva codice{2}.

- **Per utenti iOS**

  1. Per installare Bitdefender VPN su iOS, prima apri l'**App Store** sul tuo iPhone o iPad.

2. Cercare Bitdefender VPN e seleziona questa app.
3. Tocca l'icona **Scarica** e attendi il completamento del download.
4. Rubinetto **Aprire** per eseguire l'app.
5. Seleziona la casella **Accetto l'Accordo di abbonamento e l'Informativa sulla privacy**, poi tocca **Continua**.
6. **Accedi** con il tuo account Bitdefender Central. Se non hai un account, tocca **Crea un account** per crearne uno.
7. Tocca **Consenti** se desideri ricevere le notifiche di Bitdefender VPN.
8. Scegliere **Ho un codice di attivazione** se hai acquistato un abbonamento Premium VPN.
   Altrimenti, puoi scegliere Avvia 7 giorni di prova per testare il prodotto gratuitamente per 7 giorni prima di impegnarti a pagarlo.
9. Digita il codice ricevuto via e-mail, quindi tocca **Attiva il codice**.

4. UTILIZZARE BITDEFENDER VPN

4.1. Aprire Bitdefender VPN

- **Per Windows**
  Per accedere all'**interfaccia principale di Bitdefender VPN**, usa uno dei seguenti metodi:
  - **Dalla barra di sistema**
    Clicca con il pulsante destro sull'icona a forma di scudo rosso nella barra di sistema e seleziona **Mostra** nel menu.
  - **Dall'interfaccia di Bitdefender**
    Se un prodotto di sicurezza Bitdefender come Bitdefender Total Security o Bitdefender Antivirus Plus (o altri) sono già installati sul tuo computer Windows, puoi aprire Bitdefender VPN direttamente da questi software:
    1. Clicca su **Privacy** nella barra laterale a sinistra dell'interfaccia di Bitdefender.
    2. Clicca su **Apri VPN** nel pannello VPN.
  - **Dal tuo desktop**
    Clicca due volte sull'icona di Bitdefender VPN sul desktop.
- **Per macOS**
  Puoi aprire la app Bitdefender VPN cliccando sull'icona nella barra del menu in alto a destra dello schermo.
  Se non riesci a localizzare lo scudo di Bitdefender nella barra del menu, usa Launchpad o Finder del Mac per riportarlo indietro:
  - **Da Launchpad**
    1. Premi **F4** sulla tastiera per accedere al Launchpad nel tuo Mac.
    2. Sfoglia le pagine delle app installate finché non trovi la app Bitdefender VPN. In alternativa, puoi inserire **Bitdefender VPN** in Launchpad per filtrare i tuoi risultati.
    3. Una volta trovata la app Bitdefender VPN, clicca sulla sua icona per fissarla alla barra del menu.

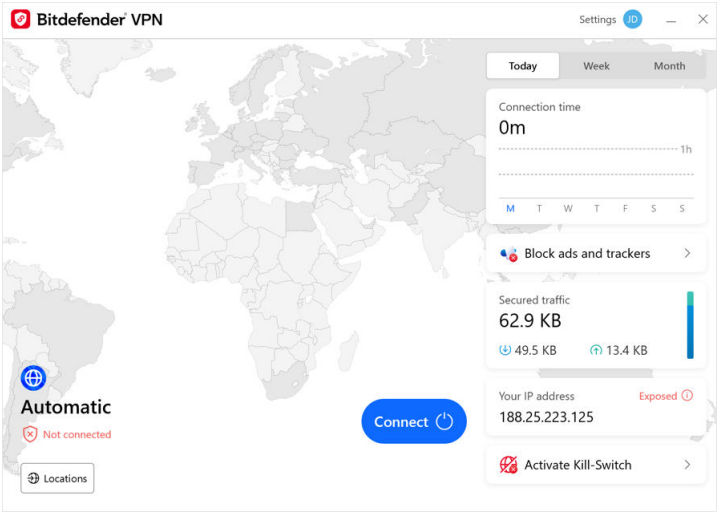
- **Da Finder**

  1. Clicca su **Finder** in basso a sinistra del Dock (Il Finder è l'icona che sembra un quadrato blu con una faccina sorridente).
  2. Poi, clicca **Vai** in alto a sinistra dello schermo nella barra del menu.
  3. Seleziona **Applicazioni** dal menu per inserire la cartella Applicazioni sul tuo Mac.
  4. Dalla cartella Applicazioni, apri la cartella **Bitdefender** e poi clicca due volte sulla app **Bitdefender VPN**.

> **Nota**
> Per accedere a Bitdefender VPN sui tuoi dispositivi mobili Android o iOS, apri semplicemente l'applicazione VPN dopo averla installata.

4.2. Come connettersi a Bitdefender VPN

L'interfaccia di VPN mostra lo stato della app: connessa o disconnessa. L'ubicazione del server per gli utenti con la versione gratuita viene impostata automaticamente da Bitdefender sul server più appropriato, mentre gli utenti premium hanno la possibilità di modificare la posizione del server a cui desiderano connettersi, selezionandola dall'elenco Posizioni virtuali. Per connettersi o disconnettersi, basta cliccare sul pulsante di accensione nell'interfaccia di VPN.



- **Per Windows:** l'icona della barra di sistema mostra una spunta di colore verde quando la VPN è connessa e una spunta di colore nero quando è disconnessa. Durante la connessione a una posizione selezionata manualmente, l'indirizzo IP viene mostrato nell'interfaccia principale.
- **Per macOS:** l'icona della barra del menu diventa nera quando la VPN è connessa e in bianco quando è disconnessa. Clicca sul pulsante circolare al centro dell'interfaccia e attendi che venga stabilita la connessione.
- **Per Android e iOS:** per connetterti a Bitdefender VPN per Android, iOS e iPadOS:
  - **Nella app Bitdefender VPN:** per connetterti o disconnetterti tocca semplicemente il pulsante di accensione nell'interfaccia di VPN. Verrà così mostrato lo stato di Bitdefender VPN.
  - **Nella app Bitdefender Mobile Security:**
    1. Accedi all'icona VPN nella barra di navigazione inferiore di Bitdefender Mobile Security.
    2. Tocca **CONNETTI** ogni volta che vuoi ottenere protezione mentre ti connetti a reti wireless non protette. Tocca

DISCONNETTI ogni volta che vuoi disattivare la connessione a VPN.

4.3. Come connettersi a un server diverso

Con un abbonamento Premium, Bitdefender VPN ti consente di connetterti a qualsiasi dei nostri server in tutto il mondo e in qualunque momento. Per farlo, dovrai:

1. Apri la app Bitdefender VPN.
2. Sul lato inferiore dell'interfaccia, tocca il pulsante **Posizione virtuale**.
3. Seleziona il paese che preferisci.
4. Nel lato inferiore dell'interfaccia, clicca sul pulsante **Connetti a [paese scelto]**.

- L'icona nella barra delle applicazioni visualizza un segno di spunta verde quando la VPN è connessa.
- L'indirizzo IP del server virtuale viene mostrato nella schermata principale mentre sei connesso a Bitdefender VPN.
- Nella dashboard principale vengono visualizzati anche un riepilogo del tempo di connessione, della quantità di traffico protetto e delle ultime 5 posizioni a cui ti sei connesso.

5. BITDEFENDER VPN IMPOSTAZIONI E FUNZIONALITÀ

5.1. Accedere alle impostazioni

Per accedere alle impostazioni di Bitdefender VPN, segui questi passaggi:

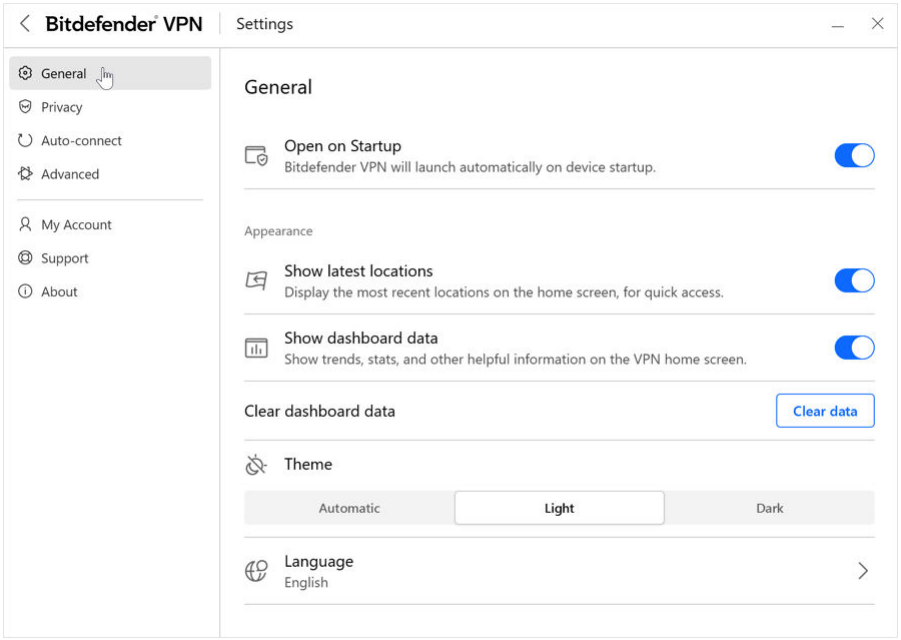
- **In Windows**
  1. Apri l'app Bitdefender VPN sul tuo dispositivo. Per farlo, clicca due volte sulla relativa icona nella barra delle applicazioni o clicca con il pulsante destro e seleziona Mostra.
  2. Sul lato sinistro dell'interfaccia, clicca sul pulsante delle **Impostazioni** (rappresentato da un ingranaggio).
- **In macOS**
  1. Per aprire l'app Bitdefender VPN sul tuo dispositivo macOS, tocca la sua icona nella barra dei menu.
  2. Nell'angolo in alto a destra dell'interfaccia di Bitdefender VPN, tocca il pulsante a forma di ingranaggio e seleziona Impostazioni.
- **Su Android**
  1. Apri la app Bitdefender VPN sul tuo dispositivo.
  2. Nell'angolo in alto a destra dell'interfaccia di Bitdefender VPN, tocca il pulsante a forma di ingranaggio.
- **Su iOS**
  1. Apri il Bitdefender VPN app sul tuo dispositivo.
  2. Fare clic sul pulsante della ruota dentata nell'angolo in alto a destra del Bitdefender VPN interfaccia.

5.2. Generale

Qui puoi modificare quanto segue:

- **Apri all'avvio**– Bitdefender VPN si avvierà automaticamente all'avvio del dispositivo.

- **Mostra le ultime posizioni**– Visualizza le posizioni più recenti sulla schermata principale, per un accesso rapido.
- **Mostra i dati del dashboard** – Mostra tendenze, statistiche e altre informazioni utili sulla schermata iniziale della VPN.
- **Cancella i dati della dashboard**– Tutti i dati della dashboard verranno cancellati e tutti i contatori verranno ripristinati.
- **Tema**– Tema chiaro/scuro
- **Lingua**– Cambia la lingua di Bitdefender VPN.
- **Notifiche**– Gestisci le tue preferenze di notifica.
- **Aiutaci a migliorare Bitdefender VPN**– Invia report anonimi sui prodotti per aiutarci a migliorare la tua esperienza.
- **Resettare tutte le impostazioni**– Ripristina la VPN alle impostazioni originali senza reinstallarla.



5.3. Caratteristiche

5.3.1. Privacy

Interruzione Internet

L'Interruzione Internet è una nuova funzionalità di Bitdefender VPN. Quando è attiva, sospende temporaneamente tutto il traffico Internet qualora la connessione VPN si interrompa. Non appena ritorni online, viene ristabilita la connessione VPN.

Per attivare l'Interruzione Internet:

- **Su Windows**
  1. Apri la app Bitdefender VPN sul tuo dispositivo cliccando due volte sulla sua icona nella barra di sistema o cliccando con il pulsante destro su di essa e selezionando **Mostra**.
  2. Clicca sul **Impostazioni** pulsante (rappresentato da una ruota dentata) sul lato sinistro dell'interfaccia.
  3. Seleziona **Avanzate**.
  4. Attiva l'opzione **Interruzione Internet**.
- **Su Android**
  1. Apri il Bitdefender VPN app sul tuo dispositivo.
  2. Fare clic sul pulsante della ruota dentata nell'angolo in alto a destra del Bitdefender VPN interfaccia.
  3. In **Impostazioni**, attiva l'opzione **Interruzione Internet**.
- **Su iOS**
  1. Apri il Bitdefender VPN app sul tuo dispositivo.
  2. Fare clic sul pulsante della ruota dentata nell'angolo in alto a destra del Bitdefender VPN interfaccia.
  3. Sotto **Impostazioni**, abilita il **Kill-Switch** opzione.

> **Nota**
> Questa funzionalità è disponibile anche per i dispositivi macOS con sistema operativo 10.15.4 o successivo.

Ad blocker e Anti-tracker

Queste funzionalità sono state sviluppate per assisterti nel mantenere la tua privacy e utilizzare il web senza pubblicità fastidiose o aziende che ti spiano. Ti aiutano a bloccare gli annunci pubblicitari e bloccare i tracker online.

Ad blocker

Ad blocker viene usato per bloccare annunci, pop-up, video pubblicità o banner mentre navighi. Ciò aiuterà i siti web a caricarsi più velocemente e ad essere più leggeri, nonché più sicuri nell'interazione.

Per attivare Ad blocker:

1. Localizza le funzionalità **Ad blocker e Antitracker** nelle **Impostazioni**.
2. Imposta l'interruttore sulla posizione **ATTIVATO**.

Anti-tracker

L'**Anti-tracker** viene usato per bloccare i tracker impostati dagli inserzionisti per seguirti e profilarti online. Alcuni siti web potrebbero non funzionare correttamente quando si bloccano i tracker, ma aggiungendo i loro URL alla whitelist dovrebbe essere possibile usarli normalmente.

Per attivare Anti-tracker:

1. Individua il **Blocco pubblicità e Antitracker** funzionalità in **Impostazioni**.
2. Sposta l'interruttore su **SU** posizione.

Whitelist

Alcuni siti web potrebbero non caricarsi correttamente se blocchi il loro codice tracker e gli annunci. Aggiungere gli URL di questi domini alla whitelist potrebbe risolvere il problema, ma ricordati che, mentre navigherai su questi siti web, visualizzerai le pubblicità e il loro codice di tracker sarà attivo.

Aggiungi i siti web a cui desideri consentire la visualizzazione delle pubblicità e l'utilizzo dei tracker:

1. Individua il **Blocco pubblicità e Antitracker** funzionalità in **Impostazioni**.

2. Clicca sul link **Gestisci**. Poi, vai nella sezione Whitelist della finestra e clicca sul link **Gestisci** corrispondente.
3. Clicca su **Aggiungi sito web** e inserisci l'URL desiderato.

5.3.2. Connetti automaticamente

Mentre sei in viaggio, lavorando in un bar o aspettando all'aeroporto, connettersi a una rete wireless pubblica per effettuare pagamenti, controllare le e-mail o gli account dei social network può essere la soluzione più rapida. Ma potrebbero esserci alcuni occhi indiscreti che cercheranno di ottenere i tuoi dati personali, sfruttando ogni falla nella rete per sottrarre informazioni.

Per proteggerti dai rischi derivanti dall'utilizzo di hotspot non sicuri o non crittografati, Bitdefender VPN include una funzionalità di connessione automatica. Questo significa che in alcune situazioni Bitdefender VPN può essere attivato automaticamente, in base alle tue preferenze e al sistema operativo che usi.

- In **Windows**, è possibile attivare la funzionalità di connessione automatica per le seguenti situazioni:
  - **Avvio:** connettiti a VPN all'avvio di Windows.
  - **Rete Wi-Fi non protetta:** usa VPN ogni volta che ti connetti a reti Wi-Fi pubbliche o non protette.
  - **App peer-to-peer:** connettiti a VPN quando avvii una app di condivisione file peer-to-peer.
  - **App e domini:** utilizza sempre VPN per determinate app e pagine web.

    Nota

    1. Clicca sul link **Gestisci**.
    2. Raggiungi l'ubicazione della app per cui vuoi utilizzare VPN, seleziona il nome della app e clicca su **Aggiungi**.

  - **Categorie siti web:** connettiti a VPN quando visiti determinate categorie di siti web. Bitdefender VPN può connettersi automaticamente per le seguenti categorie di siti web:
    - Finanza

- Pagamenti online
- Salute
- Condivisione file
- Incontri online
- Contenuti per adulti

> **Nota**
> Per ogni categoria, puoi selezionare un diverso server a cui VPN si connetterà.

- In **macOS**, è possibile attivare la funzionalità di connessione automatica per le seguenti situazioni:
  - **Avvio:** connettiti a VPN all'avvio di macOS.
  - **Wi-Fi non protetto:** Usa la VPN ogni volta che ti connetti a reti Wi-Fi pubbliche o non protette.
  - **App peer-to-peer:** Connettiti alla VPN quando avvii un'app di condivisione file peer-to-peer.
  - **Applicazioni:** connettiti sempre a VPN per determinate app.
- In **Android** e **iOS** Bitdefender VPN può essere impostato per connettersi automaticamente solo quando stai utilizzando una rete Wi-Fi pubblica o non protetta.

5.3.3. Avanzate

Split tunneling

Lo split tunneling della Virtual private network (VPN) ti consente d'indirizzare parte del traffico del tuo dispositivo o delle tue applicazioni attraverso una VPN cifrata, mentre le altre applicazioni o gli altri dispositivi avranno accesso diretto a Internet. Ciò è particolarmente utile se vuoi beneficiare di servizi che funzionano meglio quando la tua posizione è nota, ottenendo anche un accesso sicuro a comunicazioni e dati potenzialmente sensibili.

Attivando la funzionalità **Split tunneling**, le app e i siti web selezionati bypasseranno la VPN accedendo direttamente a Internet.

Per gestire le applicazioni e i siti web che bypassano la VPN:

1. Clicca sul link **Gestisci** una volta attivata la funzionalità.
2. Clicca sul pulsante **Aggiungi**.
3. Raggiungi la posizione della app in questione o inserisci l'URL del sito web desiderato, poi clicca su **Aggiungi**.

> **Nota**
> Aggiungendo un sito web, l'intero dominio, incluso tutti i sottodomini, saranno bypassati.

> **Importante**
> Nei dispositivi **macOS**, la funzionalità Split tunneling è disponibile solo per i siti web.

App Traffic Optimizer

App Traffic Optimizer di Bitdefender VPN ti consente di assegnare la priorità al traffico delle app più importanti sul dispositivo senza esporre la tua connessione a pericoli per la privacy. Le VPN reindirizzano il traffico Internet attraverso un tunnel sicuro usando potenti algoritmi di cifratura per proteggerlo.

Tuttavia, questa combinazione di tecniche può avere alcuni svantaggi, principalmente per quanto riguarda la velocità della connessione. Diversi fattori possono causare rallentamenti nella connessione, i più comuni sono la distanza dal server a cui ci si connette, la congestione della rete e l'elevato utilizzo della banda. Se hai la sensazione che a volte Bitdefender VPN causi un carico non necessario alla tua connessione e ottieni costantemente dei rallentamenti, potrebbe essere una risposta migliore alla disconnessione.

Come funziona App Traffic Optimizer?

Alcune app e determinati servizi, come piattaforme di streaming, client torrent e videogiochi, richiedono più banda. Utilizzarli costantemente potrebbe influenzare la velocità della tua connessione a Internet. Indirizzare il tuo traffico attraverso un tunnel VPN già sottopone la tua connessione a un rallentamento. Mettere a dura prova la tua connessione può seriamente degradare la tua esperienza online.

La funzionalità App Traffic Optimizer di Bitdefender VPN può aiutarti ad affrontare i rallentamenti di connessione di VPN dando la priorità alle app

di tua scelta. La funzionalità ti consente di decidere quali app dovrebbero ricevere la maggior parte del tuo traffico, successivamente assegna le risorse di conseguenza. Per esempio, se sei in una riunione e noti che la qualità della tua chiamata è scadente, App Traffic Optimizer ti consente di dare la priorità al traffico per la app di videoconferenza ottenendo risultati migliori.

In genere, gli utenti di VPN chiuderebbero tutti i processi che interferiscono sul proprio dispositivo o addirittura disattiverebbero la propria connessione VPN per ottenere una maggiore velocità di Internet. App Traffic Optimizer ti consente di ottenere una protezione alla privacy ininterrotta senza compromettere la tua velocità di connessione.

Utilizzare App Traffic Optimizer

Attualmente, la funzionalità è disponibile solo sui dispositivi Windows e ti consente di assegnare la priorità al traffico per un massimo di 3 applicazioni.

Segui questi passaggi per attivarla e configurarla senza problemi:

1. Lancia l'applicazione Bitdefender VPN sul tuo computer Windows.
2. Clicca sul pulsante nella barra laterale per accedere alle impostazioni di VPN.
3. Raggiungi la scheda **Generali** e attiva la funzionalità **App Traffic Optimizer**. Il colore dell'interruttore cambierà da grigio a blu.

Per gestire le applicazioni prioritarie per questa funzionalità

1. Clicca il**Maneggio**collegamento.
2. Raggiungi la posizione della app per la quale vuoi ottimizzare il traffico, seleziona il nome della app e clicca su **Aggiungi**. La app comparirà nella sezione **Prioritaria**.

> **Nota**
> In alternativa, se di recente hai aperto l'applicazione a cui vuoi assegnare la priorità, premi il pulsante + nella finestra App Traffic Optimizer.

3. Disconnettiti e riconnettiti a Bitdefender VPN dopo aver aggiunto o rimosso le app dall'elenco.

Per rimuovere una app da App Traffic Optimizer, clicca semplicemente sull'icona accanto al nome della app.

Nota
L'ottimizzatore del traffico dell'app non è disponibile su macOS.

Protocollo

Qui puoi scegliere il tipo di protocollo che desideri utilizzare per il trasferimento dei dati. Sono disponibili le seguenti opzioni:

- **Automatico** - Bitdefender VPN selezionerà il protocollo ottimale per il tuo dispositivo e la tua rete specifici.
- **Catapulta dell'Idra** - Veloce e sicuro, ideale per streaming e giochi.
- **OpenVPNUDP** - Ottimizzato per velocità elevate. Tuttavia, questo protocollo non è affidabile in termini di perdita di dati come altri protocolli nell'elenco.
- **Apri VPN TCP** - Progettato per l'affidabilità. Garantisce che i tuoi dati vengano consegnati interamente, ma non è veloce come OpenVPN UDP.
- **Wireguard** - Protocollo più recente, che fornisce una forte sicurezza e un elevato livello di prestazioni.

Doppio salto

Con questa funzionalità puoi gestire i server attraverso i quali inviare e crittografare doppiamente il tuo traffico internet. I tuoi dati passeranno attraverso due server VPN anziché uno, rendendo più difficile monitorare la tua attività su Internet.

Nota
Puoi aggiungere solo un totale di 5 posizioni a doppio salto. Tuttavia, puoi eliminare i doppi hop personalizzati nel tuo elenco e crearne altri in qualsiasi momento.

Importante
L'utilizzo di server situati in continenti diversi nello stesso double-hop potrebbe rallentare la velocità di connessione.

6. DISINSTALLARE BITDEFENDER VPN

La procedura di rimozione di Bitdefender VPN è simile a quella che useresti per rimuovere qualsiasi altro programma dal computer:

- **Disinstallare Bitdefender VPN dai dispositivi Windows**
  - In **Windows 7**:
    1. Clicca su **Inizia**, vai al **Pannello di controllo** e clicca due volte su **Programmi e funzionalità**.
    2. Trova **Bitdefender VPN** e seleziona **Disinstalla**.
       Attendere che il processo di disinstallazione sia terminato.
  - In **Windows 8** e **Windows 8.1**:
    1. Dal menu Start di Windows, localizza l'opzione **Pannello di controllo** (per esempio, puoi digitare direttamente "Pannello di controllo" nella finestra di ricerca del menu Start) e clicca sulla sua icona.
    2. Clicca su **Disinstalla un programma** o **Programmi e funzionalità**.
    3. Trovare **Bitdefender VPN** e seleziona **Disinstalla**.
       Attendere il completamento del processo di disinstallazione.
  - In **Windows 10** e **Windows 11**:
    1. Clicca su **Inizia** e poi su **Impostazioni**.
    2. Clicca sull'icona **Sistema** e seleziona **App installate**.
    3. Trovare **Bitdefender VPN** e seleziona **Disinstalla**.
    4. Clicca di nuovo su **Disinstalla** per confermare la tua scelta.
       Attendere il completamento del processo di disinstallazione.

- **Disinstallare dai dispositivi macOS**
  1. Clicca su **Vai** nella barra del menu e seleziona **Applicazioni**.
  2. Clicca due volte sulla cartella **Bitdefender**.
  3. Esegui **BitdefenderUninstaller**.

4. Nella nuova finestra, seleziona la casella accanto a **Bitdefender VPN**, poi clicca su **Disinstalla**.
5. Digita un nome utente e una password amministratore validi, poi clicca su **OK**.
6. Riceverai la conferma che Bitdefender VPN è stato disinstallato correttamente. Clicca su **Chiudi**.

- **Disinstallare dai dispositivi Android**
  1. Apri l'app **Play Store**.
  2. Cerca **Bitdefender VPN**.
  3. Nella pagina dello store della app Bitdefender VPN, seleziona **Disinstalla**.
  4. Conferma toccando **OK**.
- **Disinstallare dai dispositivi iOS**
  1. Mantieni il dito sulla app Bitdefender VPN.
  2. Seleziona **Elimina app**.
  3. Tocca **Elimina**.

7. DOMANDE FREQUENTI

Quando devo utilizzare Bitdefender VPN?

Devi fare sempre attenzione quando accedi, scarichi o invii contenuti su Internet. Per assicurarti di essere sempre al sicuro durante la navigazione, ti consigliamo di utilizzare la VPN quando:

- vuoi connetterti a reti wireless pubbliche
- vuoi accedere a contenuti che normalmente sono riservati a determinate aree, indipendentemente dal fatto che ti trovi a casa o all'estero
- vuoi mantenere i tuoi dati personali privati (nomi utente, password, indirizzi e-mail, informazioni della carta di credito, ecc.)
- vuoi nascondere il tuo indirizzo IP

Posso scegliere una città con Bitdefender VPN?

Sì. Attualmente, Bitdefender VPN for Windows, macOS, Android e iOS può essere utilizzato per selezionare una determinata città. Ecco l'elenco delle città attualmente disponibili:

- **Stati Uniti:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Canada:** Montreal, Toronto, Vancouver
- **Regno Unito:** Londra, Manchester

Bitdefender VPN può essere installato come app indipendente?

La app VPN viene installata automaticamente insieme alla tua soluzione di sicurezza Bitdefender. Può anche essere installata come app indipendente dalla pagina del prodotto, da Google Play Store e App Store.

Bitdefender condividerà il mio indirizzo IP e i miei dati personali con terze parti?

No, con Bitdefender VPN la tua privacy è sicura al 100%. Nessuno (agenzie pubblicitarie, ISP, compagnie d'assicurazione, ecc.) avrà accesso ai tuoi registri online.

Quale algoritmo di cifratura utilizza?

Bitdefender VPN utilizza il protocollo Hydra su tutte le piattaforme, una cifratura AES a 256 bit o la cifratura più alta disponibile supportata sia dal client che dal server, con Perfect Forward Secrecy. Ciò significa che le chiavi di cifratura vengono generate per ogni nuova sessione VPN ed eliminate dalla memoria una volta terminata la sessione.

Posso accedere a contenuti con restrizioni regionali?

Con Premium VPN hai accesso a una vasta rete di posizioni virtuali in tutto il mondo.

Avrà un impatto negativo sulla vita della batteria del mio dispositivo?

Bitdefender VPN è stato sviluppato per proteggere i tuoi dati personali, nascondere il tuo indirizzo IP mentre ti connetti a reti wireless non protette e accedere a contenuti vietati in determinati paesi. Per evitare un consumo non necessario della batteria del tuo dispositivo, ti consigliamo di utilizzare VPN solo quando ne hai bisogno e disconnetterti quando sei offline.

Perché la VPN rallenta la mia connessione a Internet?

Bitdefender VPN è stato progettato per offrirti una migliore esperienza di navigazione del web. In base alla distanza tra la tua ubicazione attuale e la posizione del server a cui scegli di connetterti, è possibile aspettarsi una certa penalizzazione nella velocità, tuttavia, è quasi sempre sufficientemente ridotta da non notarsi durante le normali attività online. Inoltre, ci affidiamo a una delle infrastrutture VPN più veloci al mondo. Se non è necessario connettersi dalla propria ubicazione a un server ospitato lontano (ad esempio dagli Stati Uniti alla Francia), ti consigliamo di consentire alla VPN di connetterti automaticamente al server più vicino o di trovare un server più vicino alla tua ubicazione attuale.

8. OTTENERE AIUTO

8.1. Richiesta d'aiuto

Bitdefender offre ai suoi clienti un livello impareggiabile di supporto rapido e accurato. Se dovessi riscontrare un qualche problema o se avessi domande sul tuo prodotto Bitdefender, potrai usare diverse risorse online per trovare una soluzione o una risposta. Allo stesso tempo, potrai contattare il servizio clienti di Bitdefender. I nostri responsabili del supporto risponderanno alle tue domande in maniera tempestiva e ti forniranno tutto l'aiuto necessario.

8.2. Risorse online

Sono disponibili diverse risorse online per aiutarti a risolvere i tuoi problemi e le tue domande relative a Bitdefender.

- Centro di supporto di Bitdefender:
  https://www.bitdefender.it/consumer/support/
- La community di esperti di Bitdefender:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Puoi anche usare il tuo motore di ricerca preferito per trovare più informazioni sulla sicurezza del computer, i prodotti Bitdefender e la società.

8.2.1. Centro di supporto di Bitdefender

Il Centro di supporto di Bitdefender è un archivio online di informazioni sui prodotti Bitdefender. Conserva, in un formato facilmente accessibile, le notifiche sui risultati delle attività di risoluzioni bug e problemi del supporto tecnico di Bitdefender e dei team di sviluppo, oltre ad articoli più generali sulla prevenzione delle minacce, la gestione delle soluzioni di Bitdefender con spiegazioni dettagliate e molti altri articoli.

Il Centro di supporto di Bitdefender è aperto al pubblico e gratuitamente esplorabile. Le ricche informazioni che contiene sono un altro modo per fornire ai clienti di Bitdefender le conoscenze tecnologiche e le

informazioni necessarie. Tutte le richieste di informazioni o i rapporti sui difetti, provenienti dai clienti di Bitdefender, prima o poi arrivano al Centro di supporto di Bitdefender, come rapporti di disinfezione, metodi per aggirare le truffe, o articoli informativi, per integrare i file di aiuto dei prodotti.

Il Centro assistenza di Bitdefender è disponibile in qualsiasi momento al seguente indirizzo: https://www.bitdefender.it/consumer/support/.

8.2.2. La community di esperti di Bitdefender

La community di esperti è un ambiente in cui gli utenti di Bitdefender, oltre a fan e appassionati, possono interagire, scambiare idee, supportarsi a vicenda e condividere le proprie conoscenze e soluzioni. È anche un luogo creativo e fornisce feedback preziosi ai nostri team di sviluppo. I membri della community sono utenti esperti di Bitdefender, felici di aiutare altri utenti nel proprio tempo libero. Grazie al loro immenso contributo e sforzi volontari, abbiamo creato una knowledge base dove gli utenti possono trovare risposte e aiuto, ma con un tocco più umano di una semplice risposta automatizzata.

Qui potrai trovare molte conversazioni utili con utenti che utilizzano Bitdefender sui propri dispositivi. La community offre una vera connessione con i nostri membri e fa sentire la loro voce. Ti invitiamo a parteciparvi sapendo che la tua opinione e le tue informazioni saranno rispettate e apprezzate. In qualità di fornitore stimato, ci sforziamo di offrire un livello senza precedenti di supporto sempre rapido e preciso, sperando di avvicinare sempre più i nostri utenti. Abbiamo progettato la nostra community con questo obiettivo sempre in mente.

Puoi trovare la pagina web della nostra community di esperti qui:

https://community.bitdefender.com/en/

8.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia include tutte le informazioni necessarie sulle minacce informatiche più recenti. È anche dove gli esperti Bitdefender condividono trucchi e suggerimenti su come restare protetti da hacker, violazioni, furti d'identità e tentativi d'impersonificazione dei social.

La pagina web di Bitdefender Cyberpedia è disponibile qui:

https://www.bitdefender.com/cyberpedia/.

8.3. Informazioni di contatto

Una comunicazione efficiente è la chiave per un business di successo. Dal 2001 BITDEFENDER ha stabilito una reputazione indiscutibile impegnandosi costantemente per una migliore comunicazione in modo da superare le aspettative dei nostri clienti e partner. In caso di domande, non esitate a contattarci direttamente tramite il ns Centro di supporto di Bitdefender (pagina 30).

https://www.bitdefender.it/consumer/support/

8.3.1. Distributori locali

I distributori locali di Bitdefender sono pronti a rispondere a ogni richiesta inerente le loro zone operative, sia in ambito commerciale sia generale.

Per trovare un distributore di Bitdefender nel tuo paese:

1. Vai a https://www.bitdefender.com/partners/partner-locator.html.
2. Seleziona il tuo paese e la tua città, utilizzando le opzioni corrispondenti.

GLOSSARIO

Codice di attivazione

È una chiave unica che può essere acquistata dal rivenditore e usata per attivare un servizio o un prodotto specifico. Un codice di attivazione consente l'attivazione di un abbonamento valido per un determinato periodo di tempo e un certo numero di dispositivi. Inoltre, può anche essere utilizzato per estendere un abbonamento, a condizione che venga generato per lo stesso prodotto o servizio.

ActiveX

ActiveX è un modello per la scrittura di programmi in modo che altri programmi e il sistema operativo possano chiamarli. La tecnologia ActiveX viene utilizzata con Microsoft Internet Explorer per creare pagine Web interattive che sembrano e si comportano come programmi per computer, piuttosto che come pagine statiche. Con ActiveX, gli utenti possono porre o rispondere a domande, utilizzare pulsanti e interagire in altri modi con la pagina web. I controlli ActiveX vengono spesso scritti utilizzando Visual Basic. Active X si distingue per una completa mancanza di controlli di sicurezza; gli esperti di sicurezza informatica ne scoraggiano l'uso su Internet.

Minaccia persistente avanzata

Advanced Persistent Threat (APT) sfrutta le vulnerabilità dei sistemi per rubare informazioni importanti per consegnarle alla fonte. Grandi gruppi come organizzazioni, aziende o governi sono presi di mira da questa minaccia. L'obiettivo di una minaccia persistente avanzata è rimanere inosservato per lungo tempo essendo in grado di monitorare e raccogliere informazioni importanti senza danneggiare le macchine mirate. Il metodo utilizzato per iniettare la minaccia nella rete è attraverso un file PDF o un documento di Office che sembra innocuo in modo che ogni utente possa eseguire i file.

Adware

L'adware è spesso combinato con un'app host fornita gratuitamente a condizione che l'utente accetti l'adware. Poiché le app adware vengono generalmente installate dopo che l'utente ha accettato un contratto di licenza che stabilisce lo scopo dell'app, non viene commesso alcun reato. Tuttavia, le pubblicità pop-up possono diventare fastidiose e in alcuni casi

degradare le prestazioni del sistema. Inoltre, le informazioni raccolte da alcune di queste app possono causare problemi di privacy per gli utenti che non erano pienamente a conoscenza dei termini del contratto di licenza.

Archivio

Un disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in un formato compresso.

Porta sul retro

Un buco nella sicurezza di un sistema deliberatamente lasciato in essere da progettisti o manutentori. La motivazione di tali buchi non è sempre sinistra; alcuni sistemi operativi, ad esempio, escono dalla confezione con account privilegiati destinati all'uso da parte dei tecnici dell'assistenza sul campo o dei programmatori di manutenzione del fornitore.

Settore di avvio

Un settore all'inizio di ogni disco che identifica l'architettura del disco (dimensione del settore, dimensione del cluster e così via). Per i dischi di avvio, il settore di avvio contiene anche un programma che carica il sistema operativo.

Avvio virus

Una minaccia che infetta il settore di avvio di un disco fisso o floppy. Un tentativo di avvio da un dischetto infettato da un virus del settore di avvio causerà l'attivazione della minaccia nella memoria. Ogni volta che avvierai il tuo sistema da quel momento in poi, avrai la minaccia attiva in memoria.

Botnet

Il termine “botnet” è composto dalle parole “robot” e “network”. Le botnet sono dispositivi connessi a Internet infettati da minacce e possono essere utilizzati per inviare e-mail di spam, rubare dati, controllare da remoto dispositivi vulnerabili o diffondere spyware, ransomware e altri tipi di minacce. Il loro obiettivo è quello di infettare il maggior numero possibile di dispositivi connessi, come PC, server, dispositivi mobili o IoT appartenenti a grandi aziende o industrie.

Navigatore

Abbreviazione di browser Web, un'app software utilizzata per individuare e visualizzare pagine Web. I browser più diffusi includono Microsoft Internet Explorer, Mozilla Firefox e Google Chrome. Questi sono browser

grafici, il che significa che possono visualizzare grafica e testo. Inoltre, la maggior parte dei browser moderni può presentare informazioni multimediali, inclusi audio e video, sebbene richiedano plug-in per alcuni formati.

Attacco di forza bruta

Attacco di indovinazione della password utilizzato per irrompere in un sistema informatico inserendo possibili combinazioni di password, per lo più a partire dalla password più facile da indovinare.

Riga di comando

In un'interfaccia a riga di comando, l'utente digita i comandi nello spazio fornito direttamente sullo schermo utilizzando il linguaggio dei comandi.

Biscotti

Nell'industria di Internet, i cookie sono descritti come piccoli file contenenti informazioni su singoli computer che possono essere analizzati e utilizzati dagli inserzionisti per tenere traccia dei tuoi interessi e gusti online. In questo ambito, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di indirizzare gli annunci direttamente a ciò che hai dichiarato di essere i tuoi interessi. È un'arma a doppio taglio per molte persone perché, da un lato, è efficiente e pertinente in quanto si vedono solo annunci su ciò che ti interessa. cosa clicchi. Comprensibilmente, c'è un dibattito sulla privacy e molte persone si sentono offese dall'idea di essere viste come un "numero SKU" (sai, il codice a barre sul retro dei pacchi che viene scansionato alla cassa della drogheria) . Sebbene questo punto di vista possa essere estremo, in alcuni casi è accurato.

Cyber bullismo

Quando coetanei o estranei commettono atti violenti contro i bambini apposta per ferirli fisicamente. Per danneggiare emotivamente, gli aggressori inviano messaggi meschini o foto poco lusinghiere, isolando così le loro vittime dagli altri o sentendosi frustrate.

Dizionario Attacco

Attacchi di indovinazione della password utilizzati per irrompere in un sistema informatico inserendo una combinazione di parole comuni per generare potenziali password. Lo stesso metodo viene utilizzato per indovinare le chiavi di decrittazione di messaggi o documenti crittografati.

Gli attacchi con dizionario hanno successo perché molte persone tendono a scegliere password brevi e con parole singole facili da indovinare.

Unità disco

È una macchina che legge e scrive dati su un disco. Un disco rigido legge e scrive dischi rigidi. Un'unità floppy accede ai dischi floppy. Le unità disco possono essere interne (alloggiate all'interno di un computer) o esterne (alloggiate in una scatola separata che si collega al computer).

Scaricamento

Per copiare i dati (di solito un intero file) da una fonte principale a un dispositivo periferico. Il termine è spesso usato per descrivere il processo di copia di un file da un servizio online al proprio computer. Il download può anche riferirsi alla copia di un file da un file server di rete a un computer in rete.

E-mail

Mail elettronica. Un servizio che invia messaggi sui computer tramite reti locali o globali.

Eventi

Un'azione o un evento rilevato da un programma. Gli eventi possono essere azioni dell'utente, come fare clic su un pulsante del mouse o premere un tasto, o occorrenze di sistema, come l'esaurimento della memoria.

Exploit

Un modo per sfruttare diversi bug o vulnerabilità presenti in un computer (software o hardware). Pertanto, gli hacker possono ottenere il controllo di computer o reti.

Falso positivo

Si verifica quando uno scanner identifica un file come infetto quando in realtà non lo è.

Estensione del nome file

La parte di un nome di file, dopo il punto finale, che indica il tipo di dati memorizzati nel file. Molti sistemi operativi utilizzano estensioni di file, ad esempio Unix, VMS e MS-DOS. Di solito sono da una a tre lettere (alcuni tristi vecchi sistemi operativi non supportano più di tre). Gli esempi includono "c" per codice sorgente C, "ps" per PostScript, "txt" per testo arbitrario.

Euristico

Un metodo basato su regole per identificare nuove minacce. Questo metodo di scansione non si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione euristica è che non viene ingannata da una nuova variante di una minaccia esistente. Tuttavia, potrebbe occasionalmente segnalare codice sospetto nei normali programmi, generando il cosiddetto "falso positivo".

Vaso di miele

Un sistema informatico esca impostato per attirare gli hacker per studiare il modo in cui agiscono e identificare i metodi eretici che utilizzano per raccogliere informazioni di sistema. Le aziende e le aziende sono più interessate a implementare e utilizzare gli honeypot per migliorare il proprio stato di sicurezza generale.

IP

Protocollo Internet - Un protocollo instradabile nella suite di protocolli TCP/IP responsabile dell'indirizzamento IP, del routing e della frammentazione e riassemblaggio dei pacchetti IP.

Applet Java

Un programma Java progettato per essere eseguito solo su una pagina Web. Per utilizzare un'applet su una pagina Web, devi 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 da un server e la esegue sulla macchina dell'utente (il client). Le applet differiscono dalle app in quanto sono governate da un rigido protocollo di sicurezza.

Ad esempio, anche se le applet vengono eseguite sul client, non possono leggere o scrivere dati sulla macchina del client. Inoltre, le applet sono ulteriormente limitate in modo che possano solo leggere e scrivere dati dallo stesso dominio da cui sono servite.

Registratore di tasti

Un keylogger è un'app che registra tutto ciò che digiti. I keylogger non sono di natura dannosa. Possono essere utilizzati per scopi legittimi, come il monitoraggio dell'attività dei dipendenti o dei bambini. Tuttavia, vengono sempre più utilizzati dai criminali informatici per scopi dannosi (ad esempio, per raccogliere dati privati, come credenziali di accesso e numeri di previdenza sociale).

Virus a macroistruzione

Un tipo di minaccia informatica codificata come macro incorporata in un documento. Molte app, come Microsoft Word ed Excel, supportano potenti linguaggi macro. Queste app ti consentono di incorporare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Cliente di posta

Un client di posta elettronica è un'app che consente di inviare e ricevere e-mail.

Memoria

Aree di archiviazione interne nel computer. Il termine memoria identifica l'archiviazione dei dati sotto forma di chip e la parola archiviazione viene utilizzata per la memoria che esiste su nastri o dischi. Ogni computer viene fornito con una certa quantità di memoria fisica, solitamente indicata come memoria principale o RAM.

Non euristico

Questo metodo di scansione si basa su uno specifico database di informazioni sulle minacce. Il vantaggio della scansione non euristica è che non si lascia ingannare da quella che potrebbe sembrare una minaccia e non genera falsi allarmi.

Predatori online

Individui che cercano di attirare minori o adolescenti in conversazioni apposta per coinvolgerli in attività sessuali illegali. I social network sono il luogo ideale in cui i bambini vulnerabili possono essere facilmente cacciati e indotti a commettere attività sessuali, online o faccia a faccia.

Programmi confezionati

Un file in un formato di compressione. Molti sistemi operativi e app contengono comandi che consentono di comprimere un file in modo che occupi meno memoria. Ad esempio, supponi di avere un file di testo contenente dieci caratteri spazio consecutivi. Normalmente, ciò richiederebbe dieci byte di archiviazione.

Tuttavia, un programma che comprime i file sostituirà i caratteri di spazio con uno speciale carattere di serie di spazi seguito dal numero di spazi da sostituire. In questo caso, i dieci spazi richiederebbero solo due byte. Questa è solo una delle tecniche di confezionamento, ce ne sono molte altre.

Sentiero

Le indicazioni esatte per un file su un computer. Queste direzioni sono solitamente descritte per mezzo del sistema di archiviazione gerarchico dall'alto verso il basso.

Il percorso tra due punti qualsiasi, ad esempio il canale di comunicazione tra due computer.

Phishing

L'atto di inviare un'e-mail a un utente che afferma falsamente di essere un'impresa legittima e consolidata nel tentativo di indurre l'utente a cedere informazioni private che verranno utilizzate per il furto di identità. L'e-mail indirizza l'utente a visitare un sito Web in cui viene chiesto di aggiornare le informazioni personali, come password e numeri di carta di credito, previdenza sociale e conto bancario, che l'organizzazione legittima già possiede. Il sito Web, tuttavia, è fasullo e impostato solo per rubare le informazioni dell'utente.

Fotone

Photon è una tecnologia di Bitdefender innovativa e discreta, progettata per minimizzare l'impatto della tua soluzione di sicurezza sulle prestazioni del sistema. Monitorando in background l'attività del PC, crea degli schemi di utilizzo, per ottimizzare i processi di avvio e scansione.

Virus polimorfo

Una minaccia che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, queste minacce sono difficili da identificare.

Porta

Un'interfaccia su un computer alla quale puoi connettere un supporto. I PC hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, schermi e tastiere. Esternamente hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per 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.

Ransomware

Un ransomware è un programma dannoso che prova a sottrarre illecitamente denaro agli utenti bloccando i loro sistemi vulnerabili.

CryptoLocker, CryptoWall e TeslaWall sono solo alcune delle varianti che cercano di bloccare i sistemi personali degli utenti.

L'infezione può partire, aprendo e-mail di spam, scaricando gli allegati di un messaggio o installando determinate applicazioni, il tutto lasciando l'utente ignaro di ciò che sta accadendo sul suo sistema. Gli autori di ransomware puntano a colpire soprattutto gli utenti normali e le aziende.

File di rapporto

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

Rootkit

Un rootkit è una serie di strumenti software che offre accesso a livello di amministratore a 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 propria presenza in modo da non dover essere visti dai veri 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 dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere minacce o per celare la presenza di un intruso nel sistema. Se combinati alle minacce, 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 registri, 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

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuti come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessione a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un Trojan che gli utenti installano inconsapevolmente installando altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

Articoli di avvio

Qualsiasi file posizionato in questa cartella si aprirà all'avvio del computer. Ad esempio, una schermata di avvio, un file audio da eseguire quando il computer si avvia la prima volta, una agenda-calendario, oppure app che possono essere elementi di avvio. Normalmente in questa cartella viene posizionato un alias di un file, al posto del file stesso.

Abbonamento

Un accordo di acquisto che offre all'utente il diritto di utilizzare un particolare prodotto o servizio su un numero specifico di dispositivi e per un certo periodo di tempo. Un abbonamento scaduto può essere rinnovato automaticamente, utilizzando le informazioni fornite dall'utente con il primo acquisto.

Area di notifica

Introdotta con Windows 95, la barra degli strumenti è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o

clicca con il pulsante destro su un'icona per visualizzare e accedere a dettagli e controlli.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete 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 relativo traffico.

Minaccia

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte delle minacce è anche in grado di auto replicarsi. Tutte le minacce informatiche sono state create dall'uomo. È relativamente facile produrre una semplice minaccia in grado di copiare sé stessa innumerevoli volte. Persino una minaccia così semplice è pericolosa in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di minaccia ancora più pericolosa è quella in grado di trasmettere sé stessa attraverso le reti superando i sistemi di sicurezza.

Aggiornamento delle informazioni sulle minacce

Lo schema binario di una minaccia, usato dalla soluzione di sicurezza per rilevare ed eliminare la minaccia.

Troiano

Un programma distruttivo che si maschera da applicazione benevola. A differenza di programmi software dannosi e worm, i trojan non si replicano ma possono essere altrettanto distruttivi. Un tipo di minaccia Trojan particolarmente insidiosa è un programma che dichiara di pulire le minacce dal computer, ma al contrario le introduce.

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, durante la notte, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Aggiornamento

Una 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 computer; diversamente non sarà possibile installare l'aggiornamento.

Bitdefender dispone della propria funzionalità di aggiornamento, che consente la verifica manuale degli aggiornamenti, oppure l'aggiornamento automatico del prodotto.

Virtual Private Network (VPN)

È una tecnologia che consente una connessione diretta temporanea e cifrata a una determinata rete su una rete meno sicura. In questo modo, la ricezione e l'invio dei dati sono sempre sicuri e cifrati, ma soprattutto più difficili da intercettare dai pirati informatici. Una prova di sicurezza è l'autenticazione, che può essere fatta solo usando un nome utente e una password.

Verme

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