Bitdefender

VPN

ANVÄNDARMAN
UAL

Bitdefender VPN

Användarmanual

Publiceringsdatum 2022-11-21

Rättsligt meddelande

Bitdefender

Innehållsförteckning

OM DEN HÄR GUIDEN

Syfte och avsedd målgrupp

Den här guiden är avsedd för alla Bitdefender användare som har valt Bitdefender VPN som deras go-to-tjänst som ger dem anonymitet online genom att kryptera all inkommande och utgående trafik på deras PC, Mac eller mobila enheter.

Du kommer att få reda på hur du konfigurerar och använder Bitdefender VPN för att skydda din onlineidentitet och dina aktiviteter från hackare, internetleverantörer och snoopar. Du kommer att lära dig hur du blir bäst av Bitdefender.

Vi önskar dig en trevlig och användbar föreläsning.

Hur man använder den här guiden

Den här guiden är organiserad kring flera viktiga ämnen:

Vad är Bitdefender VPN (sida 3)

Kom igång med Bitdefender VPN genom att lära dig vad det är och hur det kan hjälpa dig att skydda dig själv genom att ge dig äkta anonymitet online.

Använder Bitdefender VPN (sida 12)

Lär dig hur du interagerar med Bitdefender VPN och dess användargränssnitt.

Bitdefender VPN Inställningar och funktioner (sida 16)

Lär dig mer om Bitdefender VPN inställningar och funktioner.

Få hjälp (sida 27)

Var man ska leta och var man kan be om hjälp om något oväntat dyker upp.

Konventioner som används i denna guide

Typografiska konventioner

Flera textstilar används i den här guiden för att förbättra läsbarheten. Deras aspekt och betydelse presenteras i tabellen nedan.

Utseende	Beskrivning
`sample syntax`	Syntaxexempel skrivs ut med `monospaced` tecken.
https://www.bitdefender.com	URL-länken pekar på någon extern plats, på http- eller ftp-servrar.
documentation@bitdefender.com	E-postadresser infogas i texten för kontaktinformation.
Om den här guiden (sida 1)	Detta är en intern länk till någon plats i dokumentet.
`filename`	Filer och kataloger skrivs ut med `monospaced` font.
alternativ	Alla produktalternativ skrivs ut med hjälp av **djärv** tecken.
nyckelord	Viktiga sökord eller fraser markeras med hjälp av **djärv** tecken.

Förmaningar

Förmaningarna är anteckningar i texten, grafiskt markerade, som uppmärksammar dig på ytterligare information relaterad till det aktuella stycket.

Notera

Anteckningen är bara en kort observation. Även om du kan utelämna det, kan anteckningarna ge värdefull information, som specifik funktion eller en länk till något relaterat ämne.

Viktig

Detta kräver din uppmärksamhet och rekommenderas inte att hoppa över det. Vanligtvis ger den icke-kritisk men betydande information.

Varning

Detta är viktig information som du bör behandla med ökad försiktighet. Inget dåligt kommer att hända om du följer anvisningarna. Du bör läsa och förstå den, för den beskriver något extremt riskabelt.

Begäran om kommentarer

Vi inbjuder dig att hjälpa oss att förbättra boken. Vi har testat och verifierat all information efter bästa förmåga. Skriv för att berätta för oss om eventuella brister du hittar i den här boken eller hur du tror att den kan förbättras, för att hjälpa oss att förse dig med bästa möjliga dokumentation.

Meddela oss genom att skicka ett mejl till documentation@bitdefender.com. Skriv alla dina dokumentationsrelaterade e-postmeddelanden på engelska så att vi kan behandla dem effektivt.

1. VAD ÄR BITDEFENDER VPN

VPN fungerar som en tunnel mellan din enhet och nätverket du ansluter för att säkra din anslutning, kryptera data med kryptering av militär kvalitet och dölja din IP-adress var du än är. Din trafik omdirigeras via en separat server; vilket gör din enhet omöjlig att identifieras av din internetleverantör, genom de otaliga andra enheter som använder våra tjänster. Dessutom, medan du är ansluten till internet via Bitdefender VPN, kan du komma åt innehåll som normalt är begränsat i specifika områden.

Notera
Vissa länder utövar internetcensur och därför har användningen av VPN på deras territorium förbjudits enligt lag. För att undvika juridiska konsekvenser kan ett varningsmeddelande visas när du försöker använda Bitdefender VPN funktion för första gången. Genom att fortsätta använda funktionen bekräftar du att du är medveten om tillämpliga landsbestämmelser och de risker som du kan utsättas för.

1.1. Krypteringsprotokoll

Standarduppsättningarna för chiffersvit som är aktiverade i Hydra-klienten och servern finns nedan. Alla andra chiffersviter är inaktiverade.

Hydra Client ciphersuites:

- 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

Notera
Serversidans uppsättning är mycket mer restriktiv och både Hydra-klienten och servern kommer att avvisa ett läge som skiljer sig från GCM som använder AES. Hydra-servern upprätthåller serversidans prioritet för starkare chiffersviter och kommer att avvisa TLS-handskakning om en svagare svit efterfrågas av en klient. Denna lista är också konfigurerbar i runtime på serversidan.

2. VPN-PRENUMERATIONER

Med Bitdefender VPN, kan du välja två typer av prenumerationer:

- Grundprenumerationen
- Premium-prenumerationen

2.1. Grundabonnemang

Bitdefender VPN erbjuder gratis en daglig trafikkvot på 200 MB per enhet för att säkra din anslutning varje gång du behöver och låter dig ansluta till en enda plats som inte kan ändras.

Grundprenumerationen är tillgänglig för alla användare som laddar ner Bitdefender VPN.

2.2. Premiumprenumeration

För att få obegränsad tillgång till alla funktioner som ingår i Bitdefender VPN, uppgradera till Premium-versionen. Användare med ett aktivt Premium VPN-abonnemang har obegränsad skyddad trafik och kan ansluta till vilken som helst av våra servrar runt om i världen.

Det finns två tillgängliga planer för Premium-prenumerationen: Månadsplanen och Årsplanen.

- Månadsplanen: med den här planen kommer du att debiteras varje månad för Premium VPN-tjänsterna. Du kan välja bort när du vill.
- Årsplanen: kräver en engångsbetalning, vilket ger dig tillgång till våra Premium VPN-tjänster under ett helt år.

2.3. Hur man uppgraderar till Premium VPN

Det enklaste sättet att uppgradera till Premium-versionen av Bitdefender VPN är att klicka på **Uppgradera** knappen placerad i den nedre delen av huvudgränssnittet. Välj önskad prenumerationsmodell och följ sedan instruktionerna på skärmen.

Om du redan har en aktiveringskod, följ instruktionerna nedan:

- **För Windows-användare**
  1. Klicka på ikonen Mitt konto till vänster om VPN-gränssnittet.
  2. Klick **Lägg till det här**.
  3. Skriv in koden som du fått via e-post och klicka sedan på **Aktivera kod** knapp.
- **För macOS-användare**
  1. Klicka på kugghjulet i det övre högra hörnet av VPN-gränssnittet och välj **Mitt konto**.
  2. Klick **Lägg till det här**.
  3. Skriv in koden som du fått via e-post och klicka sedan på **Aktivera kod** knapp.
- **För Android-användare**
  1. Tryck på kugghjulet i det övre högra hörnet av VPN-gränssnittet och välj **Mitt konto**.
  2. Knacka **Lägg till kod**.
  3. Skriv in koden som du fått via e-post och klicka sedan på **Aktivera kod** knapp.
- **För iOS-användare**
  1. Tryck på kugghjulet i det övre högra hörnet av VPN-gränssnittet och välj **Mitt konto**.
  2. Knacka **Lägg till kod**.
  3. Skriv in koden som du fått via e-post och klicka sedan på **Aktivera kod** knapp.

3. BITDEFENDER CENTRAL-KONTOT

För att kunna använda Bitdefender VPN behöver du ett aktivt Bitdefender Central-konto. Bitdefender Central är plattformen där du har tillgång till produktens onlinefunktioner och tjänster.

Från det här kontot kommer du att kunna:

- Ladda ner och installera Bitdefender VPN på Windows, macOS, iOS och Android operativsystem.
- Hantera och förnya dina Bitdefender-prenumerationer.

3.1. Åtkomst till Bitdefender Central

För att komma åt Bitdefender Central, följ instruktionerna nedan:

- **För Windows-användare**
  1. Klicka på ikonen Mitt konto till vänster om VPN-gränssnittet.
  2. Klick **Redigera profil**.
- **För macOS-användare**
  1. Klicka på ikonen Mitt konto till vänster om VPN-gränssnittet.
  2. Klick **Redigera profil**.
- **För Android-användare**
  1. Tryck på kugghjulet i det övre högra hörnet av VPN-gränssnittet och välj **Mitt konto**.
  2. Knacka **Redigera kontoinformation i Bitdefender Central**.
- **För iOS-användare**
  1. Tryck på kugghjulet i det övre högra hörnet av VPN-gränssnittet och välj **Mitt konto**.
  2. 2. Tryck på **Redigera kontoinformation i Bitdefender Central**.

Alternativt kan du gå till ditt Bitdefender Central-konto genom att gå till https://central.bitdefender.com.

4. INSTALLATION

4.1. Förbereder för installation

Innan du installerar Bitdefender VPN, slutför dessa förberedelser för att säkerställa att installationen går smidigt:

- Se till att enheten där du planerar att installera Bitdefender uppfyller systemkraven. Om enheten inte uppfyller alla systemkrav, Bitdefender kommer inte att installeras eller, om det är installerat, kommer det inte att fungera korrekt och det kommer att orsaka systemavbrott och instabilitet.
  För en fullständig lista över alla systemkrav, se Systemkrav (sida 7)
- Logga in på enheten med ett administratörskonto.
- Det rekommenderas att din enhet är ansluten till internet under installationen, även från en CD/DVD. Om nyare versioner av appfilerna som ingår i installationspaketet är tillgängliga, Bitdefender kan ladda ner och installera dem.

4.2. Systemkrav

- **För Windows-användare**
  - **Operativ system:**Windows 7 med Service Pack 1, Windows 8, Windows 8.1 och Windows 10
  - **Minne (RAM):**1 GB
  - **Tillgängligt ledigt hårddiskutrymme:**500 MB ledigt utrymme
  - **Net Framework:**min version 4.5.2

    Viktig
    Systemprestandan kan påverkas på enheter som har gamla generationens processorer.
- **För macOS-användare**
  - **Operativ system:**macOS Sierra (10.12) eller senare
  - **Tillgängligt ledigt hårddiskutrymme:**100MB ledigt utrymme

- **För Android-användare**
  - **Operativ system:**Android 5.0 eller senare
  - **Lagring:**100 MB
  - En aktiv Internetanslutning
- **För iOS-användare**
  - **Operativ system:**iOS 12 eller senare
  - **Lagring på iPhone:**50 MB
  - **Lagring på iPad:**100 MB
  - En aktiv Internetanslutning

4.3. Installerar Bitdefender VPN

För att påbörja installationen, följ instruktionerna som motsvarar det operativsystem du använder:

- **För Windows-användare**
  1. För att påbörja installationen av Bitdefender VPN på en Windows-dator, börja helt enkelt med att ladda ner installationssatsen från https://www.bitdefender.com/solutions/vpn/download eller från e-postmeddelandet mottaget efter ett köp.
  2. Dubbelklicka på det nedladdade installationsprogrammet för att köra det.
  3. Välj Ja om det visas med dialogrutan Användarkontokontroll.
  4. Vänta tills nedladdningen är klar.
  5. Välj produktspråk med hjälp av rullgardinsmenyn på installationsprogrammet.
  6. Markera rutan "Jag bekräftar att jag har läst och jag godkänner prenumerationsavtalet och sekretesspolicyn", klicka sedan på **STARTA INSTALLATIONEN**.
  7. Vänta tills installationen är klar.
  8. **LOGGA IN** med ditt Bitdefender Central-konto. Om du inte har ett centralt konto, registrera dig för ett genom att klicka på knappen **SKAPA KONTO**.

9. Välja **Jag har en aktiveringskod** om du har köpt en Premium VPN-prenumeration.
   Annars kan du välja **STARTA TESTPERIOD** att testa produkten gratis i 7 dagar innan du förbinder dig att betala för den.
10. Skriv in koden som du fått via e-post och klicka sedan på **AKTIVERA PREMIUM** knapp.
11. Efter en kort väntan, Bitdefender VPN är installerat och redo att användas på din dator.

- **För macOS-användare**

1. För att påbörja installationen av Bitdefender VPN på macOS, börja helt enkelt med att ladda ner installationssatsen från https://www.bitdefender.com/solutions/vpn/download eller från e-postmeddelandet mottaget efter ett köp.
2. Installationsprogrammet kommer att sparas på Mac. I mappen Nedladdningar dubbelklickar du på paketfilen.
3. Följ instruktionerna på skärmen. Välja **Fortsätta**.
4. Du kommer att guidas genom de steg som krävs för att installera Bitdefender VPN på din Mac. Klicka två gånger **Fortsätta** knapp.
5. Klick **Hålla med**, efter att du har läst och godkänt villkoren i programvarulicensavtalet.
6. Klick **Installera**.
7. Ange ett användarnamn och lösenord för administratören och klicka sedan **Installera programvara**.
8. Du kommer att meddelas att ett systemtillägg undertecknats av Bitdefender har blockerats. Detta är inte ett fel, bara en säkerhetskontroll. Klick **Öppna Säkerhetsinställningar**.
9. Klicka på låsikonen för att låsa upp den.
   Ange ett administratörsnamn och lösenord och tryck sedan på **Låsa upp**.
10. Klick **Tillåta** för att ladda BitdefenderBitdefenders systemtillägg. Stäng sedan fönstret Säkerhet och sekretess och installationsprogrammet.

11. Gå sedan till sköldikonen i menyraden **Logga in** med ditt Bitdefender Central-konto. Om du inte har ett centralt konto, vänligen registrera dig för ett.
12. Välj jag har en **Aktiveringskod** om du har köpt en Premium VPN-prenumeration.
    Annars kan du välja **STARTA TESTPERIOD** att testa produkten gratis i 7 dagar innan du förbinder dig att betala för den.
13. Skriv in koden som du fått via e-post och klicka sedan på **Aktivera kod** knapp.
14. Efter en kort väntan, Bitdefender VPN är installerat och redo att användas på din Mac.

- **För Android-användare**

1. Att installera Bitdefender VPN på Android öppnar du först **Google Play Butik** app på din smartphone eller surfplatta.
2. Söka efter Bitdefender VPN och välj den här appen.
3. Tryck på **Installera** och vänta tills nedladdningen är klar.
4. Knacka **Öppen** för att köra appen.
5. Markera rutan "Jag godkänner prenumerationsavtalet och sekretesspolicyn" och tryck sedan på **Fortsätta**.
6. **Logga in** med ditt Bitdefender Central-konto. Om du inte har ett centralt konto, registrera dig för ett genom att trycka på **Skapa konto**.
7. Välja **Jag har en aktiveringskod** om du har köpt en Premium VPN-prenumeration.
   Annars kan du välja Starta 7 dagars provperiod för att testa produkten gratis i 7 dagar innan du åtar dig att betala för den.
8. Skriv in koden som du fått via e-post och tryck sedan på **Aktivera kod**.

- **För iOS-användare**

1. Att installera Bitdefender VPN på iOS, öppnas först **App Store** på din iPhone eller iPad.
2. Söka efter Bitdefender VPN och välj den här appen.

3. Tryck på **Skaffa sig** och vänta tills nedladdningen är klar.
4. Knacka **Öppen** för att köra appen.
5. Markera rutan **Jag godkänner prenumerationsavtalet och sekretesspolicyn**, tryck sedan på **Fortsätta**.
6. **Logga in** med ditt Bitdefender Central-konto. Om du inte har ett konto, registrera dig för ett genom att trycka på **Skapa konto**.
7. Knacka **Tillåta** om du vill ta emot Bitdefender VPN meddelanden.
8. Välja **Jag har en aktiveringskod** om du har köpt en Premium VPN-prenumeration.
   Annars kan du välja Starta 7 dagars provperiod för att testa produkten gratis i 7 dagar innan du åtar dig att betala för den.
9. Skriv in koden som du fått via e-post och tryck sedan på **Aktivera kod**.

5. ANVÄNDER BITDEFENDER VPN

5.1. Öppnar Bitdefender VPN

- **För Windows**
  För att komma åt**huvudgränssnittet för Bitdefender VPN**, använd någon av följande metoder:

  - **Från systemfältet**
    Högerklicka på den röda sköldikonen i systemfältet och välj sedan **Show** i menyn.

  - **Från Bitdefender-gränssnittet**
    Om en Bitdefender-säkerhetsprodukt som Bitdefender Total Security eller Bitdefender Antivirus Plus etc. redan är installerad på din Windows-dator, kan du öppna Bitdefender VPN därifrån:

    1. Klick **Integritet** på vänster sidofält i Bitdefender-gränssnittet.
    2. Klick **Öppna VPN** på VPN-rutan.

  - **Från ditt skrivbord**
    Dubbelklicka på Bitdefender VPN-genvägen på ditt skrivbord.

- **För macOS**
  Du kan öppna Bitdefender VPN-appen genom att klicka på ikonen från menyraden längst upp till höger på skärmen.
  Om Bitdefender-skölden inte kan hittas i menyraden, använd din Mac Launchpad eller Finder för att ta tillbaka den:

  - **Från Launchpad**

    1. Tryck**F4**på ditt tangentbord för att öppna Launchpad på din Mac.
    2. Bläddra igenom sidorna med installerade appar tills du hittar Bitdefender VPN-appen. Alternativt kan du skriva**Bitdefender VPN**i Launchpad för att börja filtrera dina resultat.
    3. När du ser Bitdefender VPN-appen klickar du på dess ikon för att fästa den i menyraden.

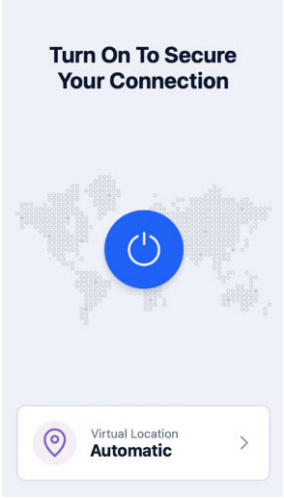
  - **Från Finder**

1. Klicka på**Upphittare**längst ner till vänster i Dock (Finder är ikonen som ser ut som en blå fyrkant med en smiley).
2. Klicka sedan**Gå**längst upp till vänster på skärmen, i menyraden.
3. Välj**Ansökningar**från menyn för att öppna mappen Program på din Mac.
4. Öppna mappen Applications**Bitdefender**mapp och dubbelklicka sedan på**Bitdefender VPN**app.

Notera
För att komma åt Bitdefender VPN på dina Android- eller iOS-mobilenheter, öppna helt enkelt Bitdefender VPN-applikationen efter att du har installerat den.

5.2. Hur man ansluter till Bitdefender VPN

VPN-gränssnittet visar status för appen: ansluten eller frånkopplad. Serverplatsen för användare med gratisversionen ställs automatiskt in av Bitdefender till den mest lämpliga servern, medan premiumanvändare har möjlighet att ändra serverplatsen de vill ansluta till genom att välja den från listan med virtuell plats. För att ansluta eller koppla från, klicka helt enkelt på strömknappen från VPN-gränssnittet.



- **För Windows:** Ikonen i systemfältet visar en grön bock när VPN är ansluten och en svart markering när VPN är frånkopplat. När du är ansluten till en manuellt vald plats visas IP-adressen på huvudgränssnittet.
- **För macOS:** Menyradens ikon visar svart när VPN är anslutet, och vit när VPN är frånkopplat. Klicka på den cirkulära knappen i mitten av gränssnittet och vänta tills anslutningen upprättas.
- **För Android och iOS:** För att ansluta till Bitdefender VPN för Android, iOS och iPadOS:
  - **I Bitdefender VPN-appen:** För att ansluta eller koppla från, tryck bara på strömknappen på VPN-gränssnittet. Status för Bitdefender VPN visas.
  - **I Bitdefender Mobile Security-appen:**
    1. Få tillgång till VPN-ikon i det nedre navigeringsfältet i Bitdefender Mobile Security.
    2. Knacka**ANSLUTA**varje gång du vill vara skyddad medan du är ansluten till osäkra trådlösa nätverk. Knacka**KOPPLA IFRÅN**närhelst du vill inaktivera VPN-anslutningen.

5.3. Hur man ansluter till en annan server

Med en Premium-prenumeration, Bitdefender VPN låter dig ansluta till någon av våra servrar runt om i världen, när som helst. För att göra detta måste du:

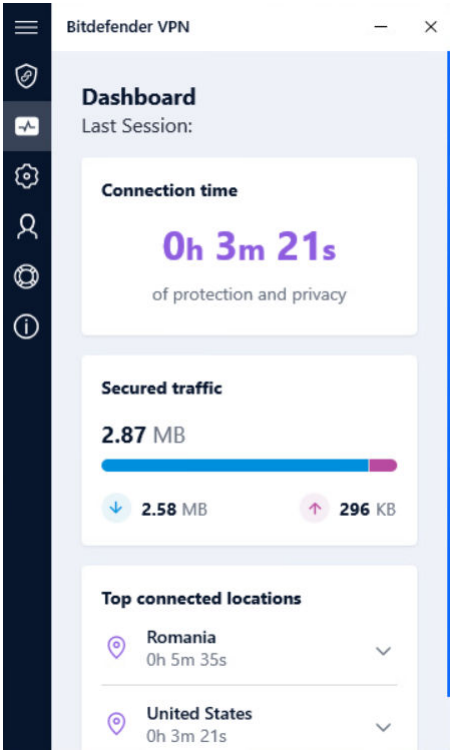
1. Öppna Bitdefender VPN app.
2. Tryck på **Virtuell plats** knappen i den nedre delen av gränssnittet.
3. Välj vilket land du vill.
4. Klicka på **Anslut till [valfritt land]** knappen i den nedre delen av gränssnittet.

5.4. instrumentbräda

För att komma åt instrumentpanelen, klicka på menyikonen finns i sidofältet och välj **instrumentbräda**.

Här hittar du en översikt över din anslutningstid, mängden säker trafik och de bästa VPN-servrarna du spenderade mest tid på att vara ansluten till.

Notera
Den här funktionen är för närvarande endast tillgänglig för Windows-enheter.



6. BITDEFENDER VPN INSTÄLLNINGAR OCH FUNKTIONER

6.1. Åtkomst till inställningar

För att komma åt Bitdefender VPN inställningar måste du följa stegen som beskrivs nedan:

- **På Windows**
  1. Öppna Bitdefender VPN app på din enhet genom att dubbelklicka på dess ikon i systemfältet eller genom att högerklicka på den och välja Visa.
  2. Klicka på **inställningar** knappen (representerad av ett kugghjul) på vänster sida av gränssnittet.
- **På macOS**
  1. Öppna Bitdefender VPN app på din macOS-enhet genom att klicka på dess ikon i menyraden.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender VPN gränssnittet och välj Inställningar.
- **På Android**
  1. Öppna Bitdefender VPN app på din enhet.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender VPN gränssnitt.
- **På iOS**
  1. Öppna Bitdefender VPN app på din enhet.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender VPN gränssnitt.

6.2. Funktioner

6.2.1. Autoanslut

När du är på språng, arbetar på ett kafé eller väntar på flygplatsen kan det vara den snabbaste lösningen att ansluta till ett allmänt trådlöst nätverk

för att göra betalningar, kolla e-post eller konton i sociala nätverk. Men nyfikna ögon som försöker kapa din personliga data kan vara där och se hur informationen läcker genom nätverket.

För att skydda dig mot farorna med osäkra eller okrypterade offentliga trådlösa hotspots, Bitdefender VPN inkluderar en autoconnect-funktion. Detta innebär att Bitdefender VPN kan aktiveras automatiskt i vissa situationer, beroende på dina preferenser och vilket operativsystem du kör.

- På **Windows** funktionen för automatisk anslutning kan aktiveras för följande situationer:
  - **Börja:** Anslut VPN vid start av Windows.
  - **Osäkert Wi-Fi:** Använd VPN när du ansluter till offentliga eller osäkra Wi-Fi-nätverk.
  - **Peer-to-peer-appar:** Anslut till VPN när du startar en peer-to-peer fildelningsapp.
  - **Appar och domäner:** Använd alltid VPN för vissa appar och webbplatser.

    Notera

    1. Klicka på**Hantera**länk.
    2. Bläddra till platsen för appen som du vill använda VPN för, välj appnamnet och klicka sedan**Lägg till**.

  - **Webbplatskategorier:** Anslut till VPN när du besöker specifika webbplatskategorier. Bitdefender VPN kan ansluta automatiskt för följande webbplatskategorier:
    - Finansiell
    - Onlinebetalningar
    - Hälsa
    - Fildelning
    - Online dejting
    - Vuxet innehåll

> **Notera**
> För varje kategori kan du välja en annan server för VPN att ansluta till.

- På **Mac OS** funktionen för automatisk anslutning kan aktiveras för följande situationer:
  - **Börja:** Anslut VPN vid start av macOS.
  - **Osäkert Wi-Fi:** Använd VPN när du ansluter till offentliga eller osäkra Wi-Fi-nätverk.
  - **Peer-to-peer-appar:** Anslut till VPN när du startar en peer-to-peer fildelningsapp.
  - **Applikationer:** Anslut alltid VPN för vissa appar.
- På **Android** och **iOS** Bitdefender VPN kan ställas in för att ansluta automatiskt endast när du är på ett osäkrat eller offentligt Wi-Fi.

6.2.2. Internet Kill-Switch

Kill-Switch är en ny funktion implementerad i Bitdefender VPN. När den är aktiverad stänger den här funktionen tillfälligt av all internettrafik om VPN-anslutningen av misstag avbryts. Så snart du är online igen kommer VPN-anslutningen att återupprättas.

För att aktivera Kill-Switch, följ stegen nedan:

- **På Windows**
  1. Öppna Bitdefender VPN app på din enhet genom att dubbelklicka på dess ikon i systemet försök eller genom att högerklicka på den och välja **Show**.
  2. Klicka på **inställningar** knappen (representerad av ett kugghjul) på vänster sida av gränssnittet.
  3. Välj **Avancerad**.
  4. Aktivera **Internet Kill-Switch** alternativ.
- **På Android**
  1. Öppna Bitdefender VPN app på din enhet.

2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender VPN gränssnitt.
3. Under **inställningar**, aktivera **Kill-Switch** alternativ.

- **På iOS**
  1. Öppna Bitdefender VPN app på din enhet.
  2. Klicka på kugghjulsknappen i det övre högra hörnet av Bitdefender VPN gränssnitt.
  3. Under **inställningar**, aktivera **Kill-Switch** alternativ.

> **Notera**
> Den här funktionen är även tillgänglig för macOS-enheter med operativsystem 10.15.4 eller senare versioner.

6.2.3. Delad tunnling

Virtual Private Network (VPN) delad tunneling låter dig dirigera en del av din applikations- eller enhetstrafik genom ett krypterat VPN, medan andra applikationer eller enheter har direktåtkomst till internet. Detta är särskilt användbart om du vill dra nytta av tjänster som fungerar bäst när din plats är känd samtidigt som du har säker åtkomst till potentiellt känslig kommunikation och data.

Genom att aktivera **Delad tunnling** funktionen kommer utvalda appar och webbplatser att kringgå VPN och komma åt Internet direkt.

Så här hanterar du applikationer och webbplatser som kringgår VPN:

1. Klicka på**Hantera**länk när funktionen är aktiverad.
2. Klicka på **Lägg till** knapp.
3. Bläddra till platsen för appen i fråga eller skriv in webbadressen till den önskade webbplatsen och klicka sedan**Lägg till**.

> **Notera**
> Genom att lägga till en webbplats kommer hela domänen inklusive alla underdomäner att kringgås.

> **Viktig**
> På **Mac OS** enheter är funktionen Split tunneling endast tillgänglig för webbplatser.

6.2.4. App Traffic Optimizer

Bitdefender VPNApp Traffic Optimizer låter dig prioritera trafik till de viktigaste apparna på din enhet utan att utsätta din anslutning för integritetsrisker. VPN:er omdirigerar internettrafik genom en säker tunnel samtidigt som de använder robusta krypteringsalgoritmer för att skydda den.

Denna kombination av tekniker kan dock ha vissa nackdelar, främst när det gäller anslutningens hastighet. Flera faktorer kan utlösa nedgångar i anslutningen, den vanligaste är avståndet till servern du ansluter till, nätverksstockning och hög bandbreddsanvändning. Om du någonsin känt det ibland Bitdefender VPN lägger en onödig börda på din anslutning och avmattningar ständigt kommer i vägen för dig, kan det finnas ett bättre svar än att koppla bort.

Hur fungerar App Traffic Optimizer?

Vissa appar och tjänster som streamingplattformar, torrentklienter och spel kräver mer bandbredd. Att ständigt använda dem kan påverka din internetanslutningshastighet. Att dirigera din trafik genom en VPN-tunnel utsätter redan din anslutning för en relativ avmattning. Att lägga ytterligare påfrestningar på din anslutning kan allvarligt försämra din onlineupplevelse.

Bitdefender VPNs App Traffic Optimizer-funktion kan hjälpa dig att ta itu med långsamma VPN-anslutningar genom att prioritera den till den app du väljer. Funktionen låter dig bestämma vilka appar som ska ta emot huvuddelen av din trafik och allokerar sedan resurserna därefter. Om du till exempel är i ett möte och märker att kvaliteten på ditt samtal är undermålig, låter App Traffic Optimizer dig prioritera trafik till videokonferensappen för förbättrade resultat.

Vanligtvis skulle VPN-användare tillgripa att stänga alla störande processer på sin enhet eller till och med inaktivera sin VPN-anslutning för att få snabbare internethastighet. App Traffic Optimizer låter dig njuta av oavbrutet integritetsskydd utan att kompromissa med din anslutningshastighet.

Använder App Traffic Optimizer

För närvarande är funktionen endast tillgänglig på Windows-enheter och låter dig prioritera trafik till upp till 3 applikationer.

Följ dessa steg för att aktivera och konfigurera det med minimal ansträngning:

1. Starta Bitdefender VPN programmet på din Windows-dator.
2. Klicka på knappen på sidofältet för att komma åt VPN-inställningarna.
3. Gå till**Allmän**fliken och aktivera**App Traffic Optimizer**funktion. Färgen på omkopplaren kommer att ändras från grå till blå.

Så här hanterar du de applikationer som prioriteras av den här funktionen:

1. Klicka på**Hantera**länk.
2. Bläddra till platsen för appen som du vill optimera trafiken för, välj appnamnet och klicka sedan**Lägg till**. Appen kommer att visas i **Prioriterat** sektion.

> **Notera**
> Alternativt, om du nyligen har öppnat programmet du vill prioritera, tryck på +-knappen i fönstret App Traffic Optimizer.

3. Koppla från och återanslut till Bitdefender VPN efter att ha lagt till eller tagit bort appar från listan.

För att ta bort en app från App Traffic Optimizer, klicka helt enkelt på ikonen bredvid appens namn.

6.2.5. Annonsblockerare och Anti-tracker

Dessa funktioner är utformade för att hjälpa dig att hålla dig privat och njuta av webben utan irriterande annonser eller företag som tittar in på dig. De hjälper till att blockera annonser och stoppa onlinespårare.

Annonsblockerare

De **Annonsblockerare** används för att blockera annonser, popup-fönster, högljudda videoannonser eller annonsbanner medan du surfar. Detta hjälper webbplatser att laddas snabbare och vara renare, samt säkrare att interagera med.

Så här aktiverar du annonsblockeraren:

1. Leta upp **Annonsblockerare och Antitracker** inslag i **inställningar**.

2. Klicka på **Hantera** länk.
3. Växla omkopplaren till **PÅ** placera.

Antispårare

De **Antispårare** används för att blockera spårare som angetts av annonsörer för att följa och profilera dig online. Vissa webbplatser kan inte fungera när spårare blockeras, men att lägga till webbadressen till vitlistan kan fixa detta.

Så här aktiverar du Anti-tracker:

1. Leta upp **Annonsblockerare och Antitracker** inslag i **inställningar**.
2. Klicka på **Hantera** länk.
3. Växla omkopplaren till **PÅ** placera.

Vitlista

Vissa webbplatser kanske inte laddas korrekt om du blockerar deras spårningskod och annonser. Att lägga till webbadresserna för dessa specifika domäner till vitlistan kan lösa det här problemet, men kom ihåg att när du surfar på dessa webbplatser kommer du att se annonser och deras spårningskod kommer att vara aktiv.

Lägg till webbplatser som du vill tillåta att visa annonser och använda spårare genom att:

1. Leta upp **Annonsblockerare och Antitracker** inslag i **inställningar**.
2. Klicka på **Hantera** länk. Gå sedan till avsnittet Vitlista i fönstret och klicka på motsvarande **Hantera** länk.
3. Klicka på **Lägg till webbplats** och infoga önskad URL.

7. AVINSTALLERAR BITDEFENDER VPN

Proceduren för att ta bort Bitdefender VPN liknar den du använder för att ta bort andra program från din dator:

- **Avinstallerar Bitdefender VPN från Windows-enheter**
  - I **Windows 7**:
    1. Klick **Start**, gå till **Kontrollpanel** och dubbelklicka **Program och funktioner**.
    2. Hitta **Bitdefender VPN** och välj **Avinstallera**.
       Vänta tills avinstallationsprocessen är klar.
  - I **Windows 8** och **Windows 8.1**:
    1. Från startskärmen i Windows, leta upp **Kontrollpanel** (du kan till exempel börja skriva "Kontrollpanelen" direkt på startskärmen) och klicka sedan på dess ikon.
    2. Klick **Avinstallera ett program** eller **Program och funktioner**.
    3. Hitta **Bitdefender VPN** och välj **Avinstallera**.
       Vänta tills avinstallationsprocessen är klar.
  - I **Windows 10** och **Windows 11**:
    1. Klick **Start**, Klicka sedan **inställningar**.
    2. Klicka på **Systemet** ikonen i området Inställningar och välj sedan **Installerade appar**.
    3. Hitta **Bitdefender VPN** och välj **Avinstallera**.
    4. Klick **Avinstallera** igen för att bekräfta ditt val.
       Vänta tills avinstallationsprocessen är klar.
- **Avinstallerar från macOS-enheter**
  1. Klicka på **Gå** i menyraden och välj **Ansökningar**.
  2. Dubbelklicka på **Bitdefender** mapp.
  3. Springa **BitdefenderUninstaller**.

4. I det nya fönstret markerar du rutan bredvid **Bitdefender VPN**, klicka sedan på **Avinstallera**.
5. Skriv ett giltigt administratörskontonamn och ett lösenord och klicka sedan **OK**.
6. Slutligen kommer du att få besked om det Bitdefender VPN har avinstallerats. Klick **Stänga**.

- **Avinstallerar från Android-enheter**
  1. Öppna **Play Butik** app.
  2. Söka efter **Bitdefender VPN**.
  3. I den Bitdefender VPN appbutikssida, välj **Avinstallera**.
  4. Bekräfta genom att trycka på **OK**.
- **Avinstallerar från iOS-enheter**
  1. Håll fingret på Bitdefender VPN app.
  2. Välj **Ta bort appen**.
  3. Knacka **Radera**.

8. VANLIGA FRÅGOR

När ska jag använda Bitdefender VPN?

Du måste vara försiktig när du använder, laddar ner eller laddar upp innehåll på Internet. För att du ska vara säker när du surfar på webben rekommenderar vi att du använder VPN när du:

- vill ansluta till offentliga trådlösa nätverk
- vill komma åt innehåll som normalt är begränsat i specifika områden, oavsett om du är hemma eller utomlands
- vill hålla dina personuppgifter privata (användarnamn, lösenord, e-postadresser, kreditkortsinformation, etc.)
- vill dölja din IP-adress

Kan jag välja en stad med Bitdefender VPN?

Ja. För närvarande kan Bitdefender VPN för Windows, macOS, Android och iOS användas för att välja en specifik stad. Här är listan över tillgängliga städer:

- **USA:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Angeles, Miami, New York, Newark, Phoenix, Portland, San Jose, Seattle, Washington
- **Kanada:** Montreal, Toronto, Vancouver
- **STORBRITANNIEN:** London, Manchester

Kan Bitdefender VPN installeras som en fristående app?

VPN-appen installeras automatiskt tillsammans med din Bitdefender-säkerhetslösning. Den kan också installeras som en fristående app från produktsidan, från Google Play Store och App Store.

Kommer Bitdefender att dela min IP-adress och personliga data som delas med tredje part?

Nej, med Bitdefender VPN är din integritet 100 % säker. Ingen (reklambyråer, internetleverantörer, försäkringsbolag, etc.) kommer att ha tillgång till dina onlineloggar.

Vilken krypteringsalgoritm använder den?

Bitdefender VPN använder Hydra-protokollet på alla plattformar, 256-bitars AES-kryptering eller den högsta tillgängliga cypher som stöds av

både klient och server, med Perfect Forward Secrecy. Detta innebär att krypteringsnycklar genereras för varje ny VPN-session och raderas från minnet när sessionen är över.

Kan jag få tillgång till GEO-IP-begränsat innehåll?

Med Premium VPN har du tillgång till ett omfattande nätverk av virtuella platser över hela världen.

Kommer det att ha en negativ inverkan på batteritiden för min enhet?

Bitdefender VPN är utformad för att skydda dina personliga data, dölja din IP-adress när du är ansluten till osäkra trådlösa nätverk och komma åt begränsat innehåll i vissa länder. För att undvika onödig batteriförbrukning av din enhet rekommenderar vi att du bara använder VPN när du behöver det och kopplar bort när du är offline.

Varför saktar VPN ner min internetanslutning?

Bitdefender VPN är designad för att erbjuda en lätt upplevelse när du surfar på webben. Beroende på avståndet mellan din faktiska plats och serverplatsen du väljer att ansluta till, förväntas en viss hastighetsstraff, men det är nästan alltid tillräckligt litet för att det går obemärkt förbi under normal onlineaktivitet. Dessutom förlitar vi oss på en av de snabbaste VPN-infrastrukturerna i världen. Om det inte är ett måste att ansluta från din plats till en fjärransluten server (t.ex. från USA till Frankrike), rekommenderar vi att du tillåter VPN att automatiskt ansluta dig till närmaste server eller hitta en server närmare din nuvarande plats.

9. FÅ HJÄLP

9.1. Ber om hjälp

Bitdefender ger sina kunder en oöverträffad nivå av snabb och exakt support. Om du upplever några problem eller om du har några frågor om din Bitdefender-produkt, kan du använda flera onlineresurser för att hitta en lösning eller ett svar. Samtidigt kan du kontakta Bitdefender Customer Care-teamet. Våra supportrepresentanter kommer att svara på dina frågor i tid och ge dig den hjälp du behöver.

9.2. Onlineresurser

Flera onlineresurser finns tillgängliga för att hjälpa dig att lösa dina Bitdefender-relaterade problem och frågor.

- Bitdefender Support Center:
  https://www.bitdefender.se/consumer/support/
- Bitdefender Expert Community:
  https://community.bitdefender.com/en/
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

Du kan också använda din favoritsökmotor för att ta reda på mer information om datorsäkerhet, Bitdefender-produkterna och företaget.

9.2.1. Bitdefender Support Center

Bitdefender Support Center är ett onlineförråd med information om Bitdefender-produkterna. Den lagrar, i ett lättillgängligt format, rapporter om resultaten av den pågående tekniska supporten och buggfixningsaktiviteterna för Bitdefender-support- och utvecklingsteamen, tillsammans med mer allmänna artiklar om hotförebyggande, hantering av Bitdefender-lösningar med detaljerade förklaringar och många andra artiklar.

Bitdefender Support Center är öppet för allmänheten och fritt sökbart. Den omfattande informationen den innehåller är ytterligare ett sätt att förse Bitdefender-kunder med den tekniska kunskap och insikt de behöver. Alla giltiga förfrågningar om information eller buggrapporter

som kommer från Bitdefender-klienter hittar så småningom vägen till Bitdefender Support Center, som bugfixrapporter, fuskblad för lösningar eller informationsartiklar för att komplettera produkthjälpfiler.

Bitdefender Support Center är tillgängligt när som helst på följande adress: https://www.bitdefender.se/consumer/support/.

9.2.2. Bitdefender Expert Community

Expertgemenskapen är en miljö där Bitdefender-användare, entusiaster och fans kan engagera sig, utbyta idéer, stödja varandra och dela sina kunskaper och lösningar. Det är också en plats för idéer och ger värdefull feedback till våra utvecklingsteam. Community-medlemmarna är erfarna Bitdefender-användare som gärna hjälper andra kamrater på sin egen tid. Med deras enorma bidrag och genuina frivilliga insatser har vi skapat en kunskapsbas där användare kan hitta svar och vägledning, men med den mänskliga touchen.

Här hittar du meningsfulla konversationer med personer som använder Bitdefender på sina enheter. Gemenskapen erbjuder en sann kontakt med våra medlemmar och gör din röst hörd. Det är en plats där du uppmuntras att delta i vetskapen om att din åsikt och din input respekteras och omhuldas. Som en uppskattad leverantör strävar vi efter att erbjuda en oöverträffad nivå av snabb, exakt support och vi vill föra våra användare närmare oss. Vi har utformat vår community med detta syfte i åtanke.

Du hittar vår webbsida för expertgemenskapen här:

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

9.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia har all information du behöver om de senaste cyberhoten. Det här är platsen där Bitdefender-experter delar med sig av tips och tricks om hur man kan hålla sig skyddad från hackare, dataintrång, identitetsstöld och sociala identitetsförsök.

Bitdefender Cyberpedias webbsida finns här:

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

9.3. Kontaktinformation

Effektiv kommunikation är nyckeln till ett framgångsrikt företag. Sedan 2001 har BITDEFENDER etablerat ett obestridligt rykte genom att ständigt

sträva efter bättre kommunikation för att överträffa våra kunders och partners förväntningar. Om du har några frågor, tveka inte att kontakta oss direkt via vår Bitdefender Support Center (sida 27).

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

9.3.1. Lokala distributörer

Bitdefender lokala distributörer är redo att svara på alla förfrågningar om deras verksamhetsområden, både i kommersiella och allmänna frågor.

Så här hittar du en Bitdefender-distributör i ditt land:

1. Gå till https://www.bitdefender.com/partners/partner-locator.html.
2. Välj ditt land och din stad med hjälp av motsvarande alternativ.

ORDLISTA

Aktiveringskod

Är en unik nyckel som kan köpas från detaljhandeln och användas för att aktivera en specifik produkt eller tjänst. En aktiveringskod möjliggör aktivering av ett giltigt abonnemang under en viss tidsperiod och antal enheter och kan även användas för att förlänga ett abonnemang med villkoret att genereras för samma produkt eller tjänst.

ActiveX

ActiveX är en modell för att skriva program så att andra program och operativsystemet kan anropa dem. ActiveX-teknik används med Microsoft Internet Explorer för att skapa interaktiva webbsidor som ser ut och beter sig som datorprogram, snarare än statiska sidor. Med ActiveX kan användare ställa eller svara på frågor, använda tryckknappar och interagera på andra sätt med webbsidan. ActiveX-kontroller skrivs ofta med Visual Basic. Active X är anmärkningsvärt för en fullständig brist på säkerhetskontroller; datorsäkerhetsexperter avråder från att använda det över internet.

Avancerat ihållande hot

Advanced persistent hot (APT) utnyttjar sårbarheter i system för att stjäla viktig information för att leverera den till källan. Stora grupper som organisationer, företag eller regeringar är föremål för detta hot. Målet med ett avancerat ihållande hot är att förbli oupptäckt under lång tid och kunna övervaka och samla in viktig information utan att skada de riktade maskinerna. Metoden som används för att injicera hotet i nätverket är genom en PDF-fil eller ett Office-dokument som ser ofarliga ut så att alla användare kan köra filerna.

Reklamprogram

Adware kombineras ofta med en värdapp som tillhandahålls utan kostnad så länge som användaren accepterar adware. Eftersom adware-appar vanligtvis installeras efter att användaren har godkänt ett licensavtal som anger syftet med appen, begås inget brott. Men popup-annonser kan bli irriterande och i vissa fall försämra systemets prestanda. Dessutom kan informationen som vissa av dessa appar samlar in orsaka integritetsproblem för användare som inte var fullt medvetna om villkoren i licensavtalet.

Arkiv

En disk, ett band eller en katalog som innehåller filer som har säkerhetskopierats.

En fil som innehåller en eller flera filer i ett komprimerat format.

Bakdörr

Ett hål i säkerheten i ett system som medvetet lämnats på plats av designers eller underhållare. Motivationen för sådana hål är inte alltid olycksbådande; vissa operativsystem, till exempel, kommer ur lådan med privilegierade konton avsedda att användas av fältservicetekniker eller säljarens underhållsprogrammerare.

Boot sektor

En sektor i början av varje disk som identifierar diskens arkitektur (sektorstorlek, klusterstorlek, och så vidare). För startdiskar innehåller bootsektorn även ett program som laddar operativsystemet.

Boot virus

Ett hot som infekterar startsektorn på en fast eller diskett. Ett försök att starta från en diskett som är infekterad med ett bootsektorvirus gör att hotet blir aktivt i minnet. Varje gång du startar ditt system från den tidpunkten kommer du att ha hotet aktivt i minnet.

Botnet

Termen "botnät" är sammansatt av orden "robot" och "nätverk". Botnät är internetanslutna enheter som är infekterade med hot och kan användas för att skicka skräppost, stjäla data, fjärrstyra sårbara enheter eller sprida spionprogram, ransomware och andra typer av hot. Deras mål är att infektera så många uppkopplade enheter som möjligt, såsom datorer, servrar, mobila eller IoT-enheter som tillhör stora företag eller industrier.

Webbläsare

Förkortning för webbläsare, en programvaruapp som används för att hitta och visa webbsidor. Populära webbläsare inkluderar Microsoft Internet Explorer, Mozilla Firefox och Google Chrome. Dessa är grafiska webbläsare, vilket innebär att de kan visa grafik såväl som text. Dessutom kan de flesta moderna webbläsare presentera multimediainformation, inklusive ljud och video, även om de kräver plugin-program för vissa format.

Brute Force Attack

Lösenordsgissningsattack används för att bryta sig in i ett datorsystem genom att ange möjliga lösenordskombinationer, oftast med det enklast att gissa lösenordet.

Kommandorad

I ett kommandoradsgränssnitt skriver användaren kommandon i utrymmet som tillhandahålls direkt på skärmen med hjälp av kommandospråk.

Småkakor

Inom internetbranschen beskrivs cookies som små filer som innehåller information om enskilda datorer som kan analyseras och användas av annonsörer för att spåra dina intressen och smaker online. I det här området utvecklas fortfarande cookieteknologi och avsikten är att rikta annonser direkt till det du har sagt att dina intressen är. Det är ett tveeggat svärd för många människor eftersom det å ena sidan är effektivt och relevant eftersom du bara ser annonser om det du är intresserad av. Å andra sidan handlar det faktiskt om att "spåra" och "följa" vart du går och vad du klickar på. Det är förståeligt nog att det finns en debatt om integritet och många känner sig kränkta av uppfattningen att de ses som ett "SKU-nummer" (ni vet, streckkoden på baksidan av paketen som skannas vid utcheckningslinjen) . Även om denna synpunkt kan vara extrem, är den i vissa fall korrekt.

Cybermobbning

När kamrater eller främlingar begår kränkande handlingar mot barn med avsikt för att fysiskt skada dem. För att skada känslomässigt skickar angriparna elaka meddelanden eller föga smickrande bilder, vilket gör att deras offer isolerar sig från andra eller känner sig frustrerade.

Ordbok Attack

Lösenordsgissningsattacker används för att bryta sig in i ett datorsystem genom att ange en kombination av vanliga ord för att generera potentiella lösenord. Samma metod används för att gissa dekrypteringsnycklar för krypterade meddelanden eller dokument. Ordboksattacker lyckas eftersom många människor är benägna att välja korta och enstaka ordlösenord som är lätta att gissa.

Diskenhet

Det är en maskin som läser data från och skriver data till en disk. En hårddisk läser och skriver hårddiskar. En diskettenhet får åtkomst till

disketter. Diskenheter kan antingen vara interna (inrymd i en dator) eller externa (inrymd i en separat låda som ansluts till datorn).

Ladda ner

Att kopiera data (vanligtvis en hel fil) från en huvudkälla till en kringutrustning. Termen används ofta för att beskriva processen att kopiera en fil från en onlinetjänst till sin egen dator. Nedladdning kan också syfta på att kopiera en fil från en nätverksfilserver till en dator i nätverket.

E-post

E-post. En tjänst som skickar meddelanden på datorer via lokala eller globala nätverk.

evenemang

En åtgärd eller händelse som upptäckts av ett program. Händelser kan vara användaråtgärder, som att klicka på en musknapp eller trycka på en tangent, eller systemhändelser, som att minnet blir slut.

Utnyttjar

Ett sätt att dra nytta av olika buggar eller sårbarheter som finns i en dator (mjukvara eller hårdvara). Således kan hackare få kontroll över datorer eller nätverk.

Falskt positivt

Uppstår när en skanner identifierar en fil som infekterad när den faktiskt inte är det.

Filnamnstillägg

Den del av ett filnamn, efter den sista punkten, som anger vilken typ av data som lagras i filen. Många operativsystem använder filnamnstillägg, t.ex. Unix, VMS och MS-DOS. De är vanligtvis från en till tre bokstäver (vissa tråkiga gamla operativsystem stöder inte mer än tre). Exempel inkluderar "c" för C-källkod, "ps" för PostScript, "txt" för godtycklig text.

Heuristisk

En regelbaserad metod för att identifiera nya hot. Denna metod för skanning är inte beroende av specifik databas med hotinformation. Fördelen med den heuristiska skanningen är att den inte luras av en ny variant av ett befintligt hot. Det kan dock ibland rapportera misstänkt kod i vanliga program, vilket genererar den så kallade "falska positiva".

Honungsburk

Ett lockdatorsystem som lockar hackare att studera hur de agerar och identifiera de kätterska metoder de använder för att samla in systeminformation. Företag och företag är mer intresserade av att implementera och använda honeypots för att förbättra sin övergripande säkerhet.

IP

Internet Protocol - Ett routbart protokoll i TCP/IP-protokollsviten som ansvarar för IP-adressering, routing och fragmentering och återmontering av IP-paket.

Java applet

Ett Java-program som är designat för att endast köras på en webbsida. För att använda en applet på en webbsida skulle du ange namnet på appleten och storleken (längd och bredd, i pixlar) som appleten kan använda. När webbsidan nås laddar webbläsaren ner appleten från en server och kör den på användarens dator (klienten). Applets skiljer sig från appar genom att de styrs av ett strikt säkerhetsprotokoll.

Till exempel, även om appletar körs på klienten, kan de inte läsa eller skriva data på klientens dator. Dessutom är appletar ytterligare begränsade så att de bara kan läsa och skriva data från samma domän som de betjänas från.

Keylogger

En keylogger är en app som loggar allt du skriver. Keyloggers är inte skadliga till sin natur. De kan användas för legitima ändamål, som att övervaka anställda eller barnaktivitet. De används dock i allt högre grad av cyberbrottslingar i skadliga syften (till exempel för att samla in privata uppgifter, såsom inloggningsuppgifter och personnummer).

Makrovirus

En typ av datorhot som är kodat som ett makro inbäddat i ett dokument. Många appar, som Microsoft Word och Excel, stöder kraftfulla makrospråk. Dessa appar låter dig bädda in ett makro i ett dokument och få makrot att köras varje gång dokumentet öppnas.

E-postklient

En e-postklient är en app som gör att du kan skicka och ta emot e-post.

Minne

Interna lagringsutrymmen i datorn. Termen minne identifierar datalagring som kommer i form av chips, och ordet lagring används för minne som finns på band eller diskar. Varje dator kommer med en viss mängd fysiskt minne, vanligtvis kallat huvudminne eller RAM.

Icke-heuristisk

Denna metod för skanning bygger på specifik databas med hotinformation. Fördelen med den icke-heuristiska skanningen är att den inte luras av vad som kan tyckas vara ett hot och inte genererar falsklarm.

Rovdjur online

Individer som försöker locka minderåriga eller tonåringar till konversationer med avsikt att involvera dem i illegala sexuella aktiviteter. Sociala nätverk är den idealiska platsen där utsatta barn lätt kan jagas och förföras till att begå sexuella aktiviteter, online eller ansikte mot ansikte.

Packade program

En fil i ett komprimeringsformat. Många operativsystem och appar innehåller kommandon som gör att du kan packa en fil så att den tar mindre minne. Anta till exempel att du har en textfil som innehåller tio på varandra följande mellanslagstecken. Normalt skulle detta kräva tio byte lagring.

Ett program som packar filer skulle dock ersätta mellanslagstecken med ett speciellt mellanslagsserietecken följt av antalet mellanslag som ersätts. I detta fall skulle de tio utrymmena endast kräva två byte. Detta är bara en packningsteknik - det finns många fler.

Väg

Den exakta vägbeskrivningen till en fil på en dator. Dessa riktningar beskrivs vanligtvis med hjälp av det hierarkiska arkiveringssystemet uppifrån och ner.

Rutten mellan två valfria punkter, till exempel kommunikationskanalen mellan två datorer.

Nätfiske

Handlingen att skicka ett e-postmeddelande till en användare som falskeligen påstår sig vara ett etablerat legitimt företag i ett försök att lura användaren till att överlämna privat information som kommer att användas för identitetsstöld. E-postmeddelandet uppmanar användaren att besöka

en webbplats där de ombeds att uppdatera personlig information, såsom lösenord och kreditkort, personnummer och bankkontonummer, som den legitima organisationen redan har. Webbplatsen är dock falsk och inrättad endast för att stjäla användarens information.

Foton

Photon är en innovativ, icke-påträngande Bitdefender-teknik, designad för att minimera prestandapåverkan från din säkerhetslösning. Genom att övervaka din dators aktivitet i bakgrunden skapar den användningsmönster som hjälper till att optimera uppstarts- och skanningsprocesser.

Polymorft virus

Ett hot som ändrar form för varje fil som den infekterar. Eftersom de inte har något konsekvent binärt mönster är sådana hot svåra att identifiera.

Hamn

Ett gränssnitt på en dator som du kan ansluta en enhet till. Persondatorer har olika typer av portar. Internt finns det flera portar för att ansluta diskenheter, bildskärmar och tangentbord. Externt har persondatorer portar för anslutning av modem, skrivare, möss och annan kringutrustning.

I TCP/IP- och UDP-nätverk, en slutpunkt till en logisk anslutning. Portnumret identifierar vilken typ av port det är. Till exempel används port 80 för HTTP-trafik.

Ransomware

Ransomware är ett skadligt program som försöker tjäna pengar på användare genom att låsa deras sårbara system. CryptoLocker, CryptoWall och TeslaWall, är bara några varianter som jagar användarnas personliga system.

Infektionen kan spridas genom att komma åt skräppostmeddelanden, ladda ner e-postbilagor eller installera appar, utan att låta användaren veta vad som händer på hans system. Dagliga användare och företag riktas mot ransomware-hackare.

Rapportfil

En fil som listar åtgärder som har inträffat. Bitdefender har en rapportfil som visar sökvägen som skannats, mapparna, antalet skannade arkiv och filer, hur många infekterade och misstänkta filer som hittades.

Rootkit

Ett rootkit är en uppsättning mjukvaruverktyg som ger åtkomst till ett system på administratörsnivå. Termen användes först för UNIX-operativsystemen och den hänvisade till omkompilerade verktyg som gav inkräktare administrativa rättigheter, så att de kunde dölja sin närvaro så att de inte syns av systemadministratörerna.

Den huvudsakliga rollen för rootkits är att dölja processer, filer, inloggningar och loggar. De kan också fånga upp data från terminaler, nätverksanslutningar eller kringutrustning, om de innehåller lämplig programvara.

Rootkits är inte skadliga till sin natur. Till exempel döljer system och till och med vissa appar viktiga filer med rootkits. Men de används mest för att dölja hot eller för att dölja närvaron av en inkräktare i systemet. I kombination med hot utgör rootkits ett stort hot mot integriteten och säkerheten i ett system. De kan övervaka trafik, skapa bakdörrar i systemet, ändra filer och loggar och undvika upptäckt.

Manus

En annan term för makro- eller batchfil, ett skript är en lista med kommandon som kan köras utan användarinteraktion.

Spam

Elektronisk skräppost eller skräpnyhetsgrupper. Allmänt känd som all oönskad e-post.

Spionprogram

All programvara som i hemlighet samlar in användarinformation via användarens internetanslutning utan hans eller hennes vetskap, vanligtvis i reklamsyfte. Spionprogram är vanligtvis paketerade som en dold komponent av gratisprogram eller shareware-program som kan laddas ner från internet; Det bör dock noteras att majoriteten av shareware och freeware-appar inte kommer med spionprogram. När det väl har installerats övervakar spionprogrammet användaraktivitet på internet och överför informationen i bakgrunden till någon annan. Spionprogram kan också samla information om e-postadresser och till och med lösenord och kreditkortsnummer.

Spionprograms likhet med ett trojansk hästhot är det faktum att användare omedvetet installerar produkten när de installerar något annat. Ett vanligt sätt att bli offer för spionprogram är att ladda ner vissa peer-to-peer filbytesprodukter som är tillgängliga idag.

Bortsett från frågorna om etik och integritet stjäl spionprogram från användaren genom att använda datorns minnesresurser och även genom att äta bandbredd då det skickar information tillbaka till spionprogrammets hembas via användarens internetanslutning. Eftersom spionprogram använder minne och systemresurser kan apparna som körs i bakgrunden leda till systemkrascher eller allmän systeminstabilitet.

Startobjekt

Alla filer som placeras i den här mappen öppnas när datorn startar. Till exempel kan en startskärm, en ljudfil som ska spelas upp när datorn startar, en påminnelseskalender eller appar vara startobjekt. Normalt placeras ett alias för en fil i den här mappen istället för själva filen.

Prenumeration

Köpeavtal som ger användaren rätt att använda en viss produkt eller tjänst på ett visst antal enheter och under en viss tid. Ett utgånget abonnemang kan förnyas automatiskt med den information som användaren lämnade vid första köpet.

Systemfältet

Systemfältet, som introducerades med Windows 95, finns i aktivitetsfältet i Windows (vanligtvis längst ner bredvid klockan) och innehåller miniatyrikoner för enkel åtkomst till systemfunktioner som fax, skrivare, modem, volym med mera. Dubbelklicka eller högerklicka på en ikon för att visa och komma åt detaljerna och kontrollerna.

TCP/IP

Transmission Control Protocol/Internet Protocol - En uppsättning nätverksprotokoll som ofta används på internet som tillhandahåller kommunikation över sammankopplade nätverk av datorer med olika hårdvaruarkitekturer och olika operativsystem. TCP/IP innehåller standarder för hur datorer kommunicerar och konventioner för att ansluta nätverk och dirigera trafik.

Hot

Ett program eller kod som läses in på din dator utan din vetskap och som körs mot din vilja. De flesta hot kan också replikera sig själva. Alla datorhot är konstgjorda. Ett enkelt hot som kan kopiera sig själv om och om igen är relativt lätt att producera. Även ett så enkelt hot är farligt eftersom det snabbt kommer att använda allt tillgängligt minne och få systemet att

stanna. En ännu farligare typ av hot är en som kan överföra sig själv över nätverk och kringgå säkerhetssystem.

Uppdatering av hotinformation

Det binära mönstret för ett hot, som används av säkerhetslösningen för att upptäcka och eliminera hotet.

Trojan

Ett destruktivt program som maskerar sig som en godartad app. Till skillnad från skadliga program och maskar replikerar trojaner inte sig själva men de kan vara lika destruktiva. En av de mest lömska typerna av trojanska hästhot är ett program som påstår sig befria din dator från hot men istället introducerar hot på din dator.

Termen kommer från en berättelse i Homeros Iliaden, där grekerna ger en gigantisk trähäst till sina fiender, trojanerna, skenbart som ett fredsoffer. Men efter att trojanerna släpat hästen innanför sina stadsmurar, smyger grekiska soldater ut ur hästens ihåliga mage och öppnar stadsportarna, så att deras landsmän kan strömma in och fånga Troja.

Uppdatering

En ny version av en mjuk- eller hårdvaruprodukt utformad för att ersätta en äldre version av samma produkt. Dessutom kontrollerar installationsrutinerna för uppdateringar ofta att en äldre version redan är installerad på din dator; Om inte kan du inte installera uppdateringen.

Bitdefender har sin egen uppdateringsfunktion som låter dig söka manuellt efter uppdateringar, eller låta den uppdatera produkten automatiskt.

Virtual Private Network (VPN)

Är en teknik som möjliggör en tillfällig och krypterad direktanslutning till ett visst nätverk över ett mindre säkert nätverk. På så sätt är det säkert och krypterat att skicka och ta emot data, svårt att fångas av snokare. Ett bevis på säkerhet är autentiseringen, som endast kan göras med ett användarnamn och lösenord.

Mask

Ett program som sprider sig över ett nätverk och reproducerar sig själv allt eftersom. Den kan inte koppla sig till andra program.