GHIDUL UTILIZATORULUI

Bitdefender CONSUMER SOLUTIONS

VPN

Bitdefender VPN

Manual de utilizare

Publication date 02/07/2024

Termeni legali

Bitdefender

Cuprins

DESPRE ACEST GHID

Scopul și publicul țintă

Acest ghid este destinat tuturor utilizatorilor Bitdefender care au ales Bitdefender VPN drept serviciul preferat care să le asigure anonimitatea online prin criptarea traficului de intrare și ieșire de pe PC, Mac sau pe dispozitivele lor mobile.

Vei afla cum să configurezi și să utilizezi Bitdefender VPN pentru a-ți proteja identitatea și activitățile online împotriva hackerilor, furnizorilor de servicii de internet și celor care te spionează. Vei afla cum să valorifici la maxim serviciul Bitdefender.

Vă dorim o prelegere plăcută și utilă.

Cum să folosiți acest ghid

Acest ghid este organizat în mai multe teme majore:

Ce este Bitdefender VPN (pagina 4)

Începe să utilizezi Bitdefender VPN și află ce este acest produs și cum te poate ajuta să te protejezi oferindu-ți o anonimitate online reală.

Cum să utilizezi Bitdefender VPN (pagina 13)

Află cum să interacționezi cu Bitdefender VPN și cu interfața sa de utilizare.

Bitdefender VPN Setări și caracteristici (pagina 17)

Află mai multe detalii despre setările și funcționalitățile Bitdefender VPN.

Obține ajutor (pagina 31)

Unde să căutați și unde să cereți ajutor în cazul în care apar situații neprevăzute.

Convenții utilizate în acest ghid

Convenții tipografice

Manualul conține diferite stiluri de text, pentru o lectură cât mai ușoară. Aspectul și semnificația acestora sunt prezentate în tabelul de mai jos.

Aspect	Descriere
sample syntax	Exemplele de sintaxă sunt imprimate cu caractere monospaced.
https://www.bitdefender.com	Linkurile URL indică locații externe, pe serverele http sau ftp.
documentation@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.
Despre acest Ghid (pagina 1)	Acesta este un link intern, care vă direcționează către o locație din document.
filename	Fișierul și directoarele sunt tipărite folosind monospaced font.
opțiune	Toate opțiunile de produs sunt imprimate folosind caractere **îngroșate**.
cuvânt cheie	Cuvintele cheie sau expresiile importante sunt evidențiate folosind caractere **îngroșate**.

Atenționări

Atenționările sunt note din text, marcate grafic, care oferă informații suplimentare legate de paragraful respectiv.

Nota

Nota este o scurtă observație. Deși pot fi omise, notele pot furniza informații importante, cum ar fi o caracteristică specifică sau un link către un subiect relevant.

Important

Segmentele marcate astfel necesită atenția ta și nu este recomandat să le omiți. De obicei, aici sunt furnizate informații importante, dar nu esențiale.

Avertizare

Acestea sunt informații esențiale, care trebuie tratate cu o atenție deosebită. Dacă urmezi indicațiile, nu se va întâmpla nimic rău. Este recomandat să citești și să înțelegi despre ce este vorba, deoarece aici se descrie ceva extrem de riscant.

Comentarii

Te invităm să participi la procesul de îmbunătățire al manualului. Toate informațiile prezentate au fost testate și verificate în mod riguros. Te rugăm să ne scrii despre orice inexactități pe care le vei găsi în acest manual, precum și să propui moduri prin care îl putem îmbunătăți, astfel încât să îți putem furniza o documentație ireproșabilă.

Anunțați-ne trimițând un e-mail la documentation@bitdefender.com. Scrieți toate e-mailurile dvs. legate de documentație în engleză, astfel încât să le putem procesa eficient.

1. CE ESTE BITDEFENDER VPN

VPN-ul servește ca un tunel între dispozitivul dvs. și rețeaua la care vă conectați, securizarea conexiunii, criptarea datelor utilizând criptare militară și ascunderea adresei IP oriunde v-ați afla. Traficul dvs. este redirecționat printr-un server separat; astfel încât dispozitivul dumneavoastră nu poate fi identificat de către ISP-ul dumneavoastră, prin multitudinea de alte dispozitive care utilizează serviciile noastre. În plus, în timp ce sunteți conectat la internet prin Bitdefender VPN, puteți accesa conținut care este în mod normal restricționat în anumite zone.

Notă

Unele țări practică cenzura online, prin urmare utilizarea aplicațiilor VPN pe teritoriul lor este interzisă prin lege. Pentru a evita consecințele legale, este posibil să apară un mesaj de avertizare atunci când încerci să utilizezi caracteristica Bitdefender VPN pentru prima dată. Prin continuarea utilizării acestei caracteristici, confirmi că îți sunt cunoscute reglementările aplicabile din țara respectivă și riscurile la care ai putea fi expus.

1.1. Protocoale de criptare

Seturile implicite de suite de cifruri activate în clientul și serverul Hydra sunt disponibile mai jos. Toate celelalte suite de cifruri sunt dezactivate.

Suite de cifruri în clientul 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

Notă

Setul pe partea de server este mult mai restrictiv și atât clientul, cât și serverul Hydra vor respinge orice alt mod de criptare în afară de GCM cu algoritm AES. Serverul Hydra susține prioritatea suitelor de cifruri pe partea de server și va respinge handshake-ul TLS dacă este solicitată de client o suită de cifruri mai slabă. Această listă poate fi configurată și în modul Runtime pe partea de server.

2. ABONAMENTE VPN

Cu Bitdefender VPN, poți opta pentru unul dintre aceste două tipuri de abonamente:

- Abonamentul Basic
- Abonamentul Premium

2.1. Abonament Basic

Bitdefender VPN îți oferă 200 MB de trafic gratuit pe zi per dispozitiv pentru a-ți securiza conexiunea ori de câte ori ai nevoie și îți permite să te conectezi la o singură locație care nu poate fi schimbată.

Abonamentul Basic este disponibil pentru orice utilizator care descarcă Bitdefender VPN

2.2. Abonament Premium

Pentru a obține acces nelimitat la toate caracteristicile incluse în Bitdefender VPN, actualizează la versiunea Premium. Utilizatorii care au un abonament Premium VPN activ beneficiază de trafic protejat nelimitat și se pot conecta la oricare șdintre serverele noastre din toată lumea.

În cazul abonamentului Premium, există două tipuri de abonamente: abonamentul lunar și abonamentul anual.

- Abonamentul lunar: alegând acest tip de abonament, vei fi facturat în fiecare lună pentru serviciile Premium VPN. Poți renunța oricând dorești.
- Abonamentul anual: necesită o singură plată și îți oferă acces la serviciile noastre Premium VPN pentru un an întreg.

2.3. Cum să actualizezi la Premium VPN

Cel mai ușor mod prin care poți actualiza la versiunea Premium a Bitdefender VPN este să selectezi butonul **Upgrade** situat în partea de jos a interfeței principale. Alege tipul de abonament dorit și apoi urmează instrucțiunile afișate pe ecran.

Dacă ai deja un cod de activare, urmează instrucțiunile de mai jos:

- **Pentru utilizatorii Windows**
  1. Selectează pictograma Contul meu din partea stângă a interfeței VPN.
  2. Fă clic pe **Adăugare aici**.
  3. Introdu codul pe care l-ai primit prin e-mail, apoi selectează butonul **Activare cod**.

- **Pentru utilizatorii de macOS**
  1. Fă clic pe rotița din colțul din dreapta sus a interfeței VPN și selectează **Contul meu**.
  2. Clic **Adaugă-l aici**.
  3. Introduceți codul primit prin e-mail, apoi faceți clic pe **Activați codul** buton.

- **Pentru utilizatorii Android**
  1. Apasă pe rotița din colțul din dreapta sus a interfeței VPN și selectează **Contul meu**.
  2. Atinge **Adăugare cod**.
  3. Introduceți codul primit prin e-mail, apoi faceți clic pe **Activați codul** buton.

- **Pentru utilizatorii iOS**
  1. Atingeți roata dințată din colțul din dreapta sus al interfeței VPN și selectați **Contul meu**.
  2. Atingeți **Adăugați cod**.
  3. Introduceți codul primit prin e-mail, apoi faceți clic pe **Activați codul** buton.

3. INSTALARE

3.1. Pregătirea pentru instalare

Pentru a instala Bitdefender VPN fără probleme, trebuie sa parcurgi acești pași prealabili:

- Asigurați-vă dacă dispozitivul pe care doriți să instalați Bitdefender îndeplinește cerințele de sistem. În cazul în care dispozitivul nu întrunește toate cerințele de sistem, Bitdefender nu va fi instalat sau nu va funcționa în mod corespunzător, determinând reducerea vitezei de funcționare și instabilitatea sistemului.
  Pentru lista completă a cerințelor de sistem, consultă Cerințe de sistem (pagina 8)
- Autentifica-te pe dispozitiv cu datele unui cont de administrator.
- Se recomandă ca, în timpul instalării, dispozitivul tău să fie conectat la internet, chiar atunci când instalarea se face de pe un CD/DVD. Dacă sunt disponibile versiuni mai noi ale fișierelor aplicației decât cele incluse în pachetul de instalare, Bitdefender le va descărca și le va instala.

3.2. Cerințe de sistem

- **Pentru utilizatorii de Windows**
  - **Sistem de operare:** Windows 7 cu Service Pack 1, Windows 8, Windows 8.1 Windows 10 și Windows 11
  - **Memorie (RAM):** 1 GB
  - **Spațiu liber disponibil pe hard disk:** 500 MB
  - **Net Framework:** minimum versiunea 4.5.2

    Important
    Performanța sistemului poate fi afectată pe dispozitivele care au procesoare de generație veche.

- **Pentru utilizatorii de macOS**
  - **Sistem de operare:** macOS Sierra (10.12) sau o versiune ulterioară

- **Spațiu liber disponibil pe hard disk:** 100 MB

- **Pentru utilizatorii de Android**
  - **Sistem de operare:** Android 5.0 sau o versiune ulterioară
  - **Spațiu de stocare:** 100 MB
  - O conexiune activă la Internet

- **Pentru utilizatorii iOS**
  - **Sistem de operare:** iOS 12 sau mai recent
  - **Spațiu de stocare pe iPhone:** 50 MB
  - **Spațiu de stocare pe iPad:** 100 MB
  - O conexiune la Internet activă

3.3. Instalarea Bitdefender VPN

Pentru a începe instalarea, urmează instrucțiunile care corespund sistemului de operare pe care îl utilizezi:

- **Pentru utilizatorii de Windows**

  1. Pentru a începe instalarea Bitdefender VPN pe un PC Windows, trebuie doar să descarci kitul de instalare accesând https://www.bitdefender.com/solutions/vpn/download sau e-mailul primit după o achiziție.
  2. Fă dublu clic pe asistentul de instalare pentru a-l executa.
  3. Alege Da dacă se afișează fereastra de dialog UAC (User Account Control).
  4. Așteaptă până la finalizarea descărcării.
  5. Selectează limba produsului, utilizând meniul derulant al instrumentului de instalare.
  6. Bifează caseta „Confirm că am citit și sunt de acord cu Contractul de abonament și Politica de confidențialitate”, apoi selectează **LANSARE INSTALARE**.
  7. Așteaptă până când instalarea este finalizată.

8. **CONECTEAZĂ-TE** cu contul tău Bitdefender Central. Dacă nu ai un cont Central, înscrie-te pentru a-ți crea unul, selectând butonul **CREARE CONT**.
9. Alege **Am un cod de activare** dacă ai achiziționat un abonament Premium VPN.
   În caz contrar, poți alege **ÎNCEPE VERSIUNEA DE EVALUARE** pentru a testa produsul gratuit timp de 7 zile înainte de a-l achiziționa.
10. Introdu codul pe care l-ai primit prin e-mail, apoi selectează butonul **ACTIVARE PREMIUM**.
11. După o scurtă așteptare, Bitdefender VPN este instalat și gata să fie utilizat pe computerul tău.

❍ **Pentru utilizatorii de macOS**

1. Pentru a începe instalarea Bitdefender VPN pe un macOS, trebuie doar să descarci kitul de instalare accesând https://www.bitdefender.com/solutions/vpn/download sau e-mailul primit după o achiziție.
2. Instrumentul de instalare va fi salvat pe Mac. În directorul Descărcări, faceți dublu clic pe directorul care conține pachetul .
3. Urmează instrucțiunile de pe ecran. Alege **Continuare**.
4. Va trebui să urmezi pașii de pe ecran necesari pentru a instala Bitdefender VPN pe dispozitivul tău Mac. Fă dublu clic pe butonul **Continuare**.
5. Selectează **Confirm**, după ce ai citit și ai confirmat termenii și condițiile contractului de licențiere pentru software.
6. Fă clic pe **Instalare**.
7. Introdu un nume de utilizator și o parolă, apoi selectează **Instalare software**.
8. Vei fi anunțat că a fost blocată o extensie de sistem semnată de Bitdefender. Selectează **Deschide preferințele de securitate**.
9. Selectează pictograma de blocare pentru a debloca extensia.
   Introdu un nume de utilizator și o parolă, apoi apasă pe **Deblocare**.

10. Selectează **Permite** pentru a încărca extensia de sistem BitdefenderBitdefender. Apoi închide fereastra Securitate și confidențialitate și asistentul de instalare.
11. Accesează pictograma care înfățișează un scut din bara de meniu, apoi **Conectează-te** cu contul tău Bitdefender Central. Dacă nu ai un cont Central, înregistrează-te pentru unul.
12. Alege Am un **cod de activare** dacă ai achiziționat un abonament Premium VPN.
    În caz contrar, poți alege **ÎNCEPE ÎNCERCAREA** pentru a testa produsul gratuit timp de 7 zile înainte de a vă angaja să plătiți pentru el.
13. Introduceți codul primit prin e-mail, apoi faceți clic pe **Activați codul** buton.
14. După o scurtă așteptare, Bitdefender VPN este instalat și gata să fie utilizat pe dispozitivul tău Mac.

❍ **Pentru utilizatorii de Android**

1. Pentru a instala Bitdefender VPN pe Android, mai întâi deschide aplicația **Google Play Store** pe smartphone-ul sau tableta ta.
2. Caută Bitdefender VPN și selectează această aplicație.
3. Apasă pe butonul **Instalare** și așteaptă până la finalizarea descărcării.
4. Apasă **Deschide** pentru a lansa aplicația.
5. Bifează caseta „Sunt de acord cu Contractul de abonament și Politica de confidențialitate”, apoi selectează **Continuare**.
6. **Conectează-te** cu contul tău Bitdefender Central. Dacă nu ai un cont Central, înregistrează-te pentru a-ți crea unul, atingând **Creare cont**.
7. Alege **Am un cod de activare** dacă ai achiziționat un abonament Premium VPN.
   În caz contrar, poți alege Începe versiunea de evaluare de 7 zile pentru a testa produsul gratuit timp de 7 zile înainte de a-l achiziționa.
8. Introdu codul pe care l-ai primit prin e-mail, apoi apasă pe **Activare cod**.

- **Pentru utilizatorii iOS**

  1. Pentru a instala Bitdefender VPN pe iOS, întâi deschide **App Store** pe iPhone-ul sau iPad-ul tău.
  2. Caută Bitdefender VPN și selectați această aplicație.
  3. Apasă pe pictograma **Obține** și așteaptă până la finalizarea descărcării.
  4. Atingeți **Deschis** pentru a rula aplicația.
  5. Bifează caseta **Sunt de acord cu Contractul de abonament și Politica de confidențialitate**, apoi selectează **Continuare**.
  6. **Conectează-te** cu contul tău Bitdefender Central. Dacă nu ai un cont, înregistrează-te pentru a-ți crea unul, atingând **Creare cont**.
  7. Atinge **Permite** dacă dorești să primești notificări Bitdefender VPN.
  8. Alege **Am un cod de activare** dacă ați achiziționat un abonament Premium VPN.
     În caz contrar, puteți alege Start 7 days Trial pentru a testa produsul gratuit timp de 7 zile înainte de a vă angaja să plătiți pentru el.
  9. Introdu codul primit prin e-mail, apoi atinge **Activați codul**.

4. CUM SĂ UTILIZEZI BITDEFENDER VPN

4.1. Activare Bitdefender VPN

- **Pentru Windows**
  Pentru a accesa **interfața principală a Bitdefender VPN**, folosește una dintre următoarele metode:
  - **Din bara de sistem**
    Fă clic dreapta pe pictograma scut roșu din bara de sistem și apoi selectează opțiunea **Afișare** din meniu.
  - **Din interfața Bitdefender**
    Dacă un produs de securitate Bitdefender, precum Bitdefender Total Security sau Bitdefender Antivirus Plus etc., este deja instalat pe computerul tău Windows, poți deschide Bitdefender VPN de acolo:
    1. Fă clic pe **Confidențialitate** din bara din partea stângă a interfeței Bitdefender.
    2. Fă clic pe **Deschide VPN** din panoul VPN.
  - **De pe desktop**
    Fă dublu clic pe comanda rapidă Bitdefender VPN de pe desktopul tău.
- **Pentru macOS**
  Poți deschide aplicația Bitdefender VPN făcând clic pe pictograma din bara de meniu din partea dreaptă sus a ecranului.
  Dacă scutul Bitdefender nu apare în bara de meniu, folosește-ți Launchpad-ul Mac sau opțiunea Finder pentru a-l găsi:
  - **Din Launchpad**
    1. Apasă pe **F4** de pe tastatura ta pentru a lansa aplicația Lanchpad pe Mac-ul tău.
    2. Navighează pe paginile cu aplicații instalate până când găsești aplicația Bitdefender VPN. Ca alternativă, poți tasta **Bitdefender VPN** în Launchpad pentru a-ți filtra rezultatele.

3. Când ai găsit aplicația Bitdefender VPN, fă clic pe pictograma sa pentru a o fixa în bara de meniu.

- **Din Finder**

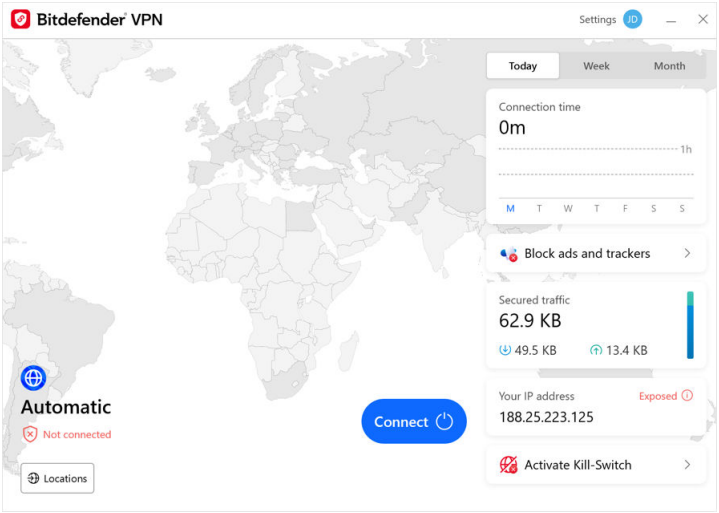
1. Fă clic pe **Finder** în partea de jos stânga a Dock (Finder este pictograma care arată ca un pătrat albastru cu o față zâmbitoare).
2. Apoi fă clic pe **Go** (Mergi la) în partea stângă sus a ecranului, în bara de meniu.
3. Selectează opțiunea **Aplicații** din meniu pentru a accesa directorul Aplicații de pe Mac-ul tău.
4. Din directorul Aplicații, deschide directorul **Bitdefender** și apoi fă dublu clic pe aplicația **Bitdefender VPN**.

Notă

Pentru a accesa Bitdefender VPN pe dispozitivele mobile Android sau iOS, trebuie doar să deschizi aplicația Bitdefender VPN după ce ai instalat-o.

4.2. Cum să te conectezi la Bitdefender VPN

Interfața VPN afișează starea aplicației: activată sau dezactivată. Locația serverului pentru utilizatorii care folosesc versiunea gratuită este setată automat de Bitdefender pe cel mai potrivit server, în vreme ce utilizatorii versiunii premium au posibilitatea de a modifica locația serverului la care doresc să se conecteze selectând-o din lista de Locații virtuale. Pentru a te conecta sau deconecta, trebuie doar să faci clic pe butonul pornire/oprire din interfața VPN.



- **Pentru Windows:** Pictograma barei de sistem afișează o bifă verde atunci când aplicația VPN este activată și o bifă neagră când aceasta este dezactivată. Atunci când ești conectat la o locație selectată manual, în interfața principală se afișează adresa IP.
- **Pentru macOS:** Pictograma barei de meniu este afișată în culoarea neagră când VPN este activată și în alb când VPN este deconectată. Fă clic pe butonul circular din centrul interfeței și așteaptă stabilirea conexiunii.
- **Pentru Android și iOS:** Pentru a te conecta la Bitdefender VPN pentru Android, iOS și iPadOS:
  - **Din aplicația Bitdefender VPN:** Pentru a activa sau dezactiva aplicația, trebuie doar să atingi butonul pornire/oprire din interfața VPN. Se afișează starea aplicației Bitdefender VPN.
  - **Din aplicația Bitdefender Mobile Security:**
    1. Accesează pictograma VPN din bara de navigare de jos a Bitdefender Mobile Security.
    2. Atinge **ACTIVARE** de fiecare dată când vrei să fii protejat atunci când ești conectat la rețele wireless nesigure. Atinge **DEZACTIVARE** când vrei să dezactivezi conexiunea VPN.

4.3. Cum te conectezi la un alt server

Cu un abonament Premium, Bitdefender VPN îți permite să te conectezi la oricare dintre serverele noastre din întreaga lume, în orice moment. Pentru a face asta, va trebui să:

1. Deschide aplicația Bitdefender VPN
2. Apeși pe butonul **Locație virtuală** în partea interioară a interfeței.
3. Selectezi orice țară dorești.
4. Apeși pe butonul **Conectare la [țara dorită]** în partea interioară a interfeței.

- Pictograma barei de sistem afișează o bifă verde când VPN-ul este conectat.
- Adresa IP a serverului virtual este afișată pe ecranul de pornire în timp ce este conectat la Bitdefender VPN.
- Un rezumat al timpului de conectare, volumul de trafic securizat și ultimele 5 locații la care v-ați conectat sunt afișate și pe tabloul de bord principal.

5. BITDEFENDER VPN SETĂRI ȘI CARACTERISTICI

5.1. Cum să accesezi Setările

Pentru a accesa setările Bitdefender VPN, va trebui să urmezi pașii de mai jos:

- **Pe Windows**
  1. Deschide aplicația Bitdefender VPN de pe dispozitivul tău, făcând dublu clic pe pictograma acesteia în system tray sau făcând clic dreapta pe aceasta și selectând Afișare.
  2. Selectează butonul **Setări** (reprezentat printr-o rotiță) în partea stângă a interfeței.

- **Pe macOS**
  1. Deschide aplicația Bitdefender VPN pe dispozitivul tău macOS selectând pictograma sa din bara de meniu.
  2. Selectează butonul în formă de rotiță din colțul din dreapta sus a interfeței Bitdefender VPN și selectează Setări.

- **Pe Android**
  1. Deschide aplicația Bitdefender VPN pe dispozitivul tău.
  2. Selectează butonul în formă de rotiță din colțul din dreapta sus a interfeței Bitdefender VPN.

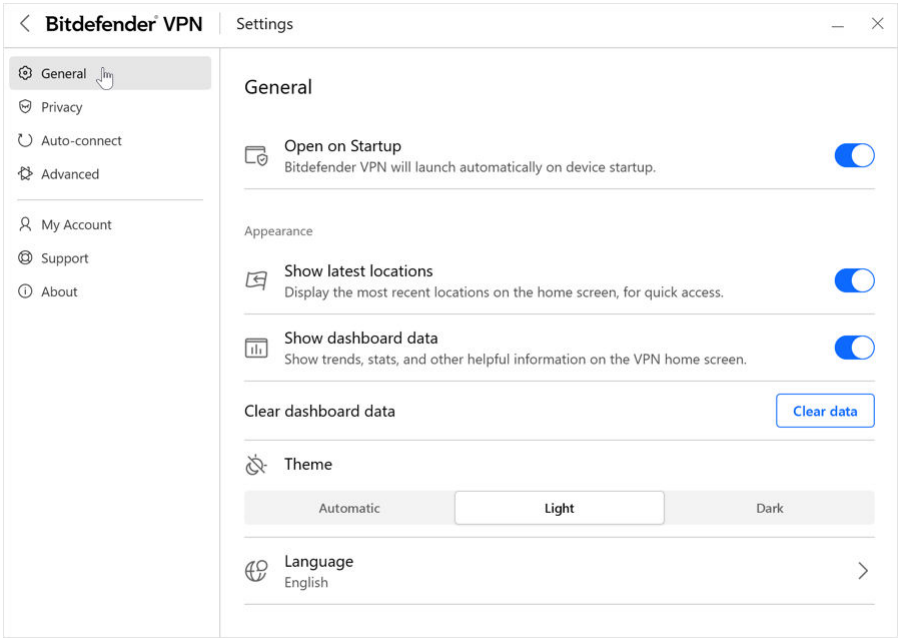
- **Pe iOS**
  1. Deschide Bitdefender VPN aplicația pe dispozitivul dvs.
  2. Faceți clic pe butonul roții dințate din colțul din dreapta sus al Bitdefender VPN interfata.

5.2. General

Aici puteți modifica următoarele:

- **Deschide la pornire**– Bitdefender VPN se va lansa automat la pornirea dispozitivului.

- **Afișează cele mai recente locații**– Afișați cele mai recente locații pe ecranul de start, pentru acces rapid.
- **Afișați datele tabloului de bord** – Afișați tendințe, statistici și alte informații utile pe ecranul de pornire VPN.
- **Ștergeți datele tabloului de bord**– Toate datele din tabloul de bord vor fi șterse și toate contoarele resetate.
- **Temă**– Temă luminoasă/întunecată
- **Limba**– Schimbați limba Bitdefender VPN.
- **Notificări**– Gestionați-vă preferințele de notificări.
- **Ajutați la îmbunătățirea Bitdefender VPN**– Trimiteți rapoarte anonime despre produse pentru a ne ajuta să vă îmbunătățim experiența.
- **Resetează toate setările**– Resetați VPN-ul la setările sale originale fără a-l reinstala.



5.3. Caracteristici

5.3.1. Confidențialitate

Internet Kill-Switch

Comutatorul pentru oprirea conexiunii la internet este o nouă funcție care a fost implementată în Bitdefender VPN. Atunci când este activat, suspendă temporar tot traficul pe internet în cazul în care conexiunea VPN se întrerupe accidental. Imediat ce revii în mediul online, conexiunea VPN va fi restabilită.

Pentru a activa comutatorul pentru oprirea conexiunii la internet, urmează pașii de mai jos:

- **Pe Windows**
  1. Deschide aplicația Bitdefender VPN de pe dispozitivul tău, făcând dublu clic pe pictograma acesteia în system tray sau făcând clic dreapta pe aceasta și selectând **Afișare**.
  2. Faceți clic pe **Setări** butonul (reprezentat printr-o roată dințată) din partea stângă a interfeței.
  3. Selectează opțiunea **Avansat**.
  4. Activează opțiunea **Comutator pentru oprirea conexiunii la internet**.

- **Pe Android**
  1. Deschide Bitdefender VPN aplicația pe dispozitivul dvs.
  2. Faceți clic pe butonul roții dințate din colțul din dreapta sus al Bitdefender VPN interfata.
  3. Din secțiunea **Setări**, activează opțiunea de oprire a conexiunii **Kill-Switch**.

- **Pe iOS**
  1. Deschide Bitdefender VPN aplicația pe dispozitivul dvs.
  2. Faceți clic pe butonul roții dințate din colțul din dreapta sus al Bitdefender VPN interfata.
  3. Sub **Setări**, activați **Kill-Switch** opțiune.

Notă

Această caracteristică este disponibilă și pentru dispozitivele macOS cu sisteme de operare 10.15.4 sau versiuni ulterioare.

Ad blocker și Anti-tracker

Aceste caracteristici sunt proiectate să te ajute să îți păstrezi confidențialitatea în siguranță și să te bucuri de lumea digitală fără reclame enervante sau companii care stau cu ochii pe tine. Acestea contribuie la blocarea reclamelor și a programelor de monitorizare online.

Ad blocker

Caracteristica **Ad blocker** este folosită pentru a bloca reclame, ferestre pop-up, reclame video enervante sau bannere publicitare, în timpul navigării. Datorită acesteia, site-urile web se vor încărca mai repede și vor fi mai aerisite, și vei putea interacționa cu ele în siguranță.

Pentru a activa Ad blocker:

1. Găsește caracteristica **Ad blocker și Antitracker** în secțiunea **Setări**.
2. Comută butonul în poziția **Pornit**.

Anti-tracker

Funcția **Anti-tracker** se folosește pentru a bloca programele de monitorizare configurate de agențiile de publicitate să te urmărească și să îți alcătuiască un profil online. Unele site-uri web pot funcționa defectuos atunci când se blochează aceste programe, dar adăugarea adreselor URL ale site-urilor respective pe lista albă poate remedia această problemă.

Pentru a activa Anti-tracker:

1. Localizați **Blocant reclame și Antitracker** caracteristică în **Setări**.
2. Comutați comutatorul la **PE** poziție.

Lista de excepții

Este posibil ca unele site-uri web să nu se încarce corespunzător în cazul în care codul tracker și reclamele acestora sunt blocate. Adăugarea adreselor URL ale acestor domenii pe lista albă poate remedia problema, dar reține că, în timp ce navighezi pe aceste site-uri web, vei vedea reclame și codul lor tracker va fi activ.

Adaugă site-uri web cărora vrei să le permiți să afișeze reclame și să utilizeze trackere astfel:

1. Localizați **Blocant reclame și Antitracker** caracteristică în **Setări**.
2. Fă clic pe linkul **Gestionare**. Apoi, accesează secțiunea Listă albă din această fereastră și apasă pe linkul **Gestionare** corespunzător.
3. Fă clic pe **Adăugare site web** și introdu adresa URL dorită.

5.3.2. Conectare automată

Atunci când te deplasezi, lucrezi dintr-o cafenea sau aștepți în aeroport, conectarea la o rețea wireless publică pentru a face plăți, verifica e-mail-ul sau conturile pe rețelele sociale poate fi soluția cea mai rapidă. Însă pot exista curioși care să încerce să-ți fure datele personale, urmărind informațiile care trec prin rețea.

Pentru a te proteja împotriva pericolelor la care te expun hotspot-urile wireless publice nesecurizate și necriptate, Bitdefender VPN include o funcție de auto-conectare. Asta înseamnă că Bitdefender VPN poate fi activat automat în anumite situații, în funcție de preferințele tale și de sistemul de operare pe care îl rulezi.

- În **Windows**, caracteristica de auto-conectare poate fi activată pentru următoarele situații:
  - **Pornire:** Activează VPN de la pornirea Windows.
  - **Rețea Wi-Fi nesecurizată:** Utilizează VPN atunci când te conectezi la rețelele Wi-Fi publice sau nesecurizate.
  - **Aplicații peer-to-peer:** Activează VPN atunci când lansezi o aplicație de partajare a fișierelor de tip peer-to-peer.
  - **Aplicații și domenii:** Folosește întotdeauna VPN când accesezi anumite aplicații și site-uri web.

> **Notă**
>
> 1. Fă clic pe linkul **GESTIONARE**.
> 2. Navighează la locația aplicației pentru care dorești să utilizezi VPN-ul, selectează denumirea aplicației și fă clic pe **Adăugare**.

- **Categorii de site-uri web:** Activează VPN atunci când accesezi anumite categorii de site-uri web. Bitdefender VPN se poate activa automat pentru următoarele categorii de site-uri web:
  - Financiar
  - Plăți online
  - Sănătate
  - Partajare de fișiere
  - Întâlniri online
  - Conținut pentru adulți

  > **Notă**
  > Pentru fiecare categorie, poți selecta un server diferit la care să se conecteze aplicația VPN.

- În **macOS**, caracteristica de auto-conectare poate fi activată pentru următoarele situații:
  - **Pornire:** Activează VPN de la pornirea macOS.
  - **Wi-Fi nesecurizat:** Utilizați VPN-ul ori de câte ori vă conectați la rețele Wi-Fi publice sau nesecurizate.
  - **Aplicații peer-to-peer:** Conectați-vă la VPN când porniți o aplicație de partajare de fișiere peer-to-peer.
  - **Aplicații:** Activează întotdeauna VPN pentru anumite aplicații.
- Pe **Android** și **iOS** Bitdefender VPN poate fi configurat pentru a se activa automat doar atunci când folosești rețele Wi-Fi nesecurizate sau publice.

5.3.3. Avansat

Split tunneling (Tunel distinct)

Caracteristica de tunel divizat (split tunneling) a rețelei private virtuale (VPN) îți permite să direcționezi o parte din traficul aplicațiilor sau dispozitivelor printr-un VPN criptat, în timp ce alte aplicații sau dispozitiv au acces direct la internet. Această caracteristică este, în mod special, utilă dacă dorești să beneficiezi de servicii care funcționează cel mai bine

atunci când locația ta este cunoscută, bucurându-te în același timp de acces sigur la comunicări și date care pot fi sensibile.

Prin activarea caracteristicii **Split tunneling** (tunel divizat), anumite aplicații și site-uri web vor evita canalul VPN și vor accesa direct internetul.

Pentru a gestiona aplicațiile și site-urile web care evită canalul VPN:

1. Fă clic pe linkul de **Gestionare** după ce ai activat caracteristica.
2. Fă clic pe butonul **Adăugare**.
3. Navighează la locația aplicației în cauză sau introdu URL-ul site-ului web dorit, apoi fă clic pe **Adăugare**.

> **Notă**
> Prin adăugarea unui site web, întregul domeniu, inclusiv toate subdomeniile acestuia, vor fi evitate.

> **Important**
> Pe dispozitivele **macOS**, caracteristica de tunel divizat (Split tunneling) este disponibilă doar pentru site-uri web.

Optimizarea traficului aplicațiilor

Caracteristica Optimizarea traficului aplicațiilor a Bitdefender VPN îți permite să stabilești traficul cu prioritate pentru aplicațiile cele mai importante pe dispozitivul tău fără să îți expui conexiunea la riscuri pentru confidențialitate. Aplicațiile VPN redirecționează traficul de internet printr-un tunel sigur fără să folosească algoritmi de criptare puternici pentru a-l proteja.

Însă, această combinație de tehnici poate prezenta anumite dezavantaje, care se referă în principal la viteza conexiunii. Anumiți factori pot provoca încetinirea conexiunii, cel mai frecvent fiind distanța față de serverul la care ești conectat, traficul aglomerat pe rețea și utilizarea mare a lățimii de bandă. Dacă ai simțit că uneori Bitdefender VPN generează o povară inutilă asupra conexiunii tale și observi constant o încetinire, există o soluție mai bună decât deconectarea.

Cum funcționează caracteristica Optimizarea traficului aplicațiilor?

Anumite aplicații și servicii, precum platformele de streaming, clienții de torente și jocurile necesită o lățime de bandă mai mare. Utilizarea

continuă a acestora ți-ar putea afecta viteza conexiunii la internet. Redirecționarea traficului printr-un tunel VPN oricum provoacă o încetinire a conexiunii tale. Suprasolicitarea conexiunii îți poate afecta serios experiența online.

Caracteristica Optimizarea traficului aplicațiilor a Bitdefender VPN te poate ajuta să combați problema încetinirii conexiunii VPN, prin asocierea acestei conexiuni cu prioritate cu aplicația dorită. Funcția îți permite să decizi ce aplicații ar trebui să primească mare parte din trafic, apoi alocă resursele în mod corespunzător. De exemplu, dacă ești într-o întâlnire și observi că apelul tău are o calitate sub cea normală, Optimizarea traficului aplicațiilor îți permite să aloci traficul cu prioritate aplicației de conferință video pentru rezultate mai bune.

În mod normal, utilizatorii VPN ar recurge la închiderea tuturor proceselor de pe dispozitiv care interferează cu calitatea conexiunii sau chiar la dezactivarea conexiunii VPN pentru a obține o viteză de internet mai mare. Caracteristica Optimizarea traficului aplicațiilor îți permite să te bucuri de protecție neîntreruptă a confidențialității tale fără compromiterea vitezei conexiunii.

Utilizarea caracteristicii Optimizarea traficului aplicațiilor

Momentan, această caracteristică este disponibilă doar pe dispozitivele Windows și îți permite să aloci trafic cu prioritate pentru până la 3 aplicații.

Urmează acești pași pentru a o activa și a o configura cu un efort minim:

1. Lansează aplicația Bitdefender VPN pe computerul tău Windows.
2. Fă clic pe butonul din bara laterală pentru a accesa setările conexiunii VPN.
3. Accesează fila **General** și activează caracteristica **Optimizarea traficului aplicațiilor**. Culoarea butonului se va schimba din gri în albastru.

Pentru a gestiona aplicațiile selectate ca prioritare de această caracteristică:

1. Apasă pe**Administra**legătură.
2. Navighează la locația aplicației pentru care dorești să optimizezi traficul, selectează denumirea aplicației, apoi fă clic pe **Adăugare**. Aplicația va apărea la secțiunea **Cu prioritate**.

> **Notă**
> Ca alternativă, dacă ai deschis recent aplicația pe care dorești să o selectezi ca prioritară, apasă butonul + în fereastra Optimizarea traficului aplicațiilor.

3. Dezactivează și reactivează Bitdefender VPN după ce ai adăugat și ai eliminat aplicații din listă.

Pentru a elimina o aplicație din Optimizarea traficului aplicațiilor, trebuie doar să faci clic pe pictograma de lângă denumirea aplicației.

> **Notă**
> Aplicația de optimizare a traficului nu este disponibil pe macOS.

Protocol

Aici puteți alege tipul de protocol pe care doriți să îl utilizați pentru transferul de date. Sunt disponibile următoarele opțiuni:

- **Automat** - Bitdefender VPN va selecta protocolul optim pentru dispozitivul și rețeaua dvs.
- **Catapulta Hidra** - Rapid și sigur, ideal pentru streaming și jocuri.
- **OpenVPN UDP** - Optimizat pentru viteze mari. Cu toate acestea, acest protocol nu este la fel de fiabil în ceea ce privește pierderea de date precum alte protocoale din listă.
- **OpenVPN TCP** - Proiectat pentru fiabilitate. Se asigură că datele dvs. sunt livrate în întregime, dar nu sunt la fel de rapide ca OpenVPN UDP.
- **Apărător de sârmă** - Protocol mai nou, oferind securitate puternică și un nivel ridicat de performanță.

Salt dublu

Cu această caracteristică puteți gestiona serverele prin care să trimiteți și să criptați dublu traficul dvs. de internet. Datele tale vor trece prin două servere VPN în loc de unul, ceea ce face mai dificilă urmărirea activității tale pe internet.

> **Notă**
> Puteți adăuga doar un total de 5 locații cu salt dublu. Cu toate acestea, puteți șterge salturile duble personalizate din lista dvs. și puteți crea altele oricând.

Important

Utilizarea serverelor situate pe continente diferite în același salt dublu poate încetini viteza conexiunii.

6. CUM SĂ DEZINSTALEZI BITDEFENDER VPN

Procedura de dezinstalare a aplicației Bitdefender VPN este similară celei utilizate pentru ștergerea altor programe din computerul tău:

- **Dezinstalarea Bitdefender VPN de pe dispozitivele Windows**
  - În **Windows 7**:
    1. Fă clic pe **Start**, accesează **Panoul de control** și fă dublu clic pe **Programe și caracteristici**.
    2. Găsește **Bitdefender VPN** și selectează **Dezinstalare**.
       Așteaptă până când procesul de dezinstalare este finalizat.
  - În **Windows 8** și **Windows 8.1**:
    1. Din ecranul de Start al Windows, localizați **Panoul de control** (de exemplu, puteți începe să tastați „Panou de control” direct în ecranul de Start) și faceți click pe pictograma acestuia.
    2. Fă clic pe **Dezinstalează un program** sau pe **Programe și caracteristici**.
    3. Găsi **Bitdefender VPN** și selectați **Dezinstalează**.
       Așteptați finalizarea procesului de dezinstalare.
  - În **Windows 10** și **Windows 11**:
    1. Fă clic pe **Start**, apoi pe **Setări**.
    2. Fă clic pe pictograma **Sistem** din secțiunea Setărilor, apoi selectează **Aplicații instalate**.
    3. Găsi **Bitdefender VPN** și selectați **Dezinstalează**.
    4. Faceți clic din nou pe **Dezinstalare** pentru a confirma selecția.
       Așteptați finalizarea procesului de dezinstalare.
- **Dezinstalarea de pe dispozitivele macOS**
  1. Fă clic pe **Go** (Mergi la) din bara de meniu și selectează **Aplicații**.
  2. Fă dublu clic pe directorul **Bitdefender**.
  3. Execută **BitdefenderUninstaller**.

4. În noua fereastră, bifează caseta de lângă **Bitdefender VPN**, apoi selectează **Dezinstalează**.
5. Introdu un cont valid de administrator și o parolă, apoi selectează**OK**.
6. În final, vei fi anunțat că Bitdefender VPN a fost dezinstalat cu succes. Selectează **Închide**.

- **Dezinstalarea de pe dispozitivele Android**
  1. Deschide aplicația **Play Store**.
  2. Caută **Bitdefender VPN**.
  3. De pe pagina magazinului de aplicații Bitdefender VPN selectează **Dezinstalare**.
  4. Confirmă atingând **OK**.

- **Dezinstalarea de pe dispozitivele iOS**
  1. Ține degetul pe aplicația Bitdefender VPN.
  2. Selectează opțiunea **Ștergere aplicație**.
  3. Atinge **Ștergere**.

7. ÎNTREBĂRI FRECVENTE

Când ar trebui să utilizez Bitdefender VPN?

Trebuie să procedezi cu atenție atunci când accesezi, descarci sau încarci conținut pe internet. Pentru a te asigura că rămâi în siguranță în timp ce navighezi pe internet, îți recomandăm să folosești VPN în următoarele situații:

- când dorești să te conectezi la rețele wireless publice
- dorești să accesezi conținut care în mod normal este restricționat în anumite zone, indiferent dacă ești acasă sau în străinătate
- dorești să-ți păstrezi confidențialitatea datelor personale (nume de utilizator, parole, datele cardului de credit etc.)
- când dorești să-ți ascunzi adresa IP

Pot alege un oraș cu Bitdefender VPN?

Da. Momentan, Bitdefender VPN pentru Windows, macOS, Android și iOS poate fi folosit pentru a selecta un anumit oraș. Iată lista orașelor disponibile în prezent:

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

Aplicația Bitdefender VPN poate fi instalată ca o aplicație autonomă?

Aplicația VPN este instalată automat împreună cu soluția de securitate Bitdefender. De asemenea, poate fi instalată ca aplicație autonomă din pagina produsului, din Google Play Store și App Store.

Va comunica Bitdefender adresa mea IP și datele mele personale unor terți?

Nu, cu Bitdefender VPN confidențialitatea ta este 100% sigură. Nimeni (agenții de publicitate, ISP, companii de asigurări etc.) nu va avea acces la jurnalele tale online.

Ce algoritm de criptare folosește?

Bitdefender VPN folosește protocolul Hydra pe toate platformele, criptare AES pe 256 de biți sau cel mai înalt cifrat disponibil acceptat atât de client, cât și de server, cu Perfect Forward Secrecy. Aceasta înseamnă că cheile de criptare sunt generate pentru fiecare nouă sesiune VPN și șterse din memorie când sesiunea se termină.

Pot avea acces la conținut restricționat geografic?

Cu VPN Premium ai acces la o rețea extinsă de locații virtuale în întreaga lume.

Va avea un impact negativ asupra autonomiei bateriei dispozitivului meu?

Bitdefender VPN este conceput să îți protejeze datele personale, să îți ascundă adresa IP în timp ce ești conectat la rețele wireless nesecurizate și la conținutul cu acces restricționat din anumite țări. Pentru a evita consumarea inutilă a bateriei, îți recomandăm să folosești funcția VPN numai atunci când ai nevoie de ea și să te deconectezi atunci când ești offline.

De ce aplicația VPN îmi încetinește conexiunea la internet?

Bitdefender VPN este concepută pentru a oferi o experiență ușoară în timp ce navighezi pe web. În funcție de distanța dintre locația ta reală și locația serverului la care alegi să te conectezi, este de așteptat să existe o anumită scădere a vitezei, însă este aproape întotdeauna suficient de mică încât să treacă neobservată în timpul activității normale online. Mai mult, ne bazăm pe una dintre cele mai rapide infrastructuri VPN din lume. Dacă nu este obligatoriu să te conectezi din locația ta la un server găzduit la mare distanță (de exemplu, din SUA până în Franța), îți recomandăm să îi permiți VPN-ului să se conecteze automat la cel mai apropiat server sau să găsească un server mai aproape de locația ta actuală.

8. OBȚINE AJUTOR

8.1. Solicitarea ajutorului

Bitdefender le oferă clienților săi un serviciu rapid și precis de asistență, la un nivel inegalabil. Dacă întâmpini probleme sau dacă ai întrebări legate de produsul tău Bitdefender, poți utiliza o serie de resurse online pentru a identifica o soluție sau un răspuns. De asemenea, poți contacta echipa Serviciului de asistență pentru clienți. Reprezentanții noștri îți vor răspunde la întrebări în timp util și îți vor oferi sprijinul de care ai nevoie.

8.2. Resurse online

Sunt disponibile mai multe resurse online pentru a vă ajuta la soluționarea problemelor și întrebărilor referitoare la produsul Bitdefender.

- Centrul de asistență Bitdefender:
  https://www.bitdefender.ro/consumer/support/
- Comunitatea de experți Bitdefender:
  https://community.bitdefender.com/ro
- Bitdefender Cyberpedia:
  https://www.bitdefender.com/cyberpedia/

De asemenea, puteți folosi motorul de căutare preferat pentru a afla informații suplimentare referitoare la securitatea informatică, produsele și compania Bitdefender.

8.2.1. Centrul de asistență Bitdefender

Centrul de Asistență Bitdefender este un depozit online ce conține informații despre produsele Bitdefender. Acesta stochează, într-un format ușor accesibil, rapoarte privind rezultatele unor activități continue de asistență tehnică și remediere ale echipelor de asistență și dezvoltare Bitdefender, alături de articole mai generale referitoare la prevenirea amenințărilor, gestionarea soluțiilor Bitdefender cu explicații detaliate și multe alte articole.

Bitdefender Support Center este pusă la dispoziția publicului. Această multitudine de informații reprezintă încă o cale de a oferi clienților BitDefender asistența tehnică de care au nevoie. Toate cererile valide de

informații sau rapoarte despre bug-uri venind de la clienții BitDefender ajung în cele din urmă în Bitdefender Support Center, ca rapoarte asupra eliminării bug-urilor, fișe de lucru sau articole informative pentru a suplimenta fișierele de suport ale produsului.

Centrul de asistență Bitdefender este disponibil oricând la următoarea adresă: https://www.bitdefender.ro/consumer/support/.

8.2.2. Comunitatea de experți Bitdefender

Comunitatea de experți este un mediu în care utilizatorii, pasionații și fanii Bitdefender pot interacționa, face schimb de idei, se pot ajuta reciproc și își pot împărtăși cunoștințele și soluțiile. De asemenea, acesta este un loc în care se nasc idei și de unde echipele noastre de dezvoltare pot obține un feedback valoros. Membrii comunității sunt utilizatori Bitdefender cu experiență, dornici să-și ajute colegii, în timpul liber. Cu contribuția lor impresionantă și prin eforturi voluntare sincere, am creat o bază de cunoștințe unde utilizatorii pot găsi răspunsuri și îndrumări, prin interacțiune.

Aici veți găsi conversații relevante cu persoane care utilizează Bitdefender pe dispozitivele lor. Comunitatea oferă o legătură reală cu membrii noștri și îți permite să te faci auzit. Este un loc unde ești încurajat să participi, având siguranța că opinia și aportul tău sunt respectate și prețuite. Pentru că activitatea noastră este apreciată, depunem eforturi pentru a asigura o asistență rapidă și precisă, la un nivel incomparabil, și ne dorim să-i aducem pe utilizatorii noștri mai aproape de noi. Cu acest scop în minte, am creat această comunitate.

Accesează pagina Comunității noastre de experți aici:

https://community.bitdefender.com/ro

8.2.3. Bitdefender Cyberpedia

Bitdefender Cyberpedia conține toate informațiile de care ai nevoie despre cele mai noi amenințări cibernetice. Acesta este locul unde experții Bitdefender își împărtășesc sfaturi și recomandări despre cum să se protejeze împotriva hackerilor, breșelor de securitate a datelor, furtului de identitate și încercărilor de asumare a identității.

Accesează pagina Bitdefender Cyberpedia aici:

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

8.3. Informații de contact

Comunicarea eficientă este cheia unei afaceri de succes. Din 2001, BITDEFENDER și-a stabilit o reputație incontestabilă prin străduința constantă pentru o mai bună comunicare, astfel încât să depășească așteptările clienților și partenerilor noștri. Dacă aveți întrebări, nu ezitați să ne contactați direct prin intermediul nostru Centrul de asistență Bitdefender (pagina 31).

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

8.3.1. Distribuitori locali

Distribuitorii locali Bitdefender sunt pregătiți să răspundă oricăror întrebări legate de aria lor de operare, atât în ce privește problemele comerciale cât și pe cele generale.

Pentru a găsi un distribuitor Bitdefender în țara dumneavoastră:

1. Mergi la https://www.bitdefender.com/partners/partner-locator.html.
2. Selectează țara și orașul folosind opțiunile corespunzătoare.

GLOSAR

Cod de activare

Este o cheie unică ce poate fi cumpărată de la distribuitorii retail și folosită pentru a activa un anumit produs sau serviciu. Codul de activare permite activarea unui abonament valabil pentru o anumită perioadă de timp și un anumit număr de dispozitive și poate fi, de asemenea, folosit pentru prelungirea unui abonament, cu condiția ca acesta să fie generat pentru același produs sau serviciu.

ActiveX

ActiveX este un model de scriere a programelor, astfel încât alte programe și sistemul de operare să le poată apela. Tehnologia ActiveX este utilizată cu Microsoft Internet Explorer pentru a crea pagini web interactive care arată și se comportă ca niște programe de calculator, mai degrabă decât ca pagini statice. Cu ActiveX, utilizatorii pot pune sau răspunde la întrebări, pot folosi butoane și pot interacționa în alte moduri cu pagina web. Controalele ActiveX sunt adesea scrise folosind Visual Basic. Active X se remarcă prin lipsa completă a controalelor de securitate; experții în securitatea computerelor descurajează utilizarea acestuia pe internet.

Amenințare persistentă avansată

Amenințarea persistentă avansată (APT) exploatează vulnerabilitățile sistemelor pentru a fura informații importante pentru a le livra la sursă. Grupurile mari, cum ar fi organizațiile, companiile sau guvernele, sunt vizate de această amenințare. Obiectivul unei amenințări persistente avansate este de a rămâne nedetectat pentru o lungă perioadă de timp, putând monitoriza și aduna informații importante fără a deteriora mașinile vizate. Metoda folosită pentru a injecta amenințarea în rețea este printr-un fișier PDF sau un document Office care arată inofensiv, astfel încât fiecare utilizator să poată rula fișierele.

Adware

Adware-ul este adesea combinat cu o aplicație gazdă care este furnizată gratuit, atâta timp cât utilizatorul este de acord să accepte adware-ul. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord cu un acord de licență care precizează scopul aplicației, nu se comite nicio infracțiune. Cu toate acestea, reclamele pop-up pot deveni o supărare și, în unele cazuri, pot degrada performanța

sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le colectează pot cauza probleme de confidențialitate pentru utilizatorii care nu cunoșteau pe deplin termenii din acordul de licență.

Arhiva

Un disc, o casetă sau un director care conține fișiere de rezervă.

Un fișier care conține unul sau mai multe fișiere într-un format comprimat.

Ușa din spate

O gaură în securitatea unui sistem lăsată în mod deliberat de proiectanți sau întreținători. Motivația pentru astfel de găuri nu este întotdeauna sinistră; unele sisteme de operare, de exemplu, ies din cutie cu conturi privilegiate destinate utilizării de către tehnicienii de service pe teren sau programatorii de întreținere ai furnizorului.

Sectorul de boot

Un sector la începutul fiecărui disc care identifică arhitectura discului (dimensiunea sectorului, dimensiunea clusterului și așa mai departe). Pentru discurile de pornire, sectorul de boot conține și un program care încarcă sistemul de operare.

Virus de pornire

O amenințare care infectează sectorul de pornire al unui disc fix sau al unei dischete. O încercare de pornire de pe o dischetă infectată cu un virus din sectorul de boot va face ca amenințarea să devină activă în memorie. De fiecare dată când porniți sistemul din acel moment, veți avea amenințarea activă în memorie.

botnet

Termenul „botnet” este compus din cuvintele „robot” și „rețea”. Rețelele bot sunt dispozitive conectate la internet infectate cu amenințări și pot fi folosite pentru a trimite e-mailuri spam, a fura date, a controla de la distanță dispozitive vulnerabile sau a răspândi programe spyware, ransomware și alte tipuri de amenințări. Obiectivul lor este de a infecta cât mai multe dispozitive conectate, precum PC-uri, servere, dispozitive mobile sau IoT aparținând marilor companii sau industrii.

Browser

Prescurtare pentru browser web, o aplicație software folosită pentru a localiza și afișa pagini web. Printre browserele populare se numără Microsoft Internet Explorer, Mozilla Firefox și Google Chrome. Acestea

sunt browsere grafice, ceea ce înseamnă că pot afișa atât grafică, cât și text. În plus, majoritatea browserelor moderne pot prezenta informații multimedia, inclusiv sunet și video, deși necesită plug-in-uri pentru unele formate.

Atac de forță brută

Atacul de ghicire a parolei folosit pentru a pătrunde într-un sistem computerizat prin introducerea de combinații posibile de parole, de cele mai multe ori începând cu parola cel mai ușor de ghicit.

Linie de comanda

Într-o interfață de linie de comandă, utilizatorul tastează comenzi în spațiul oferit direct pe ecran folosind limbajul de comandă.

Cookie-uri

În industria internetului, cookie-urile sunt descrise ca fișiere mici care conțin informații despre computere individuale care pot fi analizate și utilizate de agenții de publicitate pentru a urmări interesele și gusturile dvs. online. În acest domeniu, tehnologia cookie-urilor este încă în curs de dezvoltare și intenția este de a direcționa anunțurile direct către ceea ce ați spus că sunt interesele dvs. Este o sabie cu două tăișuri pentru mulți oameni, deoarece, pe de o parte, este eficientă și pertinentă, deoarece vedeți doar reclame despre ceea ce vă interesează. Pe de altă parte, implică de fapt „urmărirea” și „urmărirea” unde mergeți și pe ce dai click. De înțeles, există o dezbatere asupra confidențialității și mulți oameni se simt jigniți de ideea că sunt priviți ca un „număr SKU” (știți, codul de bare de pe spatele pachetelor care este scanat la linia de check-out de la băcănie) . Deși acest punct de vedere poate fi extrem, în unele cazuri este precis.

Hărțuirea cibernetică

Când colegii sau străinii comit acte abuzive împotriva copiilor intenționat pentru a-i răni fizic. Pentru a dăuna emoțional, agresorii trimit mesaje răutăcioase sau fotografii nemăgulitoare, făcând astfel victimele lor să se izoleze de ceilalți sau să se simtă frustrate.

Dicționar Attack

Atacurile de ghicire a parolelor erau folosite pentru a pătrunde într-un sistem informatic prin introducerea unei combinații de cuvinte comune pentru a genera parole potențiale. Aceeași metodă este folosită pentru a ghici cheile de decriptare ale mesajelor sau documentelor criptate.

Atacurile de dicționar reușesc, deoarece mulți oameni înclină să aleagă parole scurte și simple, care sunt ușor de ghicit.

Unitate disc

Este o mașină care citește și scrie date pe un disc. Un hard disk citește și scrie hard disk-uri. O unitate de dischetă accesează dischetele. Unitățile de disc pot fi fie interne (găzduite într-un computer), fie externe (găzduite într-o cutie separată care se conectează la computer).

Descarca

Pentru a copia date (de obicei un fișier întreg) de la o sursă principală pe un dispozitiv periferic. Termenul este adesea folosit pentru a descrie procesul de copiere a unui fișier dintr-un serviciu online pe propriul computer. Descărcarea se poate referi și la copierea unui fișier de pe un server de fișiere din rețea pe un computer din rețea.

E-mail

Poștă electronică. Un serviciu care trimite mesaje pe computere prin rețele locale sau globale.

Evenimente

O acțiune sau o apariție detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi clic pe un buton al mouse-ului sau apăsarea unei taste, sau apariții ale sistemului, cum ar fi epuizarea memoriei.

Exploatările

O modalitate de a profita de diferite erori sau vulnerabilități care sunt prezente într-un computer (software sau hardware). Astfel, hackerii pot obține controlul asupra computerelor sau rețelelor.

Fals pozitiv

Apare atunci când un scaner identifică un fișier ca fiind infectat, când de fapt nu este.

Extensie de nume de fișier

Porțiunea dintr-un nume de fișier, care urmează punctului final, care indică tipul de date stocate în fișier. Multe sisteme de operare folosesc extensii de nume de fișiere, de exemplu Unix, VMS și MS-DOS. Acestea sunt de obicei de la una la trei litere (unele sisteme de operare vechi triste nu acceptă mai mult de trei). Exemplele includ „c” pentru codul sursă C, „ps” pentru PostScript, „txt” pentru text arbitrar.

Euristică

O metodă bazată pe reguli de identificare a noilor amenințări. Această metodă de scanare nu se bazează pe baza de date cu informații despre amenințări specifice. Avantajul scanării euristice este că nu este păcălit de o nouă variantă a unei amenințări existente. Cu toate acestea, poate raporta ocazional cod suspect în programele normale, generând așa-numitul „fals pozitiv”.

Borcan cu miere

Un sistem informatic momeală creat pentru a atrage hackerii să studieze modul în care acționează şi să identifice metodele eretice pe care le folosesc pentru a colecta informații despre sistem. Companiile și corporațiile sunt mai interesate de implementarea și utilizarea honeypot-urilor pentru a-și îmbunătăți starea generală de securitate.

IP

Internet Protocol - Un protocol rutabil din suita de protocoale TCP/IP care este responsabil pentru adresarea IP, rutarea și fragmentarea și reasamblarea pachetelor IP.

applet Java

Un program Java care este proiectat să ruleze numai pe o pagină web. Pentru a utiliza un applet pe o pagină web, trebuie să specificați numele applet-ului și dimensiunea (lungime și lățime, în pixeli) pe care le poate utiliza applet-ul. Când pagina web este accesată, browserul descarcă appletul de pe un server și îl rulează pe computerul utilizatorului (clientul). Appleturile diferă de aplicații prin faptul că sunt guvernate de un protocol de securitate strict.

De exemplu, chiar dacă aplicațiile rulează pe client, acestea nu pot citi sau scrie date pe computerul clientului. În plus, applet-urile sunt restricționate în continuare, astfel încât să poată citi și scrie numai date de pe același domeniu din care sunt servite.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați. Keylogger-urile nu sunt rău intenționate în natură. Ele pot fi folosite în scopuri legitime, cum ar fi monitorizarea angajaților sau a activității copiilor. Cu toate acestea, acestea sunt din ce în ce mai folosite de infractorii cibernetici în scopuri rău intenționate (de exemplu, pentru a colecta date private, cum ar fi datele de conectare și numerele de securitate socială).

Virus macro

Un tip de amenințare informatică care este codificată ca macrocomandă încorporată într-un document. Multe aplicații, cum ar fi Microsoft Word și Excel, acceptă limbaje macro puternice. Aceste aplicații vă permit să încorporați o macrocomandă într-un document și să executați macrocomandă de fiecare dată când documentul este deschis.

Client de mail

Un client de e-mail este o aplicație care vă permite să trimiteți și să primiți e-mail.

Memorie

Zone de stocare internă în computer. Termenul de memorie identifică stocarea de date care vine sub formă de cipuri, iar cuvântul stocare este folosit pentru memoria care există pe benzi sau discuri. Fiecare computer vine cu o anumită cantitate de memorie fizică, denumită de obicei memorie principală sau RAM.

Non-euristic

Această metodă de scanare se bazează pe baza de date cu informații despre amenințări specifice. Avantajul scanării non-euristice este că nu este păcălit de ceea ce ar putea părea a fi o amenințare și nu generează alarme false.

Prădători online

Persoane care caută să atragă minori sau adolescenți în conversații cu scopul de a-i implica în activități sexuale ilegale. Rețelele de socializare sunt locul ideal în care copiii vulnerabili pot fi vânați cu ușurință și seduși să comită activități sexuale, online sau față în față.

Programe pline

Un fișier într-un format de compresie. Multe sisteme de operare și aplicații conțin comenzi care vă permit să împachetați un fișier astfel încât să ocupe mai puțină memorie. De exemplu, să presupunem că aveți un fișier text care conține zece caractere spațiale consecutive. În mod normal, acest lucru ar necesita zece octeți de stocare.

Cu toate acestea, un program care împachetează fișiere ar înlocui caracterele de spațiu cu un caracter special din seria spațială, urmat de numărul de spații înlocuite. În acest caz, cele zece spații ar necesita doar doi octeți. Aceasta este doar o tehnică de ambalare - sunt multe altele.

Cale

Indicațiile exacte către un fișier de pe un computer. Aceste direcții sunt de obicei descrise prin intermediul sistemului ierarhic de evidență de sus în jos.

Ruta dintre oricare două puncte, cum ar fi canalul de comunicații între două computere.

Phishing

Acțiunea de a trimite un e-mail unui utilizator care pretinde în mod fals că este o întreprindere legitimă stabilită în încercarea de a înșela utilizatorul pentru a renunța la informații private care vor fi folosite pentru furtul de identitate. E-mailul îl direcționează pe utilizator să viziteze un site web unde i se cere să actualizeze informații personale, cum ar fi parolele și numerele de card de credit, de securitate socială și de cont bancar, pe care organizația legitimă le are deja. Totuși, site-ul web este fals și creat doar pentru a fura informațiile utilizatorului.

Foton

Photon este o tehnologie Bitdefender inovatoare, neitruzivă, proiectată pentru minimizarea impactului soluției tale de securitate asupra performanțelor. Prin monitorizarea în fundal a activității PC-ului tău, creează modele de utilizare care vor ajuta la optimizarea pornirii și a proceselor de scanare.

Virus polimorf

O amenințare care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, astfel de amenințări sunt greu de identificat.

Port

Reprezintă o interfață a unui calculator la care se poate conecta un dispozitiv. Calculatoarele personale dispun de diferite tipuri de porturi. Există porturi interne pentru conectarea hard discurilor, monitoarelor și tastaturilor. Există porturi externe pentru conectarea modemului, imprimantei, mouse-ului și a altor dispozitive periferice.

În rețelele TCP/IP și UDP, acestea reprezintă un endpoint către o conexiune logică. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Ransomware

Ransomware este un program periculos care încearcă să obțină bani de la utilizatori prin blocarea sistemelor vulnerabile. CryptoLocker, CryptoWall și TeslaWall sunt doar câteva variante care vânează sistemele personale ale utilizatorilor.

Infecția se poate extinde prin accesarea mesajelor spam, descărcarea atașamentelor e-mail sau instalarea de aplicații, fără ca utilizator să afle ce se întâmplă pe sistemul său. Utilizatorii și companiile sunt vizate zilnic de către hackerii ransomware.

Fișier raport

Reprezintă un fișier care listează acțiunile care au avut loc. BitDefender menține un fișier log (jurnal) în care sunt listate obiectele care au fost scanate, numele fișierelor, numărul de arhive și fișiere scanate, câte fișiere infectate și suspecte au fost găsite.

Rootkit

Un rootkit este un set de instrumente soft ce oferă acces la nivel de administrator în interiorul unui sistem. Termenul a fost utilizat pentru prima oară pentru sistemele de operare UNIX și se referea la instrumente recompilate ce furnizau intrușilor drepturi administrative, permițându-le să își ascundă prezența astfel încât să nu poată fi văzuți de către administratorii de sistem.

Rolul principal al rootkiturilor este de a ascunde procese, fișiere, conectări și jurnale. Acestea pot, de asemenea, să intercepteze date de la terminale, conexiuni la rețea sau dispozitive periferice, dacă sunt dotate cu softul adecvat.

Rootkiturile nu sunt malițioase prin natură. De exemplu, sistemele și chiar unele aplicații ascunde fișiere critice utilizând rootkituri. Totuși, ele sunt folosite în general pentru a ascunde amenințări sau prezența intrușilor în sistem. În combinație cu amenințările, rootkiturile constituie o mare amenințare pentru securitatea și integritatea sistemului. Acestea pot monitoriza traficul, crea porți de acces în sistem ("backdoors"), altera fișiere și jurnale și evita detecția.

Script

Un alt termen pentru fișiere macro sau de tip "bat", un script reprezintă o listă de comenzi care pot fi executate fără intervenția utilizatorului.

Spam

Termen ce acoperă întreaga gamă a mesajelor electronice nesolicitate (junk). În general, acestea sunt cunoscute sub numele de mesaje electronice nesolicitate.

Spyware

Reprezintă orice software care strânge informații despre utilizator prin intermediul conexiunii la internet fără știrea acestuia, de obicei în scopuri publicitare. Aplicațiile spyware sunt de obicei primite ca parte ascunsă a unui program de tip freeware sau shareware, ce poate fi descărcat de pe Internet; totuși, trebuie știut că majoritatea aplicațiilor de tip shareware și freeware nu conțin aplicații spyware. Odată instalată, aplicația spyware monitorizează activitatea utilizatorului pe internet și transmite pe ascuns informații altei persoane. Aplicațiile spyware pot aduna, de asemenea, informații despre adresele e-mail și chiar parole și numere de carduri de credit.

Asemănarea dintre spyware și o amenințare de tip cal troian este legată de faptul că utilizatorul instalează aplicația fără voia sa atunci când instalează altceva. Un mod obișnuit de a deveni victima unei aplicații spyware este de a descărca prin rețelele peer-to-peer anumite produse de schimb de fișiere care sunt disponibile astăzi.

Pe lângă problemele legate de etică și intimitate, aplicația spyware fură de la utilizator atât prin folosirea memoriei calculatorului cât și a lungimii de bandă deoarece trimite informații înapoi la sursă prin intermediul conexiunii la internet a utilizatorului. Deoarece folosesc memorie și resurse ale sistemului, aplicațiile spyware pot conduce la blocarea sistemului sau la instabilitate generală.

Elemente de pornire

Orice fișier plasat în acest director se va deschide de fiecare dată când calculatorul este pornit. De exemplu, un sunet care se va auzi atunci când este pornit calculatorul sau chiar aplicații sunt considerate elemente de startup. În mod normal, un alias al programului este plasat în acest director, și nu direct fișierul.

Abonament

Contractul de cumpărare care acordă utilizatorului dreptul de a folosi un anumit produs sau serviciu pe un anumit număr de dispozitive și o anumită perioadă de timp. Un abonament expirat poate fi reînnoit automat folosind informațiile furnizate de utilizator la prima achiziție.

Zona de notificare

Introdusă odată cu apariția sistemului Windows 95, bara de sistem se află în bara de sarcini Windows (de obicei, în partea de jos, lângă ceas) și conține pictograme miniaturale pentru accesul rapid la aplicații de sistem cum ar fi cele de fax, imprimantă, modem, volum și altele. Faceți dublu-clic sau clic-dreapta cu mouse-ul pe o pictogramă pentru a vizualiza și accesa detaliile și comenzile.

TCP/IP

Transmission Control Protocol/Internet Protocol - Un set de protocoale de rețea folosite în mod larg în domeniul internet și care asigură comunicarea între rețelele de calculatoare interconectate având arhitecturi hardware și sisteme de operare diferite. TCP/IP include standarde referitoare la realizarea comunicării între calculatoare cât și convenții folosite în conectarea rețelelor și rutării traficului.

Amenințare

Reprezintă un program sau o bucată de cod care se încarcă pe calculator fără știrea dumneavoastră și rulează independent de voința dumneavoastră. Cea mai mare parte a amenințărilor se pot și înmulți. Toate amenințările informatice sunt create de om. O simplă amenințare care poate realiza copii ale sale este relativ simplu de produs. Chiar și o asemenea amenințare este periculoasă întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. O amenințare și mai periculoasă este cea care este capabilă să se răspândească în rețea și poate să treacă de sistemele de securitate.

Actualizare informații despre amenințări

Modelul binar al unei amenințări, utilizat de către soluția de securitate pentru detectarea și eliminarea amenințării.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de programele malițioase și viermi, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cele mai mascate tipuri de amenințări de tip cal troian este un program care pretinde că elimină amenințările de pe calculatorul tău, însă, în loc de aceasta, introduce amenințări pe calculatorul tău.

Termenul provine de la o poveste din opera „Iliada” a lui Homer, în care grecii le oferă dușmanilor lor, troienii, în semn de pace un cal gigantic de lemn. Dar după ce troienii aduc acest cal în interiorul orașului lor,

din interiorul calului ies o mulțime de soldați greci, care deschid porțile cetății, permițându-le celorlalți soldați greci să pătrundă în oraș și să captureze Troia.

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. Rutinele de instalare a actualizărilor verifică dacă pe calculatorul tău există instalată o altă versiune mai veche; dacă nu, nu vei putea instala actualizarea.

Bitdefender dispune de o funcție proprie de actualizare care îți permite să verifici manual actualizările sau să permiți actualizarea automată a produsului.

Virtual Private Network (VPN)

Este o tehnologie care permite o conexiune directă temporară și criptată la o anumită rețea prin intermediul unei rețele mai puțin sigure. Astfel, trimiterea și primirea de date este sigură și criptată, dificil de interceptat de către curioși. O dovadă de securitate este autentificarea, care se poate efectua numai folosind un nume de utilizator și o parolă.

Vierme

Reprezintă un program care se auto-propagă în interiorul unei rețele, reproducându-se pe măsură ce se răspândește. Nu se poate atașa la alte programe.