GHIDUL UTILIZATORULUI

Bitdefender CONSUMER SOLUTIONS

Parental Control

Bitdefender Parental Control

Manual de utilizare

Publication date 04/29/2024

Termeni legali

Bitdefender

Cuprins

DESPRE ACEST GHID

Scopul și publicul țintă

Acest ghid se adresează tuturor utilizatorilor Bitdefender care au ales Bitdefender Parental Control ca soluție pentru asigurarea securității, monitorizarea și protecția continuă a dispozitivelor și a prezenței online a copiilor lor.

Vei afla cum să instalezi, să configurezi și să profiți la maximum de Bitdefender Parental Control, pentru a beneficia de funcții îmbunătățite și un control mai bun asupra activității online a copilului tău.

Vă dorim o prelegere plăcută și utilă.

Cum să folosiți acest ghid

Acest ghid este organizat în mai multe teme majore:

Introducere (pagina 4)

Primii pași în configurarea Bitdefender Parental Control.

Caracteristici și funcționalități (pagina 10)

Află cum să utilizezi Bitdefender Parental Control și toate funcțiile sale.

Obține ajutor (pagina 22)

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. INTRODUCERE

Vom începe cu un ghid detaliat, pas cu pas, despre cum să configurezi abonamentul Bitdefender Parental Control în contul tău Bitdefender Central. Acesta este primul pas dintr-un proces simplu care trebuie parcurs pentru a putea gestiona și monitoriza eficient activitatea online a copiilor tăi.

1.1. Configurarea soluției Bitdefender Parental Control

După activarea abonamentului, parcurge următorii pași pentru a începe să configurezi Bitdefender Parental Control în contul tău:

1. Accesează-ți contul Bitdefender Central și apoi selectează fila **Control parental** din partea stângă a ecranului.
2. Fă clic pe **Primii pași**.
3. Setare cod PIN aplicație.

   > **Notă**
   > Când folosești codul PIN, copiii nu vor putea să dezactiveze singuri funcțiile de control parental prin deconectarea de la aplicația asociată profilului lor.
   >
   > Reține acest cod.

4. Fă clic pe **Înainte**.
5. Continuă cu crearea unui profil de copil. Introdu numele copilului și selectează o fotografie de profil. Apoi, fă clic pe **Înainte**.
6. Selectează vârsta copilului tău. Când ai terminat, fă clic pe **Înainte**.
7. Precizează dacă aplicația Parental Control urmează să fie instalată pe dispozitivul pe care îl utilizezi sau pe un alt dispozitiv.

Notă

Dacă selectezi **Alte dispozitive**, ți se vor prezenta trei opțiuni de instalare. Selectează metoda preferată:

- Prin scanarea codului QR.
- Prin copierea linkului furnizat și accesarea acestuia în browserul dispozitivului copilului.
- Prin trimiterea linkului de instalare prin e-mail.

8. Așteaptă ca programul de instalare să se descarce complet și apoi execută-l pe dispozitivul în cauză.

Apoi, va începe procesul de instalare. Pașii care trebuie urmați de aici încolo variază în funcție de tipul de dispozitiv și de sistemul de operare pe care se efectuează instalarea.

1.2. Instalarea Bitdefender Parental Control pe dispozitivele copilului tău

1.2.1. Pe dispozitivele Windows:

După ce execuți programul de instalare descărcat:

1. Fă clic pe **Yes** (Da) dacă apare o fereastră de dialog pentru contul de utilizator prin care ți se solicită să permiți ca fișierul de instalare să facă modificări pe dispozitiv.
2. Conectează-te introducând datele de autentificare ale contului Bitdefender Central, dacă ți se solicită acest lucru.

1.2.2. Pe dispozitivele macOS:

După ce programul de instalare a fost descărcat, fă dublu clic pe fișierul Bitdefender pentru a începe procesul de instalare:

1. Urmează pașii necesari pentru a instala Bitdefender Parental Control pentru macOS, conform îndrumărilor furnizate. Fă clic pe **Permite** dacă ți se solicită acest lucru.
2. Fă clic pe cele două butoane consecutive **Continuă**.
3. Pentru a continua instalarea, este necesar să-ți exprimi acordul cu privire la condițiile contractului de abonament pentru acest software.

4. Fă clic pe **Continuă**. Apoi, fă clic pe **Instalare**.
5. Atunci când ți se solicită acest lucru, introdu un nume de administrator și o parolă, apoi apasă pe **Instalare software**.

Așteaptă până când primești o notificare pop-up care te anunță că *o extensie de sistem a fost blocată*. Este un eveniment normal care apare în timpul acestei proceduri. Pentru a continua, trebuie să permiți extensia de sistem a aplicației Parental Control conform instrucțiunilor de mai jos:

1. Fă clic pe butonul **Open System Settings** (Deschide configurări sistem).

   Notă
   În versiunile anterioare ale macOS, acest buton este denumit **Open Security Preferences** (Deschide preferințe de securitate).

2. Fă clic pe butonul **Allow** (Permite) în ferestrele care apar pe ecran, apoi introdu un nume de administrator și o parolă pentru a debloca setările.

   Notă
   Pe macOS 11 (Big Sur) și macOS 12 (Monterey), înainte de a face clic pe butonul **Allow** (Permite), va trebui să faci clic pe pictograma lacăt din colțul din stânga jos al ferestrei **Security & Privacy** (Securitate și Intimitate), apoi să introduci un nume de administrator și o parolă pentru a putea face modificări.

3. Va apărea fereastra pop-up **Filter Network Content** (Filtrare conținut rețea). Fă clic pe butonul **Allow** (Permite) din această fereastră.
4. Apoi, fă clic pe butonul **Open System Settings** (Deschide configurări sistem).
5. Fă clic pe butonul **Allow** (Permite) încă o dată.

1.2.3. Pe dispozitivele Android:

Accesează pagina Bitdefender din Google Play Store pentru a găsi aplicația Parental Control:

1. Atinge butonul **Install** (Instalare). Procesul de descărcare și instalare a aplicației va începe.

2. După ce instalarea este finalizată, va apărea butonul **Open** (Deschide). Atingeți butonul pentru a lansa aplicația Bitdefender Parental Control.

După ce deschizi aplicația, urmează pașii de pe ecran pentru a configura aplicația Bitdefender Parental Control pe dispozitivul Android al copilului tău:

1. Atinge **Continuă**.
2. Conectează-te la aplicație folosind datele de autentificare ale contului tău Bitdefender Central.
3. Selectează profilul copilului pe care dorești să îl atribui dispozitivului Android.
4. Va trebui să acorzi drepturile de acces necesare pentru ca aplicația să funcționeze corect. Pentru a face acest lucru, atinge **Înainte**, apoi:
   a. Permite accesul VPN, apoi alege **Permite mereu** pentru a filtra conținutul online pe dispozitivul copilului tău.
   b. Pentru a permite localizarea dispozitivului Android al copilului tău, atinge **Înainte**, apoi **Permite** și alege opțiunea **Permite mereu**.
   c. Atât drepturile de acces pentru VPN, cât și cele pentru locație vor afișa o bifă verde. Atinge **Finalizare configurare** și apoi **Înainte**.
   d. În acest moment, mai există încă 3 opțiuni pentru a bloca accesul la internet și la aplicații pe dispozitivul copilului. Atinge **Setare drept de acces** în panoul **Drepturi administrator dispozitiv**.
   e. Atinge butonul **Finalizare** după ce ai terminat de configurat aplicația Bitdefender Parental Control.

1.2.4. Pe dispozitivele iOS:

Accesează pagina Bitdefender din App Store pentru a găsi aplicația Bitdefender Parental Control:

1. Atinge pictograma nor cu o săgeată îndreptată în jos. Procesul de descărcare și instalare a aplicației va începe.
2. După ce instalarea este finalizată, va apărea butonul **Open** (Deschide). Atinge butonul pentru a lansa aplicația Bitdefender Parental Control.

3. Dacă pe dispozitivul iOS al copilului se găsesc profiluri de gestionare a dispozitivelor mobile (MDM), ți se va solicita să le elimini. Atinge **Înainte** și alege **Eliminare profiluri**.
4. În aplicația **Settings** (Setări) din iOS, accesează **General**, apoi derulează în jos și atinge secțiunea **VPN & Device Management** (Gestionare VPN și dispozitive).
5. Atinge fiecare element din secțiunea **MOBILE DEVICE MANAGEMENT** (Gestionare dispozitive mobile) (MDM) și alege **Remove Management** (Eliminare gestionare) pentru fiecare dintre ele.
   Repetă acest proces până când nu mai există elemente în secțiunea MOBILE DEVICE MANAGEMENT (Gestionare dispozitive mobile).

Redeschide aplicația instalată pe dispozitivul copilului și urmează pașii de pe ecran pentru a configura aplicația Bitdefender Parental Control:

1. Atinge **Continuă**.
2. Conectează-te la aplicație folosind datele de autentificare ale contului tău Bitdefender Central.
3. Selectează profilul copilului pe care dorești să îl atribui dispozitivului iOS.
4. Va trebui să acorzi drepturile de acces necesare pentru ca aplicația să funcționeze corect. Atinge **Înainte**.
5. Permite accesul VPN pentru a filtra conținutul online pe dispozitivul copilului tău. Atinge **Permite** de două ori la rând pentru a adăuga configurațiile VPN.
6. Atinge **Înainte**, apoi selectează **Permite** pentru a permite localizarea dispozitivului iOS al copilului tău.
7. Apoi parcurge procesul de configurare Apple Family Control pentru a bloca accesul la internet și la aplicații pe dispozitivul copilului.

   Notă
   Poți atinge **Află cum** pentru îndrumări pas cu pas despre cum să faci acest lucru.

8. După ce ai configurat Apple Family Control pe propriul dispozitiv și pe dispozitivul copilului tău, selectează **Am configurat Apple Family Control** pentru a continua.

9. Apoi, permite funcției Screen Time Access să filtreze conținutul online pe dispozitivul iOS al copilului tău.
10 Atinge **Finalizare configurare**.

.

După ce ai urmat toți acești pași pe dispozitivul (dispozitivele) copilului tău, procesul de configurare este finalizat. Ca părinte, acum poți monitoriza activitățile online ale copilului tău și poți vizualiza statistici privind utilizarea în contul tău Bitdefender Central, în panoul Control parental, despre care vom vorbi în detaliu în capitolele următoare.

2. CARACTERISTICI ȘI FUNCȚIONALITĂȚI

2.1. Profiluri

Un profil de copil este un set personalizat de reguli care permit aplicației Bitdefender Parental Control să gestioneze și să monitorizeze activitatea online a unui copil. Acesta include setări adaptate vârstei copilului, cum ar fi filtre de conținut și limite de timp. Din contul Bitdefender Central, părinții pot crea, pot edita și pot șterge aceste profiluri și pot atribui și elimina dispozitive, asigurând o experiență online sigură și adecvată pentru copiii lor.

Pentru a crea un profil de copil:

1. Accesează Bitdefender Central și conectează-te la contul tău.
2. În meniul din partea stângă, fă clic pe fila **Control parental**.
3. Fă clic pe **Profil nou** pentru a crea un nou profil de copil.
4. Introdu datele copilului, precum numele, poza de profil și data nașterii.

   > **Notă**
   > În funcție de vârsta copilului, Bitdefender blochează automat anumite categorii, cum ar fi chat-urile, rețelele sociale, conținutul explicit și multe alte tipuri de conținut. Poți ajusta ulterior categoriile de conținut blocat.

5. Fă clic pe butonul **Salvare**.

Noul profil este acum creat și va apărea pe pagină.

Pentru a edita un profil de copil:

1. Fă clic pe butonul **Detalii** din profilul de copil.
2. Pentru a modifica profilul copilului tău, accesează **Editare profil**.
3. Utilizează câmpurile corespunzătoare pentru a modifica numele, ziua de naștere și/sau poza de profil a copilului.
4. Fă clic pe **Salvează modificările** după ce ai modificat datele necesare.

Pentru a șterge un profil de copil:

1. Fă clic pe butonul **Vizualizare detalii** din profilul de copil.
2. Accesează **Editare profil**.
3. Fă clic pe butonul **Ștergere profil** și confirmă ștergerea.

Pentru a atribui dispozitive unui profil de copil:

În cazul în care copilul tău are mai multe dispozitive (Windows, macOS, Android sau iOS), le poți atribui aceluiași profil de copil.

1. Apasă pe butonul **Vizualizare detalii** din profilul de copil.
2. Fă clic pe numărul de dispozitive specificate sub numele copilului.
3. Fă clic pe butonul **Atribuire dispozitive**.
4. Selectează denumirea dispozitivului și apoi fă clic pe butonul **Atribuire**.

> **Notă**
> Dacă dispozitivul nu este vizibil în listă, fă clic pe **Instalare dispozitiv nou**, apoi urmează instrucțiunile de pe ecran pentru a instala și configura aplicația Bitdefender Parental Control pe noul dispozitiv.

Pentru a elimina dispozitive atribuite unui profil de copil:

Atunci când elimini un dispozitiv atribuit unui profil de copil, înseamnă că dispozitivul nu va mai fi administrat prin aplicația Bitdefender Parental Control. Regulile și setările specificate pentru profilul de copil nu se vor mai aplica dispozitivului respectiv. Deși aplicația de control parental rămâne instalată pe dispozitiv, aceasta încetează să mai funcționeze.

1. Apasă pe butonul **Vizualizare detalii** din profilul de copil.
2. Fă clic pe numărul de dispozitive specificate sub numele copilului.
3. Identifică dispozitivul copilului și fă clic pe opțiunea **Dezactivare atribuire dispozitiv**.
4. Apasă pe **Da, dezactivare atribuire dispozitiv** pentru a confirma acțiunea.

2.2. Statistici

Aplicația Bitdefender Parental Control oferă informații despre modul în care copiii utilizează internetul și dispozitivele lor. În acest ghid, vom

aborda în detaliu statisticile disponibile părinților în Bitdefender Central, care le oferă posibilitatea de a lua decizii în cunoștință de cauză și de a asigura o experiență online sigură și echilibrată pentru copiii lor.

Pentru a vizualiza statisticile:

1. Accesează Bitdefender Central și conectează-te la contul tău.
2. După ce te-ai conectat, fă clic pe fila **Control parental** din meniul din partea stângă.
3. Fă clic pe profilul de copil ale cărui statistici dorești să le vizualizezi.

După ce ai selectat profilului copilului tău, vei fi direcționat către un panou de bord care afișează diverse panouri de statistici. Toate acestea fac referire la celelalte caracteristici descrise mai jos în această documentație.

2.3. Codul PIN pentru Control parental

Codul PIN pentru control parental este o funcție de securitate din cadrul panoului Control parental al platformei Bitdefender Central. Acesta îi ajută pe părinți să mențină controlul asupra accesului copiilor lor la aplicația Bitdefender Parental Control instalată pe dispozitivele lor. Mai jos se regăsește un ghid detaliat despre setarea, găsirea și gestionarea codului PIN pentru control parental.

Codul PIN pentru control parental împiedică deconectările neautorizate din aplicația Bitdefender Parental Control de pe dispozitivul copilului tău. Atunci când copilul tău încearcă să se deconecteze, i se va solicita să introducă acest cod PIN. Prin această opțiune, aplicația se asigură că numai tu, ca părinte cu acces la contul Bitdefender Central, poți controla setările aplicației.

> **Notă**
> Când configurezi pentru prima dată aplicația Bitdefender Parental Control, ți se va solicita să setezi un cod PIN de 4-8 cifre pentru control parental.

2.3.1. Ai uitat codul PIN?

În cazul în care uiți codul PIN pentru control parental, îl poți recupera cu ușurință din contul tău Bitdefender Central:

1. Accesează Bitdefender Central și conectează-te la contul tău.
2. După ce te-ai conectat, fă clic pe fila **Control parental** din meniul din partea stângă.
3. În colțul din dreapta sus al paginii, fă clic pe **Cod PIN**.
4. Fă clic pe pictograma în formă de ochi pentru a vedea codul PIN pentru control parental.

2.3.2. Schimbarea codului PIN

Dacă suspectezi că codul PIN a fost compromis sau pur și simplu dorești să îl actualizezi din motive de securitate:

1. În secțiunea Control parental din contul Bitdefender Central, fă clic pe opțiunea **Cod PIN**.
2. Selectează opțiunea **Schimbare PIN** și urmează instrucțiunile de pe ecran pentru a seta un cod PIN nou.

2.4. Filtrare pe bază de conținut

Caracteristica Filtrare conținut le permite părinților să restricționeze accesul copiilor lor la conținutul online, astfel încât aceștia pot bloca categorii de site-uri web sau pot crea excepții pe baza anumitor URL-uri sau subiecte abordate.

> **Notă**
> Funcția Filtrare conținut a aplicației Bitdefender Parental Control nu împiedică un copil să folosească aplicații sau site-uri web offline, deoarece aceasta gestionează doar traficul online al dispozitivelor pe care le utilizează.

Pentru a accesa Filtrare conținut:

1. Conectează-te la contul tău Bitdefender Central.
2. În meniul din partea stângă, fă clic pe fila **Control parental**.
3. Accesează profilul copilului tău și fă clic pe meniul **Mai multe** din dreapta sus. Apoi, selectează **Filtrare conținut**.

2.4.1. Căutare sigură și restricții de utilizare a YouTube

În secțiunea **Confidențialitate și siguranță** din partea dreaptă a ecranului, poți activa butoanele de comutare Căutare sigură și YouTube restricționat.

- **Căutare sigură:** atunci când utilizezi motoarele de căutare, funcția Căutare sigură împiedică afișarea conținutului considerat nesigur de Google în rezultatele căutării.
- **YouTube restricționat:** îi afișează copilului videoclipuri de pe YouTube adecvate vârstei lui.

> **Notă**
> Caracteristicile **Căutare sigură** și **YouTube restricționat** redirecționează toate solicitările DNS de la **google.com** către **safe.google.com**. Filtrarea efectivă a conținutului este asigurată de Google. Soluția Bitdefender Parental Control nu filtrează conținutul furnizat de Căutare sigură sau Google. În mod similar, este posibil ca YouTube să nu controleze în mod eficient etichetele videoclipurilor, ceea ce ar putea expune copiii la conținut necorespunzător.

2.4.2. Blocarea și permiterea accesului la categorii de site-uri web

> **Notă**
> În secțiunea **Categorii**, tipurile de site-uri web pe care copilul tău le poate accesa online sunt permise sau blocate în mod implicit, în funcție de vârsta stabilită la crearea profilului copilului.

Poți bloca sau permite oricând dorești accesul la diferite tipuri de site-uri web:

1. Selectați o categorie.
2. Pentru a bloca accesul la această categorie, selectează **Blocat** din meniul derulant. Pentru a permite accesul, selectează **Permis**.

> **Important**
> Dacă blochezi categoria **Partajare fișiere** pentru profilul copilului tău, actualizarea macOS nu va funcționa. Îți recomandăm să permiți temporar Partajarea fișierelor atunci când se actualizează macOS.

2.4.3. Excepții

În fila **Excepții** pot fi setate excepții de site-uri web și aplicații:

- **Adaugă o excepție pentru site-uri web:**
  1. Fă clic pe butonul **Adăugare excepție**.
  2. Selectează **Doar site-uri web**, apoi fă clic pe butonul **Înainte**.
  3. Introdu adresa site-urilor web și selectează dacă dorești să permiți sau să blochezi accesul la acestea din meniul derulant.
  4. Apoi fă clic pe butonul **Adăugare**.

- **Excepție pentru aplicații și platforme web:**
  1. Fă clic pe butonul **Adăugare excepție**.
  2. Selectează **Aplicații și platforme web**, apoi fă clic pe butonul **Înainte**.
  3. Din lista furnizată, alege platforma pentru care dorești să creezi o excepție. Alternativ, utilizează bara de căutare pentru a găsi ceea ce cauți.
  4. Apoi fă clic pe butonul **Adăugare**.

- **Eliminare excepții:**
  Toate excepțiile pe care le configurezi vor apărea în secțiunea Filtrare conținut din lista aferentă acestora în partea de jos.
  Pentru a șterge o excepție, fă clic pe pictograma coș de gunoi situată în dreapta elementului respectiv.

2.5. Durata zilnică de utilizare a internetului

În contul Bitdefender Central, secțiunea Control parental, pentru fiecare profil de copil creat, se afișează graficul Timp zilnic pe internet. Acest grafic arată timpul total petrecut online de către copil pe toate dispozitivele alocate. Pentru a limita timpul petrecut de un copil pe internet:

1. Accesează profilul de copil și fă clic pe butonul **Setare limită de timp** din panoul **Timp zilnic pe internet**. Alternativ, fă clic pe meniul **Mai multe** din colțul din dreapta sus și selectează **Timp zilnic pe internet**.
2. Fă clic pe butonul **Activare limită de timp** pentru a activa această caracteristică.

Notă
În mod implicit, copilul are acces la internet timp de 1 oră și 30 de minute pe zi. În cazul în care părintele nu prelungește această limită de timp, accesul copilului la internet este întrerupt când se ajunge la 1 oră și 30 de minute.

Eliminarea limitei zilnice de timp:

- Pentru a dezactiva caracteristica Timp zilnic pe internet, accesează panoul de bord al profilului copilului tău, fă clic pe butonul **Editare timp** din panoul **Timp zilnic pe internet**, apoi apasă butonul **Pauză** din panoul **Limită de timp**.
- Pentru a elimina limita de timp într-o anumită zi, fă clic pe butonul ⊗ corespunzător zilei respective a săptămânii din panoul **Planificare**.

Schimbarea limitei de timp:

- Pentru a seta o limită de timp diferită într-o anumită zi a săptămânii, fă clic pe ziua respectivă în panoul **Planificare**, selectează limita dorită din meniul derulant și apoi fă clic pe butonul **Salvare modificări**. Poți selecta mai multe zile în același timp.

2.5.1. Sistem de recompensă

Funcția **Recompensă** îți permite să recompensezi sau să prelungești timpul petrecut de copilul tău în fața ecranului, promovând obiceiuri online sănătoase. Poți utiliza sistemul de recompensă în două moduri diferite:

- **Recompensă manuală:**
  1. Navighează la secțiunea Control parental din contul tău Bitdefender Central.
  2. Accesează profilul de copil și fă clic pe butonul **Recompensă** din panoul **Timp zilnic pe internet**.
  3. Selectează timpul suplimentar pe care dorești să îl adaugi și confirmă făcând clic pe **Recompensă**.

- **La cererea copilului:**
  Atunci când copilul tău atinge limita zilnică, poate solicita timp suplimentar prin intermediul aplicației Parental Control instalate pe dispozitivul său mobil. Ca părinte, vei primi o notificare în contul Bitdefender Central.

1. După ce te-ai conectat la contul tău Bitdefender Central, caută un punct roșu pe clopoțelul de notificări din colțul din dreapta sus al ecranului, care indică o solicitare în așteptare din partea copilului tău.
2. Examinează cererea și decide cât timp suplimentar să-i acorzi.

> **Notă**
> Copiii au opțiunea de a solicita prelungirea timpului zilnic pe internet doar pe dispozitivele Android și iOS.

2.6. Dezactivarea internetului pe dispozitivul copilului tău

Modul în care tu, ca părinte, gestionezi utilizarea internetului de către copilul tău este important pentru bunăstarea și productivitatea sa. Pentru a dezactiva temporar accesul la internet pe dispozitivul copilului tău folosind Bitdefender Parental Control:

1. Accesează Bitdefender Central și conectează-te la contul tău.
2. După ce te-ai conectat, fă clic pe fila **Control parental** din meniul din partea stângă.
3. Selectează **Detalii** din profilul de copil pentru care dorești să dezactivezi internetul.
4. Fă clic pe butonul **Oprire internet** din colțul din dreapta sus al panoului de bord aferent copilului.

> **Notă**
> Internetul va fi dezactivat pe toate dispozitivele copilului tău. Această acțiune anulează orice setări de control parental existente, cum ar fi rutinele, limita zilnică de timp sau categoriile permise.

5. Cât timp accesul la internet este întrerupt, butonul **Oprire internet** se modifică în **Activare internet**. Pentru a restabili accesul la internet, fă clic pe butonul **Activare internet**.

2.7. Rutine

Din aplicația Bitdefender Parental Control poți seta până la 3 rutine distincte pentru a programa situațiile în care accesul la internet al

copilului tău se întrerupe. Acestea oferă o abordare structurată pentru gestionarea activității online a copiilor, promovând obiceiuri sănătoase și implicarea familiei, asigurând în același timp siguranța copiilor. Aceste rutine sunt independente una de cealaltă, ceea ce înseamnă că poți alege să activezi doar una, două sau toate trei, după cum dorești:

- **Timpul dedicat concentrării**
  Creează un program care să includă timp pentru teme, studiu și alte activități.
- **Timpul dedicat somnului**
  Folosește rutina Timp dedicat somnului pentru a stabili perioada de odihnă a copilului tău.
- **Timpul dedicat familiei**
  Folosește rutina Timp dedicat familiei pentru a stabili un interval de timp în care copilul tău să fie prezent, de exemplu, la masă.

> **Notă**
> **Rutine versus Timp zilnic pe Internet:**
>
> Prin activarea rutinelor, timpul petrecut online nu se ia în considerare la calcularea limitei zilnice de timp petrecut pe Internet. Odată ce rutina se sfârșește, funcția Timp zilnic pe Internet reia calcularea duratei de utilizare a Internetului de către copil.
>
> Pentru a nu genera confuzie în rândul părinților, în timp ce o rutină este în curs de desfășurare, graficul Timp zilnic pe Internet nu va fi vizibil pe panoul de bord al profilului de copil până la finalizarea rutinei. În schimb, denumirea rutinei active va fi afișată în tot acest timp.

2.7.1. Configurarea rutinelor

Pentru a configura oricare dintre rutinele de control parental:

1. Accesează Bitdefender Central și conectează-te la contul tău.
2. În meniul din partea stângă, fă clic pe fila **Control parental**.
3. Accesează profilul de copil și selectează rutina dorită din meniul **Mai multe**.
4. Fă clic pe butonul **Activare** pentru a activa rutina selectată.
5. Această acțiune va afișa panourile **Planificare** și **Acces la Internet**.
   - **Programează scanarea:**

Pentru a activa o rutină în una sau mai multe zile din săptămână:

a. Selectează zilele dorite.

b. Selectează orele de început și de sfârșit ale rutinei din meniul derulant furnizat.

c. La sfârșit, fă clic pe butonul **Salvare modificări** pentru a confirma selecțiile.

Pentru a elimina rutina setată într-o anumită zi, fă clic pe butonul ⊗ corespunzător acelei zile a săptămânii.

- **Accesul la internet:**
  Panoul Acces la internet din cadrul unei rutine oferă două funcții principale care permit controlarea activității online a unui copil în anumite intervale de timp:
  - **Întreruperea completă a internetului:** părinții au opțiunea de a dezactiva complet accesul la internet pentru copilul lor în intervalele rutinelor programate. Prin dezactivarea butonului de **Acces la internet**, dispozitivele copilului nu vor putea accesa internetul în intervalul de timp alocat.
  - **Categorii sau site-uri web selectate:** alternativ, părinții pot alege să permită accesul la internet în intervalul aferent rutinei, dar să restricționeze accesul la anumite site-uri web sau categorii de conținut. Atunci când activezi butonul de **Acces la internet**, devin vizibile două file suplimentare, și anume filele **Categorii** și **Excepții**, care oferă acces la mai multe setări pentru Filtrare conținut</link>. (pagina 13)

2.8. Monitorizarea locației copilului tău

Odată cu răspândirea smartphone-urilor și a altor dispozitive mobile, monitorizarea locului în care se află copiii a devenit un instrument esențial pentru multe familii. Fie că vor să știe unde se află după școală, fie atunci când ies cu prietenii, posibilitatea de a monitoriza locația copiilor le oferă părinților liniștea că aceștia sunt în siguranță. Iată un ghid pas cu pas despre cum să monitorizezi locația copilului tău cu ajutorul funcției de localizare din Bitdefender Parental Control.

1. Accesează Bitdefender Central și conectează-te la contul tău.

2. După ce te-ai conectat, fă clic pe fila **Control parental** din meniul din partea stângă.
3. Dacă ai mai mulți copii, selectează **Detalii** din profilul copilului a cărui locație dorești să o monitorizezi.
4. Din panoul Locație, selectează dispozitivul Android sau iOS pe care dorești să îl monitorizezi, apoi fă clic pe butonul **Localizare**.

   Notă
   Caracteristica Localizare a aplicației Bitdefender Parental Control nu este disponibilă pentru dispozitivele Windows și macOS.

5. După o scurtă așteptare, un ac roșu va indica pe hartă locația actuală a copilului tău.

   Notă
   Locația este actualizată la fiecare 20 de minute. Dacă încerci să afli locația copilului tău în mai puțin de 20 de minute de la ultima localizare, este posibil ca locația afișată să nu reflecte locul unde se află în timp real.

3. DEZINSTALAREA APLICAȚIEI PARENTAL CONTROL

Dezinstalarea Bitdefender Parental Control pe dispozitivele Windows:

1. Șterge dispozitivul din profilul copilului tău accesând Bitdefender Central.
2. Deschide Panoul de control pe dispozitivul în cauză și identifică Bitdefender Parental Control în lista de **Programe și caracteristici**.
3. Dezinstalează aplicația Bitdefender Parental Control.

Dezinstalarea Bitdefender Parental Control pe dispozitivele macOS:

1. Șterge dispozitivul din profilul copilului tău accesând Bitdefender Central.
2. Deschide **Finder** pe dispozitivul macOS.
3. Accesează Aplicații și localizează folderul Bitdefender.
4. Deschide-l și execută **Bitdefender Uninstaller**.
5. Alege Bitdefender Parental Control din lista de produse de dezinstalat.
6. Introdu datele de autentificare de administrator și așteaptă să se termine dezinstalarea.

Dezinstalarea Bitdefender Parental Control pe dispozitivele Android și iOS:

1. Șterge dispozitivul din profilul copilului tău accesând Bitdefender Central.
2. Dezinstalează aplicația Parental Control de pe dispozitivul mobil ca pe orice altă aplicație sau accesând Google Play Store sau, respectiv, Appstore.

4. OBȚINE AJUTOR

4.1. 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.

4.2. 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.

4.2.1. 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/.

4.2.2. 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

4.2.3. 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/.

4.3. 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 22).

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

4.3.1. 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.