GHIDUL UTILIZATORULUI

Bitdefender CONSUMER SOLUTIONS

SecurePass

Bitdefender SecurePass

Ghidul utilizatorului

Publication date 20/11/2024

Aviz juridic

Bitdefender

Cuprins

DESPRE ACEST GHID

Scopul și publicul țintă

Acest ghid este destinat tuturor utilizatorilor Bitdefender pe toate sistemele de operare compatibile (Windows, MacOS, Android, iOS) care au ales Bitdefender SecurePass ca instrumentul preferat pentru gestionarea parolelor. Informațiile prezentate în acest manual sunt adecvate atât specialiștilor în computere, cât și tuturor celorlalți utilizatori, fiind un ghid accesibil și ușor de înțeles.

Acest ghid te va ajuta să afli cum să valorifici la maximum instrumentul nostru pentru gestionarea parolelor, care oferă un grad înalt de siguranță și numeroase caracteristici, abordând în detaliu toate caracteristicile și funcțiile acestuia.

Îți dorim o lectură plăcută și utilă.

Cum să folosiți acest ghid

Acest ghid este organizat în mai multe teme majore:

Introducere (pagina 5)

Inițiază procesul de instalare și începe să utilizezi Bitdefender SecurePass.

Importarea și exportarea parolelor (pagina 10)

Înțelegeți cum puteți importa sau exporta parole în și în afara SecurePass.

Caracteristici și funcții (pagina 14)

Află cum să utilizezi Bitdefender SecurePass și toate caracteristicile sale.

Obține ajutor (pagina 26)

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 SECUREPASS

Bitdefender SecurePass este un serviciu multi-platformă conceput să ajute utilizatorii să stocheze și să-și organizeze toate parolele utilizate în mediul online. Acesta integrează cei mai siguri algoritmi criptografici cunoscuți în prezent, oferind siguranță și securitate digitală la cel mai înalt nivel. Acesta funcționează ca o extensie de browser și ca o soluție tip aplicație mobilă pentru gestionarea identităților și parolelor și a informațiilor bancare, precum și a altor tipuri de informații confidențiale, utilizate pe mai multe dispozitive.

Bitdefender SecurePass poate salva, completa și genera automat parole și poate gestiona parolele tale pentru toate site-urile web și serviciile online cu ajutorul unei parole principale unice, pentru ca identitatea ta digitală, în ansamblul ei, să fie mai simplu de gestionat.

1.1. Versiunea gratuită de încercare și versiunile cu plată ale Password Manager

Versiunea gratuită de încercare a Bitdefender Password Manager funcționează, din toate punctele de vedere, exact ca versiunea cu plată a produsului, însă disponibilitatea acesteia va expira după 90 de zile de la activare.

> **Notă**
> Reține că, deși versiunea cu plată a produsului poate fi achiziționată sub forma unui produs individual, abonamentele Bitdefender Premium Security și Bitdefender Ultimate Security includ acces nelimitat la Password Manager.

2. INTRODUCERE

2.1. Cerințe de sistem

Poți utiliza cea mai nouă versiune a Bitdefender SecurePass numai pe dispozitivele care rulează următoarele sisteme de operare:

- **Pentru utilizatorii de PC-uri:**
  - Windows 7 cu Service Pack 1
  - Windows 8.1
  - Windows 10
  - Windows 11
- **Pentru utilizatorii de macOS:**
  - macOS 10.14 (Mojave) și versiuni ulterioare

> **Notă**
> Reține că performanța sistemului poate fi afectată pe dispozitivele care au procesoare de generație mai veche.

- **Pentru utilizatorii iOS:**
  - iOS 11.0 sau versiuni ulterioare
- **Pentru utilizatorii Android:**
  - Android 5.1 și versiuni ulterioare

> **Notă**
> - Caracteristica de deblocare cu amprenta este disponibilă pe **Android 6.0** și pe versiunile ulterioare.
> - Funcția de completare automată a parolelor este disponibilă pe **Android 8.0** și pe versiuni ulterioare și este compatibilă cu iPhone, iPad și iPod touch.

2.1.1. Cerințe de software

Pentru a putea utiliza Bitdefender SecurePass și toate caracteristicile sale, dispozitivele tale Windows și macOS trebuie să îndeplinească următoarele cerințe de software:

- **Microsoft Edge** (bazat pe Chromium 80 și versiuni ulterioare)
- **Mozilla Firefox** (versiunea 65 sau ulterioară)
- **Google Chrome** (versiunea 72 sau versiuni ulterioare)
- **Safari** (versiunea 12 sau versiuni ulterioare)

Notă
Cerințele de software nu se aplică sistemelor de operare Android și iOS.

Avertizare
Dacă cerințele de sistem descrise mai sus nu sunt îndeplinite, fie nu vei putea instala Bitdefender SecurePass, fie produsul nu va funcționa corespunzător.

2.2. Instalare

Acest capitol îți oferă îndrumări pentru a instala Bitdefender SecurePass pe browserele web atât de pe PC-urile Windows și macOS, cât și de pe dispozitivele mobile Android sau iOS.

Important
Înainte de a-l instala, asigură-te că ai un abonament Password Manager valid în contul tău **Bitdefender Central** pentru ca această extensie de browser să își recupereze validitatea din contul tău.

Abonamentele active sunt enumerate în secțiunea **Abonamentele mele** din contul Bitdefender Central.

2.2.1. Instalarea pe dispozitivele Windows și macOS

Spre deosebire de majoritatea aplicațiilor și programelor care trebuie instalate și configurate pe aceste dispozitive, soluția Password Manager de la Bitdefender este o extensie de browser, care se mai numește și add-on și care poate fi adăugată și activată rapid în browserul tău preferat.

Browserele compatibile cu produsul în prezent sunt: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge** și **Safari**.

- **Google Chrome**
- **Mozilla Firefox**
- **Microsoft Edge**
- **Safari**

Pentru a instala Bitdefender SecurePass:

1. După achiziționarea Bitdefender SecurePass, urmați pașii furnizați în e-mailul de confirmare pentru a vă activa abonamentul.
2. Conectați-vă la Bitdefender Central folosind acreditările dvs.
   În meniul din partea stângă, selectați **SecurePass**.
3. În panoul SecurePass, selectați browserul preferat.
4. Instalați extensia Browser:
   - **Google Chrome:**
     a. Faceți clic pe **Adaugă la Chrome** buton.
     b. În caseta de confirmare, faceți clic pe **Adaugă extensie**.
   - **Mozilla Firefox:**
     a. Faceți clic pe **Adaugă la Firefox** buton.
     b. Faceți clic pe **Instalați** butonul din colțul din dreapta sus al ecranului.
   - **Microsoft Edge:**
     a. Faceți clic pe **Obține** buton.
     b. Faceți clic pe **Adăugați extensie** în promptul care apare.
   - **Safari:**
     a. Programul de instalare SecurePass se va descărca pe dispozitivul dvs. macOS. Faceți dublu clic pe fișierul descărcat și urmați instrucțiunile de pe ecran de acolo.
     b. La sfârșitul procesului de instalare, deschideți **Safari** browser și selectați **Preferințe** în bara de meniu de sus.
     c. În ferestrele Preferințe, faceți clic pe **Fila Extensii**.

d. Bifați caseta de lângă **Bitdefender SecurePass** pentru a o activa.

Odată ce extensia este instalată, puteți trece la Procesul de configurare (pagina 9).

2.2.2. Instalarea pe dispozitivele Android

Cea mai simplă metodă pentru a instala Bitdefender Password Manager pentru telefoanele și tabletele Android, este să descarci aplicația direct din Google Play.

1. Înainte de orice altceva, după cumpărare, asigurați-vă că deschideți e-mailul de confirmare pe care l-ați primit pentru a urma instrucțiunile furnizate acolo pentru a vă activa abonamentul SecurePass.
2. Deschideți Magazinul Google Play pe dispozitivul dvs. Android.
3. În bara de căutare a Magazinului Google Play, tastați **Bitdefender SecurePass**, localizați și descărcați aplicația.
4. După finalizarea descărcării, deschideți aplicația și, dacă este necesar, urmați pașii de configurare de pe ecran necesari pentru a finaliza procesul de instalare.

Instalarea pe dispozitivul tău Android este acum finalizată.

2.2.3. Instalarea pe dispozitivele iOS

Cea mai simplă metodă de instalare a Bitdefender Password Manager pe dispozitivele iOS și iPadOS este de a descărca aplicația din Apple App Store.

1. Înainte de orice altceva, după cumpărare, asigurați-vă că deschideți e-mailul de confirmare pe care l-ați primit pentru a urma instrucțiunile furnizate acolo pentru a vă activa abonamentul SecurePass.
2. Deschideți App Store pe dispozitivul dvs. iOS.
3. În bara de căutare din App Store, tastați **Bitdefender SecurePass**, localizați și descărcați aplicația.
4. După finalizarea descărcării, deschideți aplicația și, dacă este necesar, urmați pașii de configurare de pe ecran necesari pentru a finaliza procesul de instalare.

Instalarea pe dispozitivul tău iOS/iPadOS este acum finalizată!

2.3. Procesul de configurare

Pentru a configura Bitdefender SecurePass pe browserul/dispozitivul mobil:

1. După terminarea procesului de instalare, deschideți extensia/aplicația SecurePass și conectați-vă.
   Utilizați datele de acreditare ale contului Bitdefender asociate abonamentului dvs. SecurePass.
2. Vi se va solicita să creați un **Parola principală**.

   > **Important**
   > Rețineți că veți avea nevoie de această parolă principală pentru a debloca toate parolele, informațiile cardului de credit și notele salvate în Bitdefender SecurePass. Aceasta este în esență cheia care permite proprietarului să utilizeze acest produs.

   Asigurați-vă că introduceți o parolă principală puternică, fără riscul de a o uita cu ușurință.
   După ce ați decis o parolă principală puternică și unică, faceți clic pe **Salvați și continuați**.
3. În continuare, vi se va oferi un **Cheie de recuperare**.

   > **Avertizare**
   > După crearea parolei principale, veți primi un **Cheie de recuperare din 24 de cifre**. Notați cheia de recuperare într-un loc sigur și nu o pierdeți. Această cheie este singura modalitate de a accesa parolele salvate în Password Manager în cazul în care se întâmplă **uitați parola principală** configurat anterior pentru contul dvs.

   - Salvați cheia de recuperare copiând-o în clipboard sau descărcând-o ca fișier PDF.
     Puteți apăsa **Închidere** când ați terminat.
4. După ce ați terminat, selectați **Accesați seiful** buton.

Acum că procesul de configurare este finalizat, puteți începe să utilizați Bitdefender SecurePass.

3. IMPORTAREA ȘI EXPORTAREA PAROLELOR

Bitdefender Password Manager este gândit astfel încât să faciliteze o comunicare și un transfer al datelor eficient către sursele externe, platformele și instrumentele tip software. Acesta este motivul principal pentru care necesitatea des întâlnită de a importa sau exporta parole în și din Bitdefender Password Manager poate fi îndeplinită cu ușurință.

3.1. Compatibilitate

Bitdefender Password Manager poate transfera date cu ușurință de la aplicațiile din următoarea listă:

- Managerul de parole Bitdefender
- Portofel Bitdefender
- Bitdefender SecurePass
- Safer Pass
- 1Parolă
- Kaspersky
- Dashlane
- Browserul Chrome
- Browserul Firefox
- Microsoft Edge
- Bitwarden
- LastPass
- KeePass
- RoboForm

Acest transfer de date între Bitdefender Password Manager și un alt software de administrare a conturilor poate fi realizat prin următoarele formate de date:

CSV, **JSON**, **XML**, **TXT**, **1pif** și **FSK**.

3.2. Importarea în Password Manager

Bitdefender Password Manager îți permite să imporți cu ușurință parolele din alte soluții de gestionare a parolelor și browsere. Dacă intenționezi să optezi pentru Bitdefender Password Manager în locul altui serviciu de gestionare a parolelor, probabil ai stocat un volum considerabil de date conectare precum nume de utilizator, parole și alte date de autentificare necesare pentru toate conturile tale.

Acum că ai ales Bitdefender Password Manager, vei dori să imporți acele date salvate în această soluție.

Iată cum poți importa în Bitdefender Password Manager informațiile stocate în alte aplicații și browsere web, **indiferent de sistemul de operare** pe care ai ales să instalezi acest produs:

1. Deschideți Bitdefender SecurePass și accesați **Setări**.
   - În browser:
     Faceți clic pe **Setări** în colțul din dreapta sus al paginii.
   - În aplicație:
     Apăsați pe **Mai mult** butonul din colțul din dreapta jos al ecranului și, în partea de sus a listei care apare ulterior, atingeți **Setări**.
2. În **Copiere de rezervă și restaurare** secțiune, selectați **Importați parole**. Se va deschide fereastra de import.
3. Selectați numele managerului de parole sau al browserului web pe care l-ați folosit înainte din meniul derulant accesibil prin **Selectați tipul de fișier** câmp.

   > **Notă**
   > Dacă a fost utilizată o parolă pentru a cripta fișierul, vi se va cere să o introduceți în **Parola** câmp; în caz contrar, îl puteți lăsa necompletat.

4. Selectați **Selectați fișierul de importat** depus.
   Navigați la locația în care au fost salvate datele exportate aparținând vechiului dvs. manager de parole. Alegeți fișierul după ce îl găsiți, apoi faceți clic pe **Deschis**.

5. După selectarea fișierului, selectați **Importați** în colțul din stânga jos al ferestrei de import. Procesul va începe în scurt timp, însoțit de o bară de progres.

Odată importate, parolele tale vor fi apoi accesibile pe toate dispozitivele unde ai instalat aplicația sau extensia de browser Bitdefender Password Manager.

> **Notă**
> Revenind la seiful de parole din SecurePass, veți observa un folder numit **Importați**, conținând toate datele din managerul de parole anterior sau browserul web.

3.3. Exportarea din Password Manager

Dacă vrei vreodată să optezi pentru un alt serviciu de gestionare a parolelor, Bitdefender Password Manager îți permite să exporți cu ușurință parolele salvate (inclusiv date de autentificare în conturi, note securizate etc.) într-un fișier CSV (valori separate prin virgulă) sau într-un fișier criptat, pentru ca despărțirea ta de Bitdefender Password Manager să nu fie un proces dificil.

> **Important**
> Un fișier CSV **nu** este criptat și conține numele de utilizator și parolele în format text simplu, ceea ce înseamnă că informațiile tale confidențiale pot fi citite de oricine are acces la dispozitivul tău. Prin urmare, îți recomandăm să urmezi instrucțiunile de mai jos pe un dispozitiv sigur.

Iată cum îți poți exporta datele din Bitdefender Password Manager:

1. Deschideți Bitdefender SecurePass și accesați **Setări**.
   - În browser:
     Faceți clic pe **Setări** în colțul din dreapta sus al paginii.
   - În aplicație:
     Apăsați pe **Mai mult** butonul din colțul din dreapta jos al ecranului și, în partea de sus a listei care apare ulterior, atingeți **Setări**.
2. În **Copiere de rezervă și restaurare** secțiune, selectați **Exportați parole**. Se va deschide fereastra de export.
3. Faceți clic pe **Selectați tipul de fișier**. Din meniul derulant, alegeți să exportați datele fie în format JSON, fie într-un format CSV. De

asemenea, puteți introduce o parolă cu care să protejați fișierul exportat.

Bifați caseta corespunzătoare dacă doriți să includeți și elemente partajate.

4. Faceți clic pe **Export** în colțul din stânga jos al ferestrei de export și salvați fișierul exportat pe dispozitiv.

4. CARACTERISTICI ȘI FUNCȚII

Acest capitol îți va descrie toate caracteristicile și funcțiile Bitdefender Password Manager și îți va explica utilitatea lor și cum să le valorifici la maximum.

4.1. Salvați manual parolele

Puteți stoca în siguranță informații precum parole, acreditări și altele, cum ar fi informațiile cardului de credit sau notele în Bitdefender SecurePass manual, în felul următor:

1. Deschide Situl Bitdefender SecurePass
2. În **Seiful meu** fila, apăsați tasta **+Adaugă articol** buton.
3. Selectați tipul de element pe care doriți să îl adăugați. (cont, card de credit, identitate sau notă).
4. Completați câmpurile obligatorii în funcție de elementul selectat.
5. După completarea tuturor detaliilor necesare, salvați elementul pentru a-l adăuga în seiful SecurePass.

4.2. Generator de parole

Bitdefender SecurePass include o caracteristică de generare a parolelor care vă poate ajuta la crearea de parole sigure.

Pentru a accesa și utiliza generatorul de parole:

1. Deschideți Bitdefender SecurePass și accesați **Generați parola** fila din partea stângă a ecranului. Acest lucru vă va duce la Generatorul de parole integrat în SecurePass
2. Personalizați parola pe care urmează să o generați în funcție de propriile nevoi și preferințe.
   - Lungimea parolei: Trageți glisorul pentru a determina orice lungime cuprinsă între 8 și 32 de caractere.
   - Literele majuscule/minuscule: Selectați ce - sau ambele - tipuri de litere doriți adăugate pentru nivelul de complexitate al parolei.
   - Numere: Bifați această casetă vor include numere în șirul de caractere care cuprinde parola.

- Caractere speciale: Adăugați simboluri la parola dvs. pentru a spori complexitatea parolei.

> **Notă**
> Apăsați **Salvați setările** buton pentru SecurePass pentru a le aminti și pentru a genera întotdeauna parole pe baza setărilor pe care le-ați salvat.

3. Generați o nouă parolă făcând clic pe pictograma săgeată circulară situată sub parola afișată în prezent. Fiecare clic generează un nou șir de caractere.
4. Odată mulțumit de parola generată, o puteți copia în clipboard sau faceți clic pe **Salvați contul** buton pentru a-l stoca în seif (prin asociere cu alte informații despre cont).

> **Notă**
> De asemenea, puteți genera rapid o parolă **direct din formularele de înscriere** făcând clic pe pictograma Bitdefender SecurePass prezentă în câmpul de parolă al paginii de înscriere. Făcând clic pe el, puteți alege apoi **Generați parola** opțiune.

4.3. Verificarea puterii parolei

Bitdefender SecurePass oferă posibilitatea de a evalua puterea parolelor salvate și a datelor sensibile. Aceasta este o caracteristică vitală în evaluarea și evaluarea oricăror potențiale vulnerabilități la confidențialitatea și securitatea datelor.

Pentru a verifica punctele forte ale parolelor stocate:

1. Deschideți Bitdefender SecurePass și, în meniul de e-mail, selectați **Raport de securitate** fila.
   Fila Raport de securitate este defalcată în patru secțiuni: încălcat, slab, vechi și duplicat.
2. Numărul de parole care se încadrează în fiecare dintre cele patru categorii va fi afișat pe ecran.
   În plus, trecând prin lista de parole stocate, fiecare parolă va fi etichetată cu categoria sub care se află.

Pentru a înțelege semnificația din spatele acestor niveluri de securitate, mai jos sunt câteva detalii scurte despre fiecare dintre ele:

- Parole încălcate: Dacă oricare dintre acreditările dvs. a făcut parte dintr-o încălcare a datelor, acestea vor fi listate sub **încălcat** secțiunea.

  > **Notă**
  > Pentru a verifica dacă oricare dintre parolele dvs. a fost compromisă și scursă prin încălcări ale datelor, faceți clic pe **Rulați scanarea de securitate** buton.

- Parole slabe: SecurePass va identifica și semnaliza **slab** parolele stocate în seiful dvs. pe baza unui algoritm intern, care rulează local, care analizează diverse criterii, cum ar fi lungimea parolei, varietatea de caractere și includerea cifrelor sau a literelor mari, printre alți factori.
- Parole vechi: Parolele care au fost salvate și nemodificate pentru o perioadă mai lungă de șase luni vor fi marcate ca **vechi**.
- Parole duplicate: Având în vedere că utilizarea acelorași parole pe mai multe platforme și conturi prezintă un risc mare de securitate, SecurePass va semnala parolele utilizate în mai multe locuri ca fiind **duplicat**.

4.4. Organizarea datelor

În cadrul Bitdefender SecurePass, puteți organiza și, prin urmare, gestiona mai ușor toate articolele salvate.

Puteți clasifica elementele în foldere specifice pentru acces ușor urmând acești pași:

1. Deschideți Bitdefender SecurePass și accesați **Seiful meu**. Aici, atingeți **Adaugă dosar** buton.
2. Denumiți folderul și atingeți **Creați** buton.
   Noul folder va apărea acum în seif.

Pentru a muta elemente în folderul creat:

1. Faceți clic pe orice cont pe care doriți să îl mutați și apăsați tasta **Editați** buton.
2. Apăsați locația afișată lângă **Salvați elementul în** și selectați numele folderului din lista derulantă.
3. Apăsați **Salvați contul** buton.

Contul va fi acum stocat în folderul selectat.

4.5. Completare automată inteligentă

Bitdefender SecurePass vă permite să completați automat acreditările contului și informațiile pe orice formular Sing-In online.

> **Notă**
> Ca extensie de browser web, fie pe Windows, fie pe macOS, funcția de completare automată ar trebui să funcționeze perfect.

4.5.1. Completare automată pe Android

Pentru a configura SecurePass pe Android pentru a utiliza Autofill:

1. Deschideți aplicația Bitdefender SecurePass pe dispozitivul dvs. Android.
2. Apăsați pe **Mai mult** buton de meniu.
3. În partea de sus a ecranului, atingeți **Setări**.
4. Apăsați pe **Faceți din acesta managerul de parole implicit**
5. Activați Bitdefender SecurePass în lista de servicii de completare automată.

> **Notă**
> De asemenea, puteți accesa setările dispozitivului dvs. Android, în **Parole și conturi** > **Serviciu de completare automată** > activați Bitdefender SecurePass.
>
> Pentru Android 11 sau versiunile anterioare ale sistemului de operare, setările sunt: **Sistem** > **Limbă și introducere** > **Avansat**.

6. Apăsați **OK**.

Odată ce această configurare este finalizată, ori de câte ori atingeți un câmp de conectare, o opțiune numită Bitdefender SecurePass va apărea pe ecran. Puteți să o atingeți pentru a deschide aplicația. Conectați-vă la SecurePass și acreditările dvs. vor fi completate automat

4.5.2. Completare automată pe iOS

Pentru a configura SecurePass pe dispozitivul dvs. iOS pentru a utiliza Completarea automată:

1. Deschideți **Setare** aplicație pe iPhone sau iPad și selectați **Generale**.

2. Apăsați pe **Completare automată și parole**. Asigurați opțiunea **Completarea automată a parolelor și cheilor de acces** sau **Completarea automată a parolelor** - în funcție de versiunea iOS - este activată.
3. În **Formular de completare automată** listă, activați **Bitdefender SecurePass** aplicație.

Odată ce această configurare este finalizată, ori de câte ori atingeți un câmp de conectare, o opțiune numită Bitdefender SecurePass va apărea pe ecran. Puteți să o atingeți pentru a deschide aplicația. Conectați-vă la SecurePass și acreditările dvs. vor fi completate automat

4.5.3. Completarea automată a detaliilor cardului

În timp ce SecurePass oferă o pictogramă ușor accesibilă pentru completarea automată a acreditărilor de conectare și a parolelor, funcția de completare automată a informațiilor despre cardul de credit funcționează diferit:

1. Navigați la pagina de plată sau de plată a site-ului web pe care doriți să utilizați informațiile stocate despre cardul de credit.
2. Faceți clic dreapta pe orice zonă goală a paginii de plată. Aceasta va solicita ca meniul contextual să apară pe ecran.
3. Selectați Bitdefender SecurePass din Meniu plasând cursorul peste opțiune. Aceasta va deschide un submeniu cu opțiuni suplimentare
4. Alege **Completarea automată a informațiilor despre cardul de credit**. Aceasta va afișa o listă a oricăror carduri de credit pe care le-ați stocat în seiful SecurePass
5. Selectați cardul preferat.

În acest fel, SecurePass va completa automat formularul de plată depus cu detaliile cardului de credit pe care l-ați ales.

5. UTILIZAȚI CA APLICAȚIE 2FA

Puteți alege oricând să utilizați Bitdefender SecurePass ca aplicație de autentificare cu doi factori pentru orice site web sau platformă doriți și să gestionați codurile 2FA alături de parole în felul următor:

1. Accesați setările de securitate ale site-ului web sau ale aplicației în care doriți să activați funcția 2FA. De obicei, vi se va prezenta un cod QR sau un cod de verificare în timpul procesului.
2. Lansați Bitdefender SecurePass și accesați contul corespunzător pe care doriți să îl configurați pentru utilizarea 2FA. Faceți clic pe **Editați** buton.
3. Derulați în partea de jos a paginii de intrare a contului în SecurePass și apăsați pe **Autentificare cu doi factori** opțiune.
4. Scanați codul QR sau introduceți codul manual.
   Odată făcut acest lucru, SecurePass va confirma configurarea reușită a autentificării cu doi factori.
5. După aceasta, apăsați noul **Vizualizați codul** buton acum vizibil în interfață. Acolo este afișat un cod sensibil la timp
6. Reveniți la contul în care ați activat funcția 2FA și introduceți codul de la Bitdefender SecurePass pentru a verifica configurarea.

După finalizarea acestui proces de configurare, apăsați tasta **Salvați contul** butonul din SecurePass pentru a finaliza procesul.

De acum înainte, când cântați pe platforma pentru care ați configurat funcția 2FA, vi se va solicita să utilizați codurile 2FA SecurePass pentru contul respectiv, oferind un nou nivel de securitate pentru contul în cauză.

6. PARTAJAȚI DATELE

Bitdefender SecurePass vine cu posibilitatea de a partaja în siguranță informații sensibile, cum ar fi acreditările, parolele sau detaliile cardului de credit.

Puteți utiliza funcția de partajare prin link-uri:

1. Alegeți un element stocat în seif.
   - În browser:
     Accesați seiful dvs. și faceți clic pe elementul pe care doriți să îl partajați. În partea dreaptă, faceți clic pe meniul cu trei puncte și selectați **Partajați linkul**.
   - În aplicație:
     Accesați seiful și atingeți elementul pe care doriți să îl partajați. Atingeți pictograma linkului și alegeți **Generați link de partajare** opțiune.
2. Creați linkul Partajare specificând:
   - Data de expirare a link-ului.
   - Limita de utilizare.
   - Dacă linkul ar trebui sau nu să fie protejat prin parolă.
3. Odată generat, copiați linkul generat și trimiteți-l destinatarului dorit.

6.1. Partajare cu grupuri

Grupurile sunt create în scopul de a face partajarea datelor și mai ușoară. Puteți crea diverse grupuri în cadrul Bitdefender SecurePass cu alți utilizatori pentru a partaja în siguranță date sensibile:

1. Creați un grup:
   - Du-te la **Grupuri** și apăsați tasta **Creați un grup** buton din fila Grupuri.
   - Setați un nume de grup și apoi apăsați tasta **Creați grup** buton.
2. Adăugați elemente în grupuri:
   - În browser:

Accesați seiful dvs. și faceți clic pe elementul pe care doriți să îl partajați. Faceți clic pe meniul cu trei puncte din partea dreaptă a elementului și alegeți **Adaugă în grup**.

- În aplicație:
  Accesați seiful dvs. și faceți clic pe elementul pe care doriți să îl partajați. Alege **Împărtășește cu grupul** opțiune.

Selectați grupul cu care doriți să partajați elementul.

3. Setați drepturile de acces (citire, scriere, acordare) în funcție de nivelul de control pe care doriți să îl oferiți membrilor grupului.
4. Apăsați **Salvați**, apoi **Terminat**.

Dvs. și membrii grupului puteți revizui elementele partajate din secțiunea grupului.

6.2. Gestionarea grupurilor

În **Grupuri** secțiunea Bitdefender SecurePass puteți revizui toate grupurile create și le puteți gestiona în funcție de nevoile dvs.:

- Redenumiți grupuri.
- Editați membrii. (invitați membri noi, atribuiți drepturi anumitor membri, acordați drepturi de administrator sau partajare și eliminați membrii existenți)
- Lăsați grupurile.
- Ștergeți grupurile.

7. BLOCAȚI CONTUL

Bitdefender SecurePass vine cu un **Blocați contul** funcție care vă blochează instantaneu contul și încheie toate sesiunile active pe toate dispozitivele care au acces la acesta. Această caracteristică este deosebit de utilă atunci când apar suspiciuni de acces neautorizat.

Pentru a vă bloca contul SecurePass:

1. Deschideți Bitdefender SecurePass.
2. Odată ajuns în SecurePass:
   - În browser:
     Faceți clic pe **Setări** în colțul din dreapta sus al paginii.
   - În aplicația mobilă:
     Apăsați pe **Asigură-mă** buton de meniu.
3. Apăsați **Blocați contul** buton pentru a vă deconecta instantaneu de pe toate dispozitivele și pentru a termina sesiunile în curs.

8. ÎNTREBĂRI FRECVENTE

Întrucât există anumite întrebări în legătură cu Bitdefender Password Manager care au tendința să revină, noi avem răspunsurile! De aici puteți afla mai multe detalii despre contul dvs. Bitdefender, cum să importați parolele, despre protocoalele de securitate a datelor și alte subiecte importante pentru clienții noștri.

Întrebări generale despre Bitdefender Password Manager

Ce se întâmplă când Bitdefender Password Manager expiră?

Când abonamentul tău Password Manager expiră și nu mai este activ, ai la dispoziție cel mult 90 de zile pentru a-ți exporta parolele. Parolele tale vor mai fi păstrate pentru încă 30 de zile, ca back-up. În aceste 90 de zile, vei avea acces numai la funcția de exportare datelor. Nu vei mai putea utiliza Password Manager. Caracteristica de completare automată nu va mai funcția și nici nu vei mai putea genera parole.

La finalul perioadei de grație de 90 de zile, ai la dispoziție încă 30 de zile pentru a contacta serviciul de asistență al Bitdefender și a solicita restituirea parolelor tale în baza de date live. În acel moment, îți vei putea exporta parolele de la Bitdefender Password Manager.

Datele tale vor fi păstrate în baza de date live doar până la finalul zilei în care a fost restabilită la cerere. La miezul nopții, baza de date va fi ștearsă și, dacă nu ai depășit perioada suplimentară de 30 de zile, parolele tale vor putea fi restabilite din nou din datele back-up. Datele neprelucrate din baza de date, păstrate ca back-up, pot fi furnizate la cerere utilizatorului, însă baza de date este criptată și informațiile nu pot fi accesate.

Ce este o Parolă principală și de ce trebuie să o țin minte?

Parola principală este cheia care deblochează accesul la toate parolele stocate în contul tău Bitdefender Password Manager. Parola principală trebuie să conțină cel puțin 8 caractere. De aceea, îți recomandăm să creezi o parolă principală puternică, să o memorezi și să nu o împărtășești nimănui. Pentru a crea o parolă principală puternică, îți recomandăm să utilizezi o combinație de litere mari și litere mici, cifre și caractere speciale (precum #, $ sau @).

De ce nu stocați Parola principală și ce se întâmplă dacă o uit?

Motivul pentru care nu stocăm Parola ta principală pe serverele noastre este ca tu să fii singurul care are acces la contul tău. Astfel este siguranță. Dacă Bitdefender Password Manager nu-ți recunoaște parola principală, asigură-te că ai introdus-o corect și că tasta Caps Lock nu este activă pe tastatura ta.

Dacă nu mai știi care este parola ta principală, poți utiliza întotdeauna Cheia de recuperare pentru a-ți debloca contul Password Manager. În timpul procesului de conectare, Bitdefender Password Manager generează o {1}cheie de recuperare{2} care poate fi utilizată pentru a redobândi accesul la cont fără a-ți pierde datele.

Ce este modul offline?

Modul offline este activat automat atunci când conexiunea la Internet se întrerupe în timpul utilizării Bitdefender SecurePass. Dacă sunteți deja conectat și ați introdus parola principală, modul Offline vă permite să accesați parolele atunci când o conexiune la Internet nu este la îndemână.

Cum dezinstalez Bitdefender Password Manager?

Pentru a dezinstala Bitdefender Password Manager:

- Pe Windows și macOS:
  Elimină extensia Password Manager din browserul tău web. Fă clic dreapta pe pictograma Bitdefender și selectează „Elimină”.
- Pe Android:
  Apasă lung pe aplicația Password Manager, apoi gliseaz-o în partea de sus a ecranului unde apare mesajul „Dezinstalare”.
- Pe iOS și iPadOS:
  Apasă lung pe aplicația Password Manager până când toate aplicațiile de pe ecran se mișcă, apoi apasă pe X din partea stângă sus a pictogramei Bitdefender.

Întrebări privind confidențialitatea și securitatea Bitdefender Password Manager

Este posibil ca angajații Bitdefender să aibă acces la parolele mele?

Categoric nu. Confidențialitatea ta este prioritatea noastră principală. Acesta este motivul pentru care nu stocăm parola principală pe serverele noastre de date: pentru ca nimeni să nu aibă acces la contul tău, nici măcar angajații companiei. Fiecare parolă și cont sunt criptate la nivel

înalt cu cel mai puternic algoritm de securitate a datelor, iar codul pe care îl vedem arată ca un șir aleatoriu de numere și litere amestecate.

Ce s-ar întâmpla dacă serverele Password Manager ar fi compromise?

Fiecare parolă este criptată la nivel local, pe dispozitivul tău, înainte să ajungă la serverele noastre, astfel că dacă hackerii ar încerca să pătrundă în sistemul nostru, ar obține doar pagini de litere și cifre aleatorii fără cheia care le poate decripta. Acest lucru înseamnă că atât tu, cât și datele contului tău sunt întotdeauna păstrate în siguranță de noi.

9. OBȚINE AJUTOR

9.1. 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.

9.2. 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.

9.2.1. 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/.

9.2.2. 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

9.2.3. 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/.

9.3. 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 26).

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

9.3.1. 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.