



Bitdefender®

**Bitdefender Endpoint
Security Tools for
Windows**

MANUAL DE UTILIZARE

Bitdefender Endpoint Security Tools for Windows Manual de utilizare

Publicat 2019.11.29

Copyright© 2019 Bitdefender

Termeni legali

Toate drepturile rezervate. Nicio parte a acestui document nu va putea fi reprodusă sau transmisă sub nicio formă și prin niciun mijloc, fie el electronic sau mecanic, inclusiv fotocopiere, înregistrare, sau orice sistem de stocare și recuperare de date, fără acordul scris al unui reprezentant autorizat al Bitdefender. Este posibilă includerea unor scurte citate în recenzii, dar numai cu condiția menționării sursei citate. Conținutul documentului nu poate fi modificat în niciun fel.

Avertisment și declinarea responsabilității. Acest produs și documentația aferentă sunt protejate de legea drepturilor de autor. Informațiile incluse în acest document sunt furnizate „ca atare”, fără nicio garanție. Deși s-au luat toate măsurile de prevedere în momentul alcătuirii acestui document, autorii săi nu vor fi în niciun fel ținuti responsabili față de nici o persoană fizică sau juridică pentru pierderi sau daune cauzate sau care se presupune a fi fost cauzate, direct sau indirect, de informațiile cuprinse în acest material.

Acest document conține linkuri către siteuri web aparținând unor terți, care nu se află sub controlul Bitdefender; prin urmare, Bitdefender nu este responsabilă pentru conținutul respectivelor siteuri. Responsabilitatea accesării oricăruia dintre siteurile terților al căror link este furnizat în acest document vă aparține în totalitate. Bitdefender furnizează aceste linkuri exclusiv pentru ușurarea consultării documentului și prezența lor nu presupune faptul că Bitdefender susține sau își asumă responsabilitatea pentru conținutul siteurilor către care duc acestea.

Mărci înregistrate. Acest document poate conține nume de mărci înregistrate. Toate mărcile comerciale înregistrate sau neînregistrate din acest document aparțin exclusiv proprietarilor acestora și sunt redată ca atare.

Cuprins

Prefață	iv
1. Scopul și publicul țintă	iv
2. Cum să folosiți acest ghid	iv
3. Convenții utilizate în ghid	iv
4. Comentarii	v
1. Introducere	1
1.1. Pictograma din bara de sistem	1
1.2. Fereastra principală	2
1.2.1. Zona de stare	3
1.2.2. Cronologia evenimentelor	4
1.3. Fereastra Module	5
1.4. Meniul Acțiuni	10
2. Scanarea pentru identificarea programelor periculoase	12
2.1. Scanarea unui fișier sau folder	12
2.2. Rularea unei scanări rapide	12
2.3. Efectuarea unei scanări complete	13
2.4. Configurarea și executarea unui proces de scanare personalizat	14
2.4.1. Tipuri de fișiere	15
2.4.2. Ce se scanează?	16
2.4.3. Ce trebuie făcut?	17
2.5. Examinarea rapoartelor de scanare	18
3. Utilizarea criptării de volum	20
3.1. Criptarea sistemului	20
3.2. Decriptarea sistemului	22
3.3. Verificarea stării de criptare	22
3.4. Modificarea codului PIN sau a parolei de criptare	23
4. Actualizări	24
4.1. Tipuri de actualizări	24
4.2. Cum verificați dacă protecția este la zi	24
4.3. Efectuarea unei actualizări	25
5. Evenimente	26
6. Utilizarea interfeței cu linie de comandă	28
6.1. Comenzi acceptate	29
6.2. Coduri de eroare aferente liniei de comandă	39
7. Obținere ajutor	40
Vocabular	41

Prefață

1. Scopul și publicul țintă

Această documentație este destinată utilizatorilor de **Bitdefender Endpoint Security Tools**, software-ul client al serviciului de securitate Security for Endpoints care se instalează pe calculatoare și servere pentru a le proteja împotriva programelor periculoase și a altor amenințări de pe Internet și pentru a asigura aplicarea politicilor destinate controlului utilizatorilor.

Informațiile prezentate în acest document sunt accesibile pentru orice utilizator familiarizat cu sistemul de operare Windows.

2. Cum să folosiți acest ghid

Acest ghid este organizat astfel încât să găsiți cu ușurință informațiile de care aveți nevoie.

[„Introducere” \(p. 1\)](#)

Familiarizați-vă cu interfața utilizator Bitdefender Endpoint Security Tools.

[„Scanarea pentru identificarea programelor periculoase” \(p. 12\)](#)

Aflați cum să realizați scanările pentru identificarea programelor periculoase.

[„Actualizări” \(p. 24\)](#)

Aflați despre actualizările Bitdefender Endpoint Security Tools.

[„Evenimente” \(p. 26\)](#)

Verificați activitatea Bitdefender Endpoint Security Tools.

[„Obținere ajutor” \(p. 40\)](#)

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

3. Convenții utilizate în ghid

Convenții tipografice

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

Aspect	Descriere
business-docs@bitdefender.com	Adresele de e-mail sunt inserate în text ca informație de contact.
„Prefață” (p. iv)	Acesta este un link intern, către o locație din document.
nume fișier	Numele fișierelor și ale directoarelor sunt tipărite cu caractere monospațiate.
opțiuni	Toate opțiunile produsului sunt tipărite cu caractere bold .
cuvânt cheie	Cuvintele cheie sau frazele importante sunt evidențiate cu ajutorul caracterelor bold .

Atenționări

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



Notă

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



Important

Acest lucru necesită atenția dumneavoastră și nu este recomandat să-l ocoliți. De obicei, aici sunt furnizate informații importante, dar care nu sunt critice.

4. Comentarii

Vă rugăm să ne scrieți despre cum considerați că ar putea fi îmbunătățit acest ghid, ajutându-ne astfel să vă oferim cea mai bună documentație posibilă.

Anunțați-ne printr-un e-mail la business-docs@bitdefender.com.

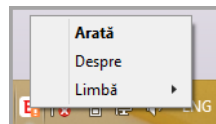
1. INTRODUCERE

Bitdefender Endpoint Security Tools este un program de securizare a calculatorului complet automatizat, administrat de la distanță de către administratorul de rețea. După instalare, vă protejează contra tuturor tipurilor de programe periculoase (cum ar fi viruși, spyware și cai troieni), atacuri în rețea, atacuri de tip phishing și furtul de date. De asemenea, poate fi folosit pentru punerea în aplicare a politicilor organizației dvs. privind calculatoarele și utilizarea internetului. Bitdefender Endpoint Security Tools va lua pentru dvs. majoritatea deciziilor în materie de securitate și rareori va afișa alerte de tip pop-up. Detaliile privind acțiunile întreprinse și informațiile despre utilizarea programului sunt disponibile în istoricul **Evenimente**.

1.1. Pictograma din bara de sistem

La momentul instalării, Bitdefender Endpoint Security Tools afișează o pictogramă **B** în bara de sistem. Dacă faceți dublu clic pe această pictogramă, se deschide fereastra principală. Dacă faceți clic dreapta pe pictogramă, un meniu contextual vă va oferi câteva opțiuni utile.

- **Arată** - deschide fereastra principală a Bitdefender Endpoint Security Tools.
- **Despre** - deschide o fereastră cu informații despre Bitdefender Endpoint Security Tools și indică unde trebuie să căutați ajutor în cazul în care apar probleme neprevăzute. Această fereastră include, de asemenea, un link către politica de confidențialitate Bitdefender.
- **Limbă** - vă permite să modificați limba interfeței cu utilizatorul.
- **Utilizator privilegiat** - vă permite să accesați și să modificați setările de securitate, după introducerea parolei în fereastra de autentificare. Control Center primește o notificare atunci când o stație de lucru este în modul Utilizator privilegiat, iar administratorul Control Center poate suprascrie oricând setările de securitate locale.





Pictograma din bara de sistem



Important

Această opțiune este disponibilă numai dacă este permisă de administratorul de rețea prin intermediul setărilor politicii de securitate. Această opțiune nu este disponibilă pentru Bitdefender Endpoint Security Tools for Windows Legacy.

Pictograma Bitdefender Endpoint Security Tools din bara de sistem vă informează dacă apar probleme care vă afectează calculatorul, prin modificarea aspectului:

-  Critical issues affect the security of the system.
-  Some issues affect the security of the system.




Notă

Administratorul de rețea poate decide să ascundă pictograma barei de sistem.

1.2. Fereastra principală

Fereastra principală a Bitdefender Endpoint Security Tools vă permite să verificați starea de protecție și să efectuați sarcini de scanare. Puteți accesa orice opțiune prin doar câteva clicuri. Configurarea și administrarea protecției sunt realizate de la distanță, de către administratorul de rețea.

Pentru a accesa interfața principală a Bitdefender Endpoint Security Tools, navigați din meniul Start al Windows, urmând calea **Start** → **All Programs** → **Bitdefender Endpoint Security Tools** → **Deschideți Consola de Securitate** sau, mai rapid, faceți dublu clic pe pictograma Bitdefender Endpoint Security Tools  din bara de sistem.



Fereastra principală

Fereastra este organizată în două secțiuni principale:

- Zona de stare
- Cronologia evenimentelor

1.2.1. Zona de stare

Zona de **Stare** oferă informații utile cu privire la securitatea sistemului.



Zona de stare

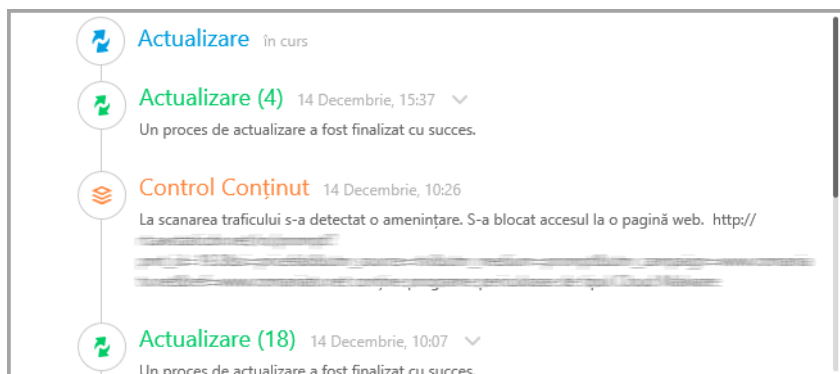
Puteți afla cu ușurință care este starea de securitate a sistemului pe baza simbolului de stare afișat în stânga zonei de stare:

- **Bifă de culoare verde.** Nu există probleme de rezolvat. Calculatorul și datele dumneavoastră sunt protejate.
- **Semn de exclamație de culoare galbenă.** Există probleme non-critice care afectează securitatea sistemului dumneavoastră.
- **X de culoare roșie.** Probleme critice afectează securitatea sistemului dumneavoastră.

Pe lângă simbolul de stare, un mesaj detaliat privind starea de securitate este afișat în dreapta zonei de stare. Puteți vedea problemele de securitate detectate făcând clic în interiorul zonei de stare. Problemele existente vor fi rezolvate de administratorul de rețea.

1.2.2. Cronologia evenimentelor


Bitdefender Endpoint Security Tools păstrează un jurnal detaliat al evenimentelor referitoare la activitatea sa pe computer dvs. (inclusiv activitățile monitorizate de Content Control).

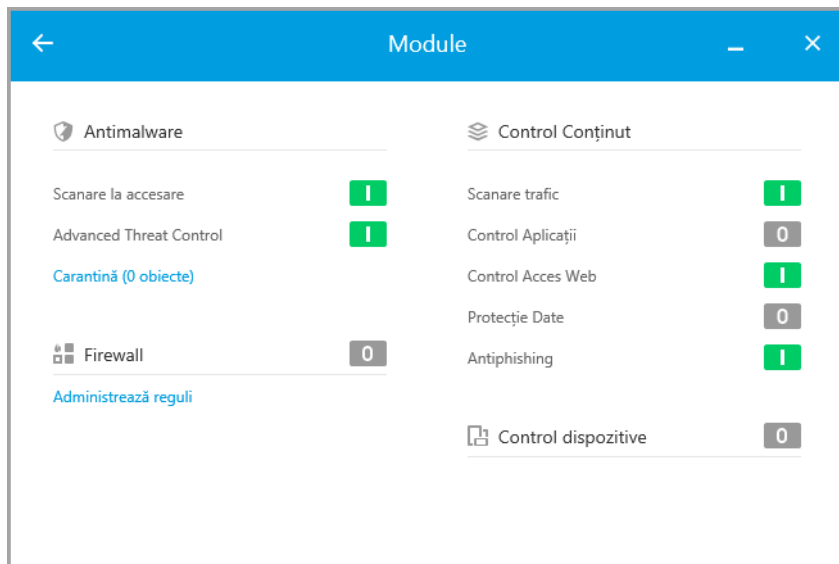


Cronologia evenimentelor

Cronologia **Evenimente** reprezintă un instrument foarte important pentru monitorizarea protecției dumneavoastră Bitdefender. De exemplu, puteți verifica rapid dacă actualizarea a fost efectuată cu succes sau dacă au fost detectate aplicații periculoase pe calculatorul dumneavoastră.

1.3. Fereastra Module

Fereastra **Module** afișează informații utile referitoare la starea și activitatea modulelor de protecție instalate. Pentru a deschide fereastra **Module**, faceți clic pe butonul **Module**  din fereastra principală Bitdefender Endpoint Security Tools.



Fereastra Module

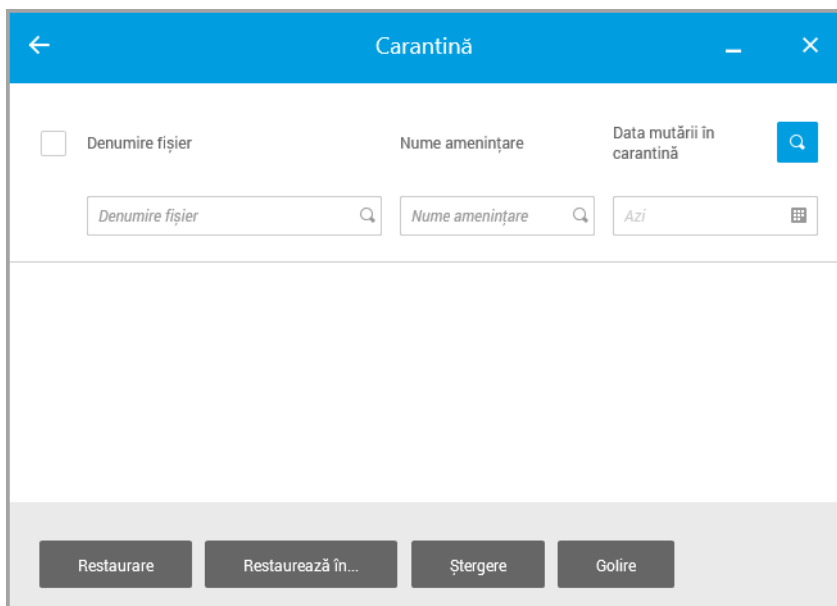
Antimalware

Protecția antimalware reprezintă fundația securității dumneavoastră. Bitdefender Endpoint Security Tools vă protejează în timp real și la cerere împotriva tuturor tipurilor de malware, precum viruși, troieni, programe de tip spyware, adware etc.

- **la accesare.** Scanarea la accesare previne pătrunderea în sistem a noilor amenințări malware prin scanarea fișierelor locale și din rețea atunci când acestea sunt accesate (deschise, mutate, copiat sau executate), a sectoarelor de boot și a eventualelor aplicații nedorite.
- **HyperDetect.** HyperDetect detectează atacurile avansate și activitățile suspecte încă din faza de pre-executare. Acest nivel de securitate conține

modele de învățare automată (machine learning) și tehnologie de detecție a atacurilor ascunse.

- **Advanced Threat Control.** Aceasta monitorizează continuu aplicațiile, funcționând pe stația de lucru în cazul acțiunilor de tip malware. Advanced Threat Control va încerca automat să dezinfecteze fișierul detectat.
- **Carantină** afișează o listă a fișierelor trecute în carantină, locația lor inițială, ora și data mutării în carantină și starea lor de securitate. Folosiți butoanele din josul paginii pentru a șterge sau restaura fișierele dorite. Dacă doriți să ștergeți toate fișierele din Carantină, faceți clic pe butonul **Golire**.



Carantină

Control Conținut

Modulul de control al conținutului vă protejează când navigați pe internet contra atacurilor de tip phishing, tentativelor de fraudă, scurgerilor de date confidențiale și conținutului web nedorit. De asemenea, cuprinde o varietate de funcții de control al activității utilizatorului care ajută administratorul de rețea să aplice politicile de utilizare a calculatorului și internetului.

- **Scanare trafic.** Această componentă previne descărcarea programelor malware pe stația de lucru prin scanarea mesajelor de e-mail primite și a traficului web în timp real. E-mailurile trimise sunt scanate pentru a preveni infectarea altor stații de lucru cu programe periculoase.
- **Lista neagră de aplicații.** Această componentă previne accesul la aplicațiile neautorizate din compania dumneavoastră. Administratorul este responsabil de crearea regulilor pentru aplicații în cadrul organizației.
- **Control acces web.** Această componentă vă protejează de accesarea site-urilor periculoase pe baza unor reguli definite de administrator.
- **Protecție Date.** Această componentă împiedică divulgarea neautorizată a datelor confidențiale pe baza regulilor definite de administrator.
- **Antiphishing.** Această componentă blochează automat paginile web de phishing cunoscute pentru a împiedica utilizatorii să divulge accidental informații private sau confidențiale unor infractori online.
- **Network Attack Defense.** Modulul Network Attack Defense detectează tehnicile de atac în rețea folosite pentru a obține drepturi de acces pe anumite endpoint-uri, cum ar fi atacurile de tip „brute force”, exploit-urile în rețea și furtul de parole.



Notă

Acest modul nu este disponibil pentru Bitdefender Endpoint Security Tools for Windows Legacy.

Firewall

Firewall-ul vă protejează când sunteți conectat la rețele și la Internet prin filtrarea tentativelor de conectare și blocarea conexiunilor suspecte sau riscante.



Notă

Acest modul nu este disponibil pentru Bitdefender Endpoint Security Tools for Windows Legacy.

Control dispozitive

De asemenea, acesta previne scurgerea de informații confidențiale și infecțiile cu programe periculoase prin dispozitivele externe atașate la stațiile de lucru, aplicând reguli de blocare și excepții cu ajutorul politicilor de securitate pentru o gamă largă de dispozitive. Administratorul este responsabil de administrarea drepturilor pentru următoarele tipuri de dispozitive:

- Adaptoare Bluetooth

- Dispozitive CDROM
- Unități dischetă
- IEEE 1284.4
- IEEE 1394
- Dispozitive de imagine
- Modemuri
- Unități cu bandă magnetică
- Windows portabil
- Porturi COM/LPT
- Raid SCSI
- Imprimante
- Adaptoare rețea
- Adaptoare de rețea wireless
- Memorie internă și externă

**Notă**

Acest modul nu este disponibil pentru Bitdefender Endpoint Security Tools for Windows Legacy.

Control Aplicații

Modulul Controlul aplicații blochează aplicațiile neautorizate și procesele care rulează pe stația de lucru. Funcția Control aplicații reduce frecvența și impactul incidentelor malware, reducând suprafața de atac și vulnerabilitățile prin controlarea numărului de aplicații nedorite din rețeaua dumneavoastră.

**Notă**

Acest modul nu este disponibil pentru Bitdefender Endpoint Security Tools for Windows Legacy.

Sandbox Analyzer

Modulul Sandbox Analyzer oferă un strat puternic de protecție împotriva amenințărilor avansate, efectuând analize automate în profunzime asupra fișierelor suspecte care nu sunt încă semnate de motoarele antimalware ale Bitdefender. Sandbox Analyzer utilizează o serie de tehnologii brevetate pentru a executa sarcinile într-un mediu virtual închis, găzduit de Bitdefender, pentru a analiza comportamentul acestora și raporta orice schimbări subtile aduse sistemului, care semnalează intenții periculoase.

**Notă**

Acest modul nu este disponibil pentru Bitdefender Endpoint Security Tools for Windows Legacy.

Criptare volume

Modulul de Criptare a volumelor vă permite să asigurați criptarea integrală a discului prin administrarea BitLocker pe echipamente cu sistem de operare Windows. Puteți cripta și decripta volume boot și non-boot, cu un singur clic, în timp ce GravityZone gestionează întregul proces, cu intervenție minimă din partea utilizatorilor. În plus, GravityZone stochează codurile de recuperare necesare pentru a debloca volumele atunci când utilizatorii își uită parolele.

**Notă**

Acest modul nu este disponibil pentru Bitdefender Endpoint Security Tools for Windows Legacy.

Senzor EDR

Senzorul (Endpoint Detection and Response) colectează, administrează și raportează date referitoare la comportamentul stațiilor de lucru și aplicațiilor. Unele informații sunt prelucrate la nivel local, în timp ce un set mai complex de date sunt raportate către o componentă backend a GravityZone.

Modulul generează o mică amprentă în ceea ce privește utilizarea lățimii de bandă și consumul de resurse hardware.

**Notă**

Acest modul nu este disponibil pentru Bitdefender Endpoint Security Tools for Windows Legacy.

Patch Management

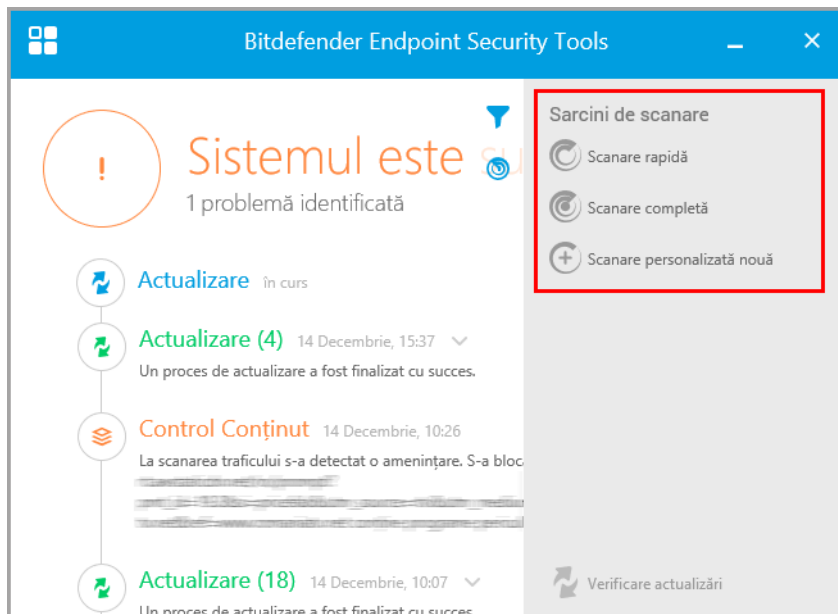
Modulul Patch Management menține sistemul de operare și aplicațiile software actualizate. Acest modul include numeroase funcționalități, cum ar fi scanarea la cerere/programată pentru identificarea patch-urilor disponibile, instalarea manuală/automată a patch-urilor sau raportarea patch-urilor lipsă.

**Notă**

Acest modul nu este disponibil pentru Bitdefender Endpoint Security Tools for Windows Legacy.

1.4. Meniul Acțiuni

Pentru a defini sau executa o sarcină de scanare, faceți clic pe butonul **Acțiuni** pentru a deschide meniul **Acțiuni**. Aici puteți verifica și actualizările disponibile.



Meniul Acțiuni

Scanare Rapidă

Folosește scanarea în cloud pentru detectarea programelor periculoase care rulează în sistemul dumneavoastră. Efectuarea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.

Scanare Sistem

Verifică întregul calculator pentru identificarea tuturor tipurilor de malware care îi amenință siguranța, cum ar fi virusi, spyware, adware, rootkit-uri și altele.

Scanare personalizată

Vă permite să alegeți locațiile pentru scanare și să configurați opțiunile de scanare.



Verificare actualizări

În cazul în care este detectată o actualizare, fie vi se va solicita să confirmați actualizarea, fie aceasta va fi realizată automat, în funcție de setările de actualizare configurate de administratorul de sistem.

2. SCANAREA PENTRU IDENTIFICAREA PROGRAMELOR PERICULOASE

Principalul obiectiv al Bitdefender Endpoint Security Tools este acela de a vă proteja calculatorul contra programelor periculoase. Face acest lucru în primul rând prin scanarea în timp real a fișierelor atașate, mesajelor e-mail și oricăror fișiere noi descărcate sau copiate în calculatorul dumneavoastră. Pe lângă protecția în timp real, permite și efectuarea scanărilor pentru detectarea și ștergerea programelor periculoase din calculatorul dumneavoastră.

Puteți scana computerul oricând doriți prin rularea sarcinilor implicite sau a propriilor sarcini de scanare (sarcini definite de utilizator). Sarcinile de scanare sunt cele care specifică opțiunile de scanare și obiectele care să fie scanate. Dacă doriți să scanați anumite locații de pe computerul dumneavoastră sau să configurați opțiunile de scanare, puteți configura și rula o scanare personalizată.

În orice moment în timpul scanării, puteți vizualiza progresul în cronologia **Evenimente**.

2.1. Scanarea unui fișier sau folder

Trebuie să scanați fișierele și directoarele ori de câte ori considerați că acestea pot fi infectate. Faceți clic dreapta pe fișierul sau directorul care doriți să fie scanat și selectați **Scanează cu Bitdefender Endpoint Security Tools**. Scanarea va începe și veți putea monitoriza progresul în cronologia **Evenimente**.

La sfârșitul scanării, veți putea vedea rezultatul. Pentru informații detaliate, faceți clic pe **Vizualizare jurnal**.

2.2. Rularea unei scanări rapide

Scanare rapidă folosește scanarea în cloud pentru detectarea programelor periculoase care rulează în sistemul dumneavoastră. Rularea unei scanări rapide durează de obicei mai puțin de un minut și utilizează o mică parte din resursele de sistem necesare pentru o scanare antivirus obișnuită.

Funcția **Scanare rapidă** este preconfigurată pentru a permite scanarea următoarelor:

- Procesele în curs, **sectoarele de boot** și regiștrii.
- Regiuni critice de memorie
- Doar fișiere noi sau modificate

- După **rootkituri**, programe **adware**, **spyware** și aplicații dialer în căi critice pentru sistemul de operare, precum: %windir%\system32\, %temp%, /etc, /lib.
- Pentru aplicații potențial nedorite (PUA).

Pentru a executa o scanare rapidă, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender Endpoint Security Tools.
2. Faceți clic pe butonul **Acțiuni** din colțul din dreapta sus.
3. Faceți clic pe **Scanare rapidă**.
4. Așteptați finalizarea procesului de scanare. Puteți vedea evoluția scanării în cronologie. După finalizare, faceți clic pe **Vizualizare jurnal** pentru a vedea rezultatele detaliate.

2.3. Efectuarea unei scanări complete

Sarcina de **Scanare completă** scanează computerul în totalitate pentru a depista toate tipurile de programe periculoase care-i amenință securitatea, cum ar fi viruși, spyware, adware, rootkituri și altele.

i Notă
Deoarece opțiunea de **Scanare completă** efectuează o scanare riguroasă a întregului sistem, aceasta poate dura un timp. În consecință, este recomandat să executați această activitate într-un moment când nu utilizați computerul.

Dacă doriți să scanați anumite locații de pe computer sau pentru a configura opțiunile de scanare, puteți configura și rula o sarcină de scanare personalizată. Pentru mai multe informații, consultați „[Configurarea și executarea unui proces de scanare personalizată](#)” (p. 14).

Înainte de efectuarea unei scanări complete, asigurați-vă că Bitdefender Endpoint Security Tools are semnăturile malware actualizate. Scanarea calculatorului folosind semnături vechi poate împiedica Bitdefender Endpoint Security Tools să detecteze noi aplicații periculoase descoperite după ultima actualizare efectuată. Pentru mai multe informații, consultați „[Actualizări](#)” (p. 24).

Funcția **Scanare completă** este configurată pentru a permite scanarea următoarelor:

- Procesele în curs, **sectoarele de boot** și regiștrii.
- Arhive e-mail și fișiere de rețea de pe toate unitățile, inclusiv cele detașabile.

- După **rootkituri**, programe **adware**, **spyware**, keylogger și aplicații dialer, pe toate unitățile, inclusiv cele detașabile.
- Pentru aplicații potențial nedorite (PUA)
- Fișierele cookie din browser

Pentru a executa o scanare completă, urmați pașii de mai jos:

1. Deschideți fereastra Bitdefender Endpoint Security Tools.
2. Faceți clic pe butonul **Acțiuni** din colțul din dreapta sus.
3. Dați clic pe **Scanare completă**.
4. Așteptați finalizarea procesului de scanare. Puteți vedea evoluția scanării în cronologie. Dați clic pe **Vizualizare detalii** pentru a vedea detaliile scanării în curs. De asemenea, puteți pune scanarea pe pauză, o puteți amâna sau opri.
5. Bitdefender Endpoint Security Tools va întreprinde automat acțiunile recomandate asupra fișierelor detectate. După finalizare, faceți clic pe **Vizualizare jurnal** pentru a vedea rezultatele detaliate.

2.4. Configurarea și executarea unui proces de scanare personalizat

Pentru a configura o scanare antimalware în detaliu și pentru a o lansa, urmați pașii de mai jos:

1. Deschideți fereastra principală Bitdefender Endpoint Security Tools.
2. Faceți clic pe butonul **Acțiuni** din colțul din dreapta sus.
3. Faceți clic pe **Scanare personalizată nouă**. Fereastra **Scanare personalizată** se va deschide.
4. Configurați opțiunile de scanare: **Agresiv**, **Normal**, **Permisiv**, **Personalizat**. Utilizați opțiunea de mai jos pentru a identifica nivelul de scanare care se potrivește mai bine nevoilor dumneavoastră.
5. Selectați ținta scanării din secțiunea din stânga.
6. De asemenea, puteți configura scanarea astfel încât să execute sarcina cu prioritate scăzută bifând caseta corespunzătoare. Aceasta reduce prioritatea procesului de scanare. Veți permite altor programe să ruleze cu o viteză superioară, dar timpul necesar pentru finalizarea scanării va crește.

După configurarea sarcinii de scanare personalizată, o puteți salva ca favorită. Pentru a face acest lucru, introduceți o denumire și faceți clic pe butonul **Favorit**

Utilizatorii avansați ar putea profita de setările de scanare pe care le oferă Bitdefender Endpoint Security Tools. Pentru configurarea detaliată a opțiunilor de scanare, faceți clic pe **Personalizare** și apoi **Setări**.

În mod alternativ, puteți configura și executa o sarcină personalizată folosind utilitarul de tip linie de comandă al produsului. Pentru detalii, consultați capitoulul „[Utilizarea interfeței cu linie de comandă](#)” (p. 28).

2.4.1. Tipuri de fișiere

În fila **Tipuri de fișiere**, precizat tipurile de fișiere pe care doriți să le scanați. Puteți seta agentul de securitate să scaneze toate fișierele (indiferent de extensie), fișierele de aplicație sau extensiile specifice de fișiere pe care le considerați periculoase.

Scanarea tuturor fișierelor asigură cea mai bună protecție în timp ce scanarea aplicațiilor poate fi utilizată pentru efectuarea unei scanări mai rapide. Aplicațiile (sau fișierele de program) sunt mult mai vulnerabile la atacurile malware decât alte tipuri de fișiere. Această categorie include următoarele extensii de fișiere:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf;

xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xism; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

Opțiuni de scanare a arhivelor

Arhivele ce conțin fișiere infectate nu reprezintă o amenințare imediată la adresa securității sistemului dumneavoastră. Codurile periculoase (malware) vă pot afecta sistemul numai dacă fișierul infectat este extras din arhivă și este executat fără a avea activată protecția în timp real. Cu toate acestea, se recomandă să utilizați această opțiune pentru a detecta și elimina orice amenințare potențială chiar dacă nu este o amenințare imediată.

Scanare arhive de e-mail

Selectați această opțiune dacă doriți să activați scanarea fișierelor atașate la mesajele e-mail și bazele de date e-mail, inclusiv format de fișiere de tipul .eml, .msg, .pst, .dbx, .mbx, .tbb și altele.

2.4.2. Ce se scanează?

În fila **Scanare**, bifați casetele corespunzătoare pentru a activa opțiunile de scanare dorite.

Scanare sectoare de boot

Puteți seta Bitdefender Endpoint Security Tools să scaneze sectoarele de boot ale hard-diskului. Acest sector al hard disk-ului conține codul de computer necesar pentru a iniția procesul de boot. Atunci când un virus infectează sectorul de boot, partiția poate deveni inaccesibilă și există posibilitatea să nu puteți porni sistemul și accesa datele.

Scanează după rootkituri

Selectați această opțiune pentru a lansa procesul de scanare pentru identificarea **rootkit-urilor** și a obiectelor ascunse, cu ajutorul acestui software.

Scanează memoria

Selectați această opțiune pentru a scana programele ce rulează în memoria sistemului dumneavoastră.

Scanează regiștrii

Selectați această opțiune pentru a scana cheile de regiștri. Regiștrii Windows sunt o bază de date care stochează setările de configurare și opțiunile pentru componentele sistemului de operare Windows, precum și pentru aplicațiile instalate.

Scanare după keyloggers

Selectați această opțiune pentru a scana software-urile de tip **keylogger**.

Scanare pentru aplicații potențial nedorite (PUA)

O aplicație potențial nedorită (PUA) este un program care ar putea fi nedorit pe PC, care uneori vine la pachet cu software-ul freeware. Astfel de programe pot fi instalate fără consimțământul utilizatorului (numite și adware), sau vor fi incluse în mod implicit în kit-ul de instalare în mod expres (ad-supported). Efectele potențiale ale acestor programe includ afișarea de pop-up-uri, instalarea de bare de instrumente nedorite în browser-ul implicit sau rularea mai multor procese în fundal și încetinirea performanței PC-ului.

Scanează doar fișierele noi și cele modificate

Prin scanarea exclusivă a fișierelor noi și a celor modificate, puteți îmbunătăți considerabil performanța sistemului cu un risc minim pentru securitatea acestuia.

Scanează fișiere cookie

Selectați această opțiune pentru a scana fișierele de tip cookie stocate de browsere pe computerul dumneavoastră.

2.4.3. Ce trebuie făcut?

În tab-ul **Acțiuni**, setați acțiunea ce va fi întreprinsă asupra fișierelor detectate, dacă există.

Fișiere infectate

Fișierele detectate ca fiind infectate se potrivesc unei semnături malware din baza de date a Bitdefender.

Fișiere suspecte

Fișierele sunt identificate ca fiind suspecte în urma analizei euristice. Fișierele suspecte nu pot fi dezinfectate deoarece nu este disponibilă nicio metodă de dezinfectare.

Rootkit-uri

Rootkit-urile reprezintă aplicații specializate utilizate pentru ascunderea fișierelor de sistemul de operare. Deși nu sunt periculoase, rootkit-urile sunt adesea utilizate pentru ascunderea programelor periculoase sau pentru a disimula prezența unui intrus în sistem.

Aplică acțiunile optime

În funcție de tipul fișierelor detectate, sunt disponibile una sau mai multe dintre următoarele opțiuni:

Ștergere

Îndepărtează fișierele identificate ca fiind infectate de pe disc.

Dacă într-o arhivă sunt stocate fișiere infectate împreună cu fișiere curate, Bitdefender Endpoint Security Tools ca încerca să șteargă fișierele infectate și să refacă arhiva incluzând doar fișierele curate. Dacă reconstrucția arhivei nu este posibilă, veți fi notificat de faptul că nu poate fi aplicată nicio acțiune astfel încât să se evite pierderea fișierelor curate.

Ignoră

Nu se va lua nicio acțiune asupra fișierelor detectate. După finalizarea scanării, puteți deschide raportul de scanare pentru a vedea informații despre aceste fișiere.

Mută fișierele în carantină

Fișierele aflate în carantină nu pot fi executate sau deschise; ca urmare, dispare riscul de a fi infectat.

Dezinfectează

Șterge codul malware din fișierele infectate și reconstruiește fișierul original.

2.5. Examinarea rapoartelor de scanare

De fiecare dată când realizați o scanare, se creează un raport de scanare. Raportul de scanare conține informații detaliate despre procesul de scanare înregistrat, cum ar fi opțiunile de scanare, locațiile scanate, amenințările găsite și acțiunile luate asupra acestor amenințări.

Puteți deschide raportul de scanare direct din fereastra principală, după ce scanarea a luat sfârșit, apăsând **Vizualizare jurnal**.

Pentru a verifica jurnalele de scanare ulterior, urmați pașii de mai jos:

1. Deschideți fereastra principală Bitdefender Endpoint Security Tools.
2. Faceți clic pe butonul **Filtrare** pentru a deschide meniul **Filtre**.
3. Faceți clic pe butonul **Antimalware**. Aici puteți găsi toate evenimentele de scanare, inclusiv amenințările detectate prin scanarea la accesare, scanările recente, prin scanarea inițiată de utilizator, precum și modificările de stare rezultate de scanările automate.



4. Faceți clic pe un eveniment pentru a vizualiza detaliile acestuia.
5. Pentru a deschide un jurnal de scanare, faceți clic pe **Vizualizare jurnal**. Se va afișa jurnalul de scanare.

3. UTILIZAREA CRIPTĂRII DE VOLUM

Modulul Criptare de volum vă oferă opțiunea de criptare de tip „Full Disk Encryption” pe sistemul dumneavoastră Windows prin intermediul unor politici aplicate de administratorul care se ocupă de securitate.

3.1. Criptarea sistemului

Atunci când se aplică o politică de criptare pe sistemul dumneavoastră Windows:

1. Va apărea o fereastră de configurare prin care vi se va solicita să introduceți:

- Un cod de identificare personală (PIN) dacă sistemul este prevăzut cu cip TPM (Trusted Platform Module) (precum laptopurile mai noi).



Notă

Dacă sistemul dumneavoastră are un TPM funcțional, administratorul care se ocupă de securitate poate configura o politică ce criptează automat volumele, fără a solicita codul PIN.

- O parolă dacă sistemul nu are cip TPM (Trusted Platform Module). Parola este necesară și atunci când cipul TPM nu funcționează sau nu este detectat de Bitdefender Endpoint Security Tools.

Criptare volum

Setare parolă de criptare

Configurați o parolă cu caractere EN-US. Veți avea nevoie de aceasta pentru a porni sistemul de operare sau pentru a debloca volumul.

Criptarea este un proces care are loc o singură dată și vă puteți continua activitatea ca de obicei.

Introduceți parola de criptare pentru volumul C:. Veți avea nevoie de această parolă pentru a debloca volumul.

Alegeți parola:

Confirmați parola:

Cerințe privind parola:

- Are cel puțin 8 caractere
- Trebuie să conțină litere mici și mari
- Trebuie să conțină un număr

[Închide](#)

2. Faceți clic pe butonul **Salvează**. Procesul de criptare începe imediat, mai întâi pe volumul de boot.

Puteți anula criptarea selectând **Anulare**. Cu toate acestea, fereastra va apărea din nou după o vreme, solicitându-vă să configurați un cod PIN sau o parolă de criptare.

Aveți nevoie de un singur PIN sau o singură parolă pentru a cripta toate volumele, boot și non-boot, pe discuri fixe, pe sisteme desktop și laptopuri. Discurile amovibile nu se criptează. Pentru detalii despre configurarea codului PIN sau a parolei de criptare, consultați [acest articol KB](#).

După criptare, este posibil să fie necesar să introduceți codul PIN sau parola într-un ecran de autentificare pre-boot la fiecare pornire a sistemului Windows, în funcție de politica de securitate care se aplică în cazul sistemului dumneavoastră.



Dacă ați uitat codul de criptare sau parola, contactați administratorul care se ocupă de securitate.

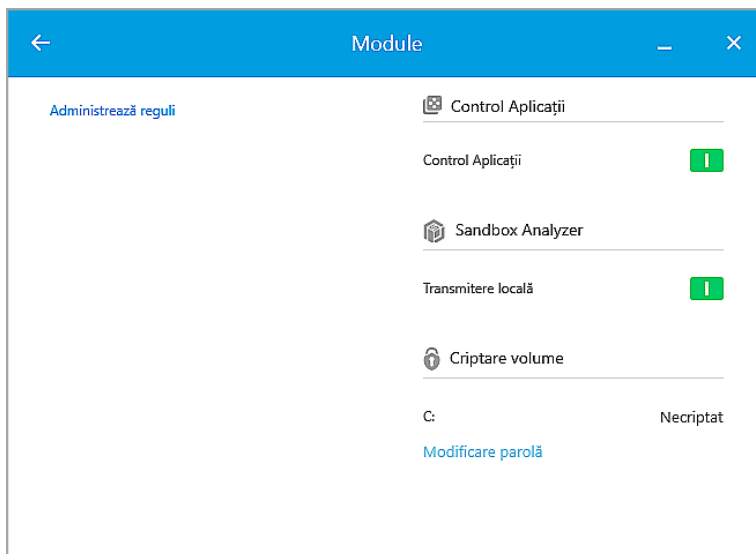
3.2. Decriptarea sistemului

Atunci când se aplică o politică de decriptare, discurile criptate sunt decriptate automat, fără să necesite intervenția dumneavoastră. Cu toate acestea, nu puteți decripta manual sistemul, atâta timp cât este activă o politică de criptare.

3.3. Verificarea stării de criptare

Iată cum puteți verifica starea de criptare pe sistemul dumneavoastră:

1. În bara de sistem, faceți dublu clic pe pictograma  pentru a accesa interfața Bitdefender Endpoint Security Tools.
2. În colțul din dreapta sus, selectați butonul  pentru a deschide fereastra **Module**.
3. Accesați secțiunea **Criptare de volum**, unde puteți vedea care dintre volume sunt criptate și care nu.



3.4. Modificarea codului PIN sau a parolei de criptare

Iată cum puteți modifica codul PIN sau parola de criptare:

1. Din fereastra principală a interfeței Bitdefender Endpoint Security Tools, clic pe numele unității de disc criptate.
2. Selectați opțiunea **Modificare parolă**.
3. În fereastra de configurare, introduceți noul cod PIN sau noua parolă.
4. Faceți clic pe butonul **Salvează**.

4. ACTUALIZĂRI

Într-o lume în care infractorii cibernetici încearcă permanent să descopere noi metode de a acționa, este esențial să vă mențineți la zi programul de securitate pentru a fi mereu cu un pas înaintea acestora.

Dacă sunteți conectat la Internet, prin bandă largă sau ADSL, Bitdefender Endpoint Security Tools se ocupă singur de actualizări. În mod implicit, acesta caută actualizări la pornirea sistemului, precum și după fiecare **oră**.

Notă

Frecvența de actualizare automată poate fi modificată de administratorul dumneavoastră de rețea.

Procesul de actualizare este realizat progresiv, ceea ce înseamnă că fișierele care trebuie actualizate sunt înlocuite unul câte unul. Astfel, procesul de actualizare nu va afecta funcționarea produsului și, în același timp, orice vulnerabilitate va fi exclusă.

Dacă vă conectați la Internet prin dial-up, atunci este recomandat să actualizați manual Bitdefender în mod regulat. Pentru mai multe informații, consultați [„Efectuarea unei actualizări”](#) (p. 25).

4.1. Tipuri de actualizări

Actualizările sunt de mai multe tipuri:

- **Actualizările semnăturilor malware** - pe măsură ce apar amenințări noi, fișierele cu semnături malware trebuie actualizate pentru a asigura protecția la zi împotriva acestora.
- **Actualizări de produs** - la lansarea unei noi versiuni, sunt introduse noi funcții și tehnici de scanare pentru a îmbunătăți performanțele produsului.

Un upgrade de produs reprezintă lansarea unei noi versiuni.

4.2. Cum verificați dacă protecția este la zi

Pentru a verifica dacă protecția oferită de produsul dumneavoastră este la zi, urmați pașii de mai jos:

1. Faceți clic dreapta pe pictograma Bitdefender Endpoint Security Tools în bara de sistem și selectați **Despre**.

2. Puteți vedea informații despre starea actualizării și momentul ultimei actualizări.

Pentru mai multe informații despre cele mai recente actualizări, verificați evenimentele privind actualizările:

1. În fereastra principală, faceți clic pe butonul **Filtrare** pentru a deschide meniul **Filtre**.
2. Efectuați clic pe butonul **Update**. Cele mai recente actualizări vor fi afișate în cronologia **Evenimente**.

Puteți vedea când anume au fost inițiate actualizări, precum și informații despre acestea, dacă au fost finalizate cu succes, dacă este necesară o repornire pentru a finaliza instalarea. Dacă este necesar, reporniți sistemul cât mai curând posibil.

4.3. Efectuarea unei actualizări

Pentru efectuarea actualizărilor este necesară existența unei conexiuni la internet.

Pentru a porni o actualizare:

- Faceți dublu clic pe pictograma Bitdefender Endpoint Security Tools din [bara de sistem](#).
- Faceți clic pe butonul **Acțiuni** pentru a deschide meniul **Acțiuni**.
- Faceți clic pe **Verificare actualizări**. Modulul Actualizare se va conecta la serverul de actualizare al Bitdefender și va căuta noi actualizări.
- În cazul în care este detectată o actualizare, fie vi se va solicita să confirmați actualizarea, fie aceasta va fi realizată automat, în funcție de setările de actualizare configurate de administratorul de sistem.



Important

Dacă este necesar, reporniți sistemul cât mai curând posibil. Vă recomandăm să faceți acest lucru cât mai repede cu putință.




5. EVENIMENTE

Bitdefender Endpoint Security Tools afișează un jurnal detaliat al evenimentelor referitoare la activitatea sa pe computer dvs., inclusiv activitățile calculatorului monitorizate de Content Control și aplicațiile blocate de modulul Control Aplicații. Cronologia **Evenimente** reprezintă un instrument foarte important pentru monitorizarea protecției Bitdefender. De exemplu, puteți verifica rapid dacă produsul a fost actualizat, dacă au fost detectate coduri sau aplicații periculoase pe calculatorul dumneavoastră etc. Pentru a consulta jurnalul de evenimente, urmați pașii de mai jos:

1. Deschideți fereastra principală Bitdefender Endpoint Security Tools.
2. Toate evenimentele sunt afișate în cronologia **Evenimente**.
3. Faceți clic pe butonul **Filtrare** pentru a deschide meniul **Filtre**.
4. Selectați categoria de eveniment din meniu. Evenimentele sunt grupate în următoarele categorii:
 - **Setări generale**
 - **Antimalware**
 - **Firewall**
 - **Actualizare**
 - **Control Conținut**
 - **Control dispozitive**
 - **Control Aplicații**
 - **Sandbox Analyzer**
 - **Criptare volume**

Fiecare eveniment este însoțit de următoarele informații: o scurtă descriere, acțiunea aplicată de Bitdefender în momentul producerii evenimentului și data și ora producerii acestuia. Pentru a vedea informații detaliate cu privire la un anumit eveniment din listă, faceți clic pe **Vizualizare jurnal**.

De asemenea, puteți filtra evenimentele după importanța lor pentru nivelul de protecție. Există trei tipuri de evenimente:

-  indică operațiunile reușite.
-  indică probleme non-critice.
-  indică probleme critice.



Unele probleme critice și non-critice afișate în cronologia **Evenimente** sunt asociate cu acțiunile recomandate pentru remedierea lor.

6. UTILIZAREA INTERFEȚEI CU LINIE DE COMANDĂ

Bitdefender Endpoint Security Tools vă permite să executați automat sarcini de scanare și actualizări la cerere folosind consola produsului, o interfață cu linie de comandă care se regăsește în directorul de instalare al produsului de pe mașinile dumneavoastră Windows.

Interfața cu linie de comandă BEST are două moduri de lucru:

- **Comenzi multiple simultan.** Acest mod utilizează interfața cu linie de comandă proprie și vă permite să introduceți comenzi și să primiți rezultate până la ieșirea din acest mod.

Pentru a accesa acest mod:

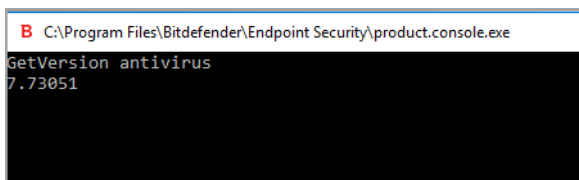
1. Accesați `c:\Program Files\Bitdefender\Endpoint Security` sau directorul unde a fost instalat BEST.
2. Găsiți și efectuați dublu clic pe executabilul **product.console**. Se deschide interfața cu linie de comandă.
3. Executați comanda dorită.

Exemplu:

```
GetVersion antivirus
```

Rezultatul generat reprezintă numărul versiunii semnăturilor antimalware.

4. Executați comanda `exit` pentru a închide interfața cu linie de comandă.



```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion antivirus
7.73051
```

- **O singură comandă simultan.** Acest mod utilizează Command Prompt și revine la interfața de comandă a sistemului după ce este executată comanda.

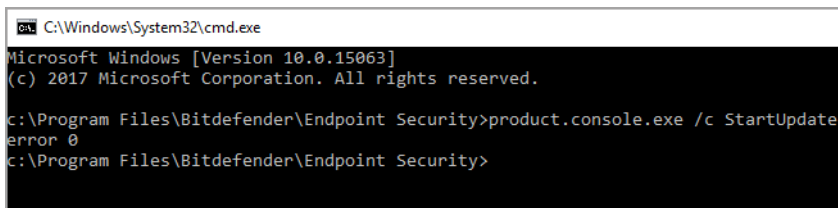
Pentru a accesa acest mod:

1. Deschideți Command Prompt (cmd.exe).
2. Utilizați comanda cd pentru a naviga la directorul de instalare Bitdefender Endpoint Security Tools.
3. Executați comanda dorită.

Exemplu:

```
C:\Program Files\Bitdefender\Endpoint Security>
product.console.exe /c StartUpdate
```

4. Dacă comanda este executată cu succes, rezultatul generat este error 0.



```
cmd C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

c:\Program Files\Bitdefender\Endpoint Security>product.console.exe /c StartUpdate
error 0
c:\Program Files\Bitdefender\Endpoint Security>
```

6.1. Comenzi acceptate

Interfața cu linie de comandă acceptă mai multe comenzi, unele dintre acestea necesită anumiți parametri pentru a genera rezultate valide.

Toate exemplele din această secțiune sunt date folosind Consola produsului din directorul de instalare BEST.

GetUpdateStatus product|antivirus

Extrageți informațiile despre ultima(ele) actualizare(ări).

Această comandă necesită unul dintre următorii parametri:

- product – se referă la versiunea BEST.
- antivirus – se referă la versiunea semnăturilor antimalware.

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetUpdateStatus product
lastSucceededTime: 1504513705
lastAttemptedTime: 1504513705
lastError: 0
GetUpdateStatus antivirus
lastSucceededTime: 1505739144
lastAttemptedTime: 1505739144
lastError: 0
```

GetVersion product|antivirus

Extrage informațiile despre versiunea actuală a produsului.

Această comandă necesită unul dintre următorii parametri:

- **product** – se referă la versiunea BEST.
- **antivirus** – se referă la versiunea semnăturilor antimalware.

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion product
6.2.24.938
GetVersion antivirus
7.73205
```

IsUpdateInProgress

Verificați dacă o actualizare a produsului este în curs de desfășurare.

Valori generate:

- **true** - o actualizare a produsului este în curs de desfășurare.
- **false** - nicio actualizare a produsului nu este în curs de desfășurare.

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateInProgress
false
```

IsUpdateRestartNeeded

Verifică dacă mașina necesită o repornire a sistemului după efectuarea actualizării.

Valori generate:

- true - mașina necesită o repornire a sistemului după efectuarea actualizării.
- false - mașina nu necesită o repornire a sistemului după efectuarea actualizării.

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateRestartNeeded
false
```

StartUpdate

Pornește o actualizare și generează rezultatul fără a aștepta finalizarea sarcinii.

Exemplu:

```
StartUpdate
```

Format generat: error 0 (comanda a fost executată cu succes)

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
StartUpdate
error 0
```

FileScan.OnDemand.RunScanTask custom [option]

Pornește o sarcină de scanare la cerere și afișează calea către jurnalul de scanare și rezumatul scanării.

Această comandă necesită parametrul `custom`, urmat, dacă este cazul, de una sau mai multe opțiuni. De exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-1505742554_1_01.xml
Scanned items: 990886
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

Cu ajutorul opțiunilor, puteți personaliza o sarcină de scanare. Aceste opțiuni nu sunt obligatorii.

Fiecare opțiune are două sau mai multe valori disponibile, însă puteți utiliza o singură valoare.

Atunci când comanda `FileScan.OnDemand.RunScanTask` nu specifică nicio opțiune, sarcina personalizată ia în considerare valoarea implicită a opțiunii respective. De exemplu, dacă executați această comandă fără a menționa opțiunea `scanKeyloggers`, aceasta înseamnă că Bitdefender Endpoint Security Tools va efectua în continuare o scanare pentru identificarea programelor keylogger, conform valorii implicite pentru `scanKeyloggers` (`true`).



Notă

Nu există comenzi specifice pentru **Scanare rapidă** sau **Scanare completă**. Cu toate acestea, puteți configura `FileScan.OnDemand.RunScanTask` pentru

a scana fie numai locația sistemului de operare sau întregul sistem, cu toate opțiunile activate, după cum este necesar.

Opțiuni

`path="<path>"`

Introduceți calea locației vizate pentru scanare. Pentru a specifica mai multe căi, utilizați: `path="<path1>" path="<path2>"`.

Exemplu:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
```

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505746495_1_01.xml
Scanned items: 74074
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`infectedAction1=ignore|disinfect|disinfectOnly|delete|quarantine`

Selectați prima acțiune ce trebuie aplicată atunci când se detectează un fișier infectat: ignorare, dezinfectare, ștergere sau mutare în carantină. Puteți utiliza această acțiune împreună cu `infectedAction2`.

Valoarea implicită: `disinfect`

Exemplu:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" infectedAction1=ignore
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505813252_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`infectedAction2=ignore|disinfect|disinfectOnly|delete|quarantine`

Selectați cea de-a doua acțiune ce trebuie aplicată atunci când se detectează un fișier infectat, dacă prima acțiune eșuează.

Valoarea implicită: `quarantine`

Exemplu:

```
FileScan.OnDemand.RunScanTask custom infectedAction1=disinfect infectedAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505824102_1_01.xml
Scanned items: 500139
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

suspiciousAction1=ignore|delete|quarantine

Selectați prima acțiune ce trebuie aplicată atunci când se detectează un fișier suspect. Puteți utiliza această acțiune împreună cu suspiciousAction2.

Valoarea implicită: ignore

Exemplu:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" suspiciousAction1=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505824920_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

suspiciousAction2=ignore|delete|quarantine

Selectați cea de-a doua acțiune ce trebuie aplicată atunci când se detectează un fișier suspect, dacă prima acțiune eșuează.

Valoarea implicită: ignore

Exemplu:

```
FileScan.OnDemand.RunScanTask custom path="C:\Users" suspiciousAction1=delete suspiciousAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505825170_1_01.xml
Scanned items: 54455
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanBootSectors=true|false

Scanați sectoarele de boot ale hard disk-ului.

Valoarea implicită: false

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanBootSectors=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073447_1_01.xml
Scanned items: 416206
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRegistry=true | false

Scanați cheile de regiștri de pe mașina dumneavoastră.

Valoarea implicită: false

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRegistry=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073099_1_01.xml
Scanned items: 419060
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanMemory=true | false

Scanați programele care rulează în memoria sistemului dumneavoastră.

Valoarea implicită: false

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanMemory=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506072517_1_01.xml
Scanned items: 427016
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom scanMemory=true
```

smartScan=true | false

Scanați doar fișierele noi și cele modificate.

Valoarea implicită: true

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom smartScan=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506070911_1_01.xml
Scanned items: 1614889
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRootKits=true | false

Scanați pentru identificarea rootkit-urilor și a obiectelor ascunse folosind un astfel de software.

Valoarea implicită: false

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRootKits=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506070601_1_01.xml
Scanned items: 416548
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanKeyloggers=true | false

Scanați pentru identificarea programelor keylogger

Valoarea implicită: true

Exemplu:

```
FileScan.OnDemand.RunScanTask custom scanKeyloggers=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanPUA=true | false

Scanați pentru identificarea aplicațiilor potențial nedorite (PUA).

Valoarea implicită: false

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanPUA=true
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanArchives=true | false

Scanați pentru identificarea fișierelor infectate din interiorul arhivelor.

Valoarea implicită: true

Exemplu:

```
FileScan.OnDemand.RunScanTask custom scanArchives=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

extensionType=all | application | custom | none

Scanați fișierele în funcție de extensia lor: toate fișierele, numai fișierele executabile, numai fișierele cu extensiile dorite sau nu scanați niciun fișier.

Valoarea implicită: all

Exemplu:

```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom extensionType=application
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`customExt="<string>"`

Această opțiune vă permite să scanați numai fișierele cu extensiile dorite. Necesită un șir în cadrul căruia fiecare extensie este încadrată de bare verticale (de ex., " | exe | ini | txt | "). Această opțiune este valabilă numai împreună cu opțiunea `extensionType=custom`.

Exemplu:

```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom path="c:\Program Files\WinRAR" extensionType=custom customExt="|dll|"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506351027_1_01.xml
Scanned items: 6
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom path="c:\Program Files\WinRAR" extensionType=custom customExt="|dll|dat|"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0-0\1506351335_1_01.xml
Scanned items: 8
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`lowPriority=true|false`

Rulați sarcina cu prioritate scăzută.

Valoarea implicită: `false`

Exemplu:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe  
FileScan.OnDemand.RunScanTask custom lowPriority=true
```

Aceste opțiuni reprezintă o alternativă la opțiunile disponibile în consola BEST. Pentru mai multe informații consultați capitolul „Configurarea și executarea unui proces de scanare personalizat” (p. 14).

6.2. Coduri de eroare aferente liniei de comandă

Utilitarul cu linie de comandă poate genera următoarele coduri de eroare:

Cod de eroare	Descriere
0	Comanda a fost executată cu succes.
87	Parametru incorect.
160	Argumente incorecte.
1627	Executare nereușită a funcției - a apărut o eroare la executarea comenzii.

7. OBȚINERE AJUTOR

Pentru orice probleme sau întrebări referitoare la Bitdefender Endpoint Security Tools, vă rugăm să contactați administratorul de rețea.

Pentru a găsi un produs și informațiile de contact, faceți clic dreapta pe pictograma Bitdefender Endpoint Security Tools din bara de sistem și selectați **Despre** pentru a deschide fereastra **Despre**.

Vocabular

Actualizare

O versiune nouă de produs hardware sau software proiectat să înlocuiască o versiune mai veche a aceluiași produs. În afară de acesta, rutinele de instalare verifică dacă există instalată pe calculatorul dumneavoastră o altă versiune mai veche; dacă nu, nu puteți instala actualizarea.

Bitdefender dispune de modulul său propriu care realizează actualizarea automată sau manuală.

adware

Aplicația adware este adesea combinată cu o aplicație gazdă care este oferită gratuit dacă utilizatorul acceptă aplicația adware. Deoarece aplicațiile adware sunt de obicei instalate după ce utilizatorul a fost de acord în prealabil cu un contract de licențiere care explică scopul aplicației, nu este comisă nicio infracțiune.

Totuși, reclamele de tip pop-up pot fi supărătoare, iar în unele cazuri pot afecta performanțele sistemului. De asemenea, informațiile pe care unele dintre aceste aplicații le adună pot cauza motive de îngrijorare utilizatorilor care nu cunosc în întregime termenii din contractul de licențiere.

Aplicație de descărcare Windows

Este un nume generic pentru un program a cărui funcție principală este descărcarea de conținut pentru activități nedorite sau periculoase.

Arhivă

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.

Atacuri targetate

Atacuri cibernetice care vizează în principal avantaje financiare sau denigrarea reputației. Ținta poate fi un individ, o companie, un software sau un sistem, toate studiate în detaliu înainte de lansarea atacului. Aceste atacuri se derulează pe perioade mai lungi de timp și în etape, folosind mai multe puncte de infiltrare. Sunt observate rar, de cele mai multe ori doar după ce daunele au fost deja făcute.

Backdoor

Reprezintă o breșă de securitate realizată în mod deliberat. Motivația acestor "găuri" nu este întotdeauna malițioasă: unele sisteme de operare, de exemplu, sunt puse în circulație cu conturi privilegiate pentru tehnicienii din service sau de responsabili cu mentenanța produsului din partea producătorului.

Bara de sistem

Introdusă odată cu apariția sistemului Windows 95, bara de sistem este plasată 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 legate 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.

Bootkit

Un bootkit este un program periculos care are capacitatea de a infecta sectoarele de date Master Boot Record (MBR), Volume Boot Record (VBR) sau boot. Bootkit-ul rămâne activ chiar și după repornirea sistemului.

Browser

Este prescurtarea de la Web Browser, o aplicație utilizată pentru a localiza și încărca pagini de Web.

Cookie

În domeniul Internetului, cookie-urile reprezintă mici fișiere ce conțin informații despre fiecare calculator care pot fi analizate și folosite de către cei care publică reclame pentru a vă urmări interesele și preferințele online. În acest domeniu, tehnologia cookie-urilor este în curs de dezvoltare, iar intenția este de a afișa direct acele anunțuri care corespund intereselor dumneavoastră. Această facilitare are avantaje și dezavantaje pentru mulți deoarece, pe de o parte, este eficientă și pertinentă din moment ce vizualizați doar acele anunțuri despre subiecte care vă interesează. Pe de altă parte, cookie-urile implică de fapt o "monitorizare" și "urmărire" a site-urilor vizitate și a link-urilor accesate. Astfel, în mod logic, părerile sunt împărțite în ceea ce privește confidențialitatea și mulți se simt jigniți de faptul că sunt văzuți ca un simplu "număr SKU" (este vorba de codul de bare de pe spatele ambalajelor care este scanat pe bandă la supermarket). Deși acest punct de vedere poate fi considerat extrem, în anumite cazuri el reprezintă chiar ceea ce se întâmplă în realitate.

Evenimente

O acțiune sau întâmplare detectată de un program. Evenimentele pot fi acțiuni ale utilizatorului, cum ar fi executarea unui clic cu mouse-ul sau apăsarea unei taste, sau întâmplări în sistem cum ar fi epuizarea memoriei.

Extensie de fișier

Reprezintă porțiunea dintr-un nume de fișier ce urmează după caracterul punct, și care indică tipul de date pe care le stochează fișierul.

Multe sisteme de operare, cum ar fi Unix, VMS, and MS-DOS, utilizează extensii de fișiere. De obicei aceasta este formată din una până la trei litere (unele sisteme de operare mai vechi nu suportă mai mult de trei). De exemplu: "c" pentru fișierele sursă scrise în limbajul C, "ps" pentru fișiere PostScript sau "txt" pentru fișierele text oarecare.

Fals pozitiv

Apare atunci când un analizator detectează un fișier ca fiind infectat când de fapt acesta nu este infectat.

Fișier de 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.

Fișiere suspecte și trafic în rețea suspect

Fișierele suspecte sunt cele cu reputație îndoielnică. Această caracteristică este dată de numeroși factori, printre care se numără: existența semnăturii digitale, numărul de apariții în rețelele de calculatoare, packerul utilizat etc. Traficul de rețea este considerat suspect dacă se abate de la model. De exemplu, surse nesigure, solicitări de conexiune la porturi neobișnuite, creșterea lățimii de bandă utilizate, timpi aleatorii de conectare etc.

Furtună de scanare antimalware

O utilizare intensivă a resurselor de sistem care intervine atunci când software-ul antivirus scanează simultan mai multe mașini virtuale pe o singură gazdă fizică.

Grayware

O clasă de aplicații software între software legitim și malware. Deși nu sunt la fel de periculoase ca programele malware care afectează integritatea sistemului, comportamentul lor este totuși deranjant, conducând la situații nedorite cum ar fi furtul de date și utilizarea neautorizată, publicitatea nedorită. Cele mai des întâlnite aplicații grayware sunt [spyware](#) și [adware](#).

Hoț de parole

Un password stealer colectează date care pot fi nume de conturi și parole asociate. Aceste date de autentificare furate sunt utilizate apoi pentru activități periculoase, precum furtul de cont.

IP

Internet Protocol - Un protocol rutabil din suita protocoalelor TCP / IP căruia i se atribuie adresarea IP, rutarea, fragmentarea cât și reasamblarea pachetelor IP.

Keylogger

Un keylogger este o aplicație care înregistrează orice tastați.

Keyloggererele nu au o natură periculoasă. Pot fi folosite în scopuri legitime, cum ar fi monitorizarea activității angajaților sau a companiilor subordonate. Cu toate acestea, utilizarea lor de către infractorii cibernetici în scopuri negative este din ce în ce mai răspândită (de exemplu, pentru colectarea informațiilor cu caracter privat, cum ar fi acreditările de înregistrare și codurile numerice personale).

Linie de comandă

Într-o interfață cu linie de comandă, utilizatorul scrie comenzile în spațiul prevăzut direct pe ecran utilizând limbajul de comandă.

Malware

Malware este termenul generic pentru software-ul care este proiectat pentru a face rău - o contracție a "malicious software". Acesta nu este încă în uz universal, dar popularitatea sa ca un termen general pentru viruși, cai troieni, viermi, și coduri malware mobile este în creștere.

Metoda euristică

Reprezintă o metodă bazată pe anumite reguli pentru identificarea de viruși noi. Această metodă de scanare nu se bazează pe semnături de viruși

cunoscuți. Avantajul metodei euristice e dat de faptul că nu poate fi păcălită de o nouă variantă a unui virus deja existent. Totuși ocazional poate raporta un cod suspicios în programe normale, generând așa-numitul "fals pozitiv".

Metoda ne-euristică

Această metodă de scanare se bazează pe semnături de viruși cunoscuți. Avantajul metodelor ne-euristice constă în aceea că scannerul nu poate fi "păcălit" de ceea ce poate părea un virus și din acest motiv nu generează fals pozitiv.

Phishing

Reprezintă acțiunea de a trimite un e-mail către un utilizator, pretinzând a fi o companie legitimă, în încercarea de a păcăli utilizatorul să furnizeze informații confidențiale ce vor fi folosite la furtul identității. E-mailul îndreaptă utilizatorul către un site Web unde acesta este rugat să actualizeze informații personale, cum ar fi parole și numere de card de credit, de asigurări sociale și de conturi bancare pe care compania respectivă deja le are. Site-ul Web este însă fals și folosit pentru a fura informațiile despre utilizator.

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 punct terminus al unei conexiuni logice. Numărul portului identifică ce tip de port este. De exemplu, portul 80 este utilizat pentru traficul HTTP.

Ransomware

Un program malware care vă blochează accesul la calculator sau la fișiere și aplicații. Programele ransomware vă solicită să achitați o anumită sumă (răscumpărare) în schimbul unui cod de decriptare care vă permite să redobândiți accesul la calculatoarele sau fișierele dvs.

Rootkit

Un rootkit este un set de unelte 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 unelte 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, loginuri și jurnale. Acestea pot de asemenea să intercepteze date de la terminale, conexiuni la rețea sau perifice 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 aplicații malițioase sau prezența intrușilor în sistem. În combinație cu aplicații malițioase, 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.

Sector de boot:

Un sector la începutul fiecărui disc care identifică arhitectura discului (mărimea sectorului, mărimea clusterului și altele). În cazul discurilor de startup, sectorul de boot conține un program care încarcă sistemul de operare.

Semnătură malware

Semnăturile malware sunt fragmente de coduri extrase din mostre reale de malware. Acestea sunt utilizate de către programele antivirus pentru a realiza o identificare după model și detectare a programelor malware. Semnăturile sunt utilizate și pentru a elimina codul malware din fișierele infectate.

Baza de date cu semnături malware a Bitdefender reprezintă o colecție de semnături malware actualizate în fiecare oră de către cercetătorii malware ai Bitdefender.

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

publicitate. Aplicațiile spyware sunt de obicei permise 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 un cal troian este 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.

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.

Tehnică de exploatare

O exploatare se referă, în general, la orice metodă folosită pentru a câștiga acces neautorizat la calculatoare sau la o vulnerabilitate din securitatea unui sistem care expune un sistem unui atac.

Troian

Este un program distructiv care este mascat sub forma unei aplicații benigne. Spre deosebire de viruși, troienii nu se multiplică, dar pot fi la fel de distructivi. Unul dintre cei mai mascați troieni este acela care pretinde că elimină virușii de pe computerul dumneavoastră, dar în loc de aceasta, introduce viruși pe calculatorul dumneavoastră.

Termenul provine de la o poveste din opera "Iliada" lui Homer, în care grecii 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.

Vierme

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

Virus

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 virușilor se pot și înmulți. Toți virușii informatici sunt creați de om. Un simplu virus care poate realiza copii ale sale este relativ simplu de produs. Chiar și un asemenea virus este periculos întrucât poate duce la blocarea sistemului, prin utilizarea la maxim a resurselor de memorie. Un virus și mai periculos este acela care este capabil să se răspândească în rețea și poate să treacă de sistemele de securitate.

Virus de boot

Reprezintă un virus care infectează sectorul de boot al unui disc fix sau al unei dischete. Orice încercare de a face boot de pe o dischetă infectată cu un virus de boot va determina virusul să devină activ în memorie. Din acest moment de fiecare dată când veți realiza boot-area sistemului, virusul va deveni activ în memorie.

Virus de macro

Un tip de virus informatic este acela inclus ca macro într-un document. Multe aplicații cum ar fi de exemplu Microsoft Word și Excel suportă limbaje macro puternice.

Aceste limbaje permit încapsularea de macro-uri în documente și execută aceste macro-uri de fiecare dată când este deschis documentul.

Virus polimorf

Reprezintă un virus care își schimbă forma cu fiecare fișier pe care îl infectează. Din cauză că nu au un tipar binar consistent, asemenea viruși sunt greu de identificat.