

The logo for VirusBuster Scanner 1.5 is positioned in the lower right quadrant of the image. It features the word "VirusBuster" in a bold, white, sans-serif font, with a stylized orange and white arrow pointing upwards and to the right, integrated into the letter "V". Below "VirusBuster" is the word "Scanner" in a smaller, white, sans-serif font. At the bottom right of the logo is the version number "1.5" in a white, sans-serif font. The background is a solid dark blue with several light blue, curved, overlapping lines that sweep across the left and bottom portions of the image, creating a sense of motion and depth.

VirusBuster
Scanner
1.5

TARTALOMJEGYZÉK

VIRUSBUSTER SCANNER	2
Rendszerkövetelmények	2
A program működése	3
Kapcsolók	3
Néhány példa kapcsolókkal való indításra.....	10
Időzített indítás lehetősége (Linux rendszereken)	12
Visszatérési értékek	12
A konfigurációs fájl kialakítása	13
Vírusadatbázis frissítése	14
VÉGFELHASZNÁLÓI SZERZŐDÉS	15
KAPCSOLAT	16

VIRUSBUSTER SCANNER

Hasonlóságuk és azonos kezelési módjuk miatt a VirusBuster Scanner programok különböző rendszereken működő verzióinak leírásait összevonva tárgyaljuk. Az esetleges eltérések a dokumentációban jelezve vannak. A VirusBuster Scanner programok feladata, hogy felderítsék az adathordozókon található állományok, vagy más területek vírusfertőzését, és lehetőség szerint eltávolítsák azt. A VirusBuster Scanner programok tehát vírusfelismerő és -irtó alkalmazások, segítségével bizonyos időközönként ellenőrizheti számítógépe állapotát. A programok parancssorból indíthatók, működésük kapcsolókkal szabályozható. A kapcsolók használatával bizonyos fokú automatikus védelem is megvalósítható.

A termék főbb tulajdonságai:

- Interaktív és automatikus üzemmódban történő működés
- Heurisztikus keresési szintek
- Többszálú keresés lehetősége
- Ki/bekapcsolható boot vizsgálat
- Fájlból beolvasandó beállítások kezelése (konfigurációs fájl kezelése)
- Parancssori karantén kezelés
- Inkrementális vírusadatbázis frissítés

Rendszerkövetelmények

A felsorolt operációs rendszerek támogatottak a következő rendszerösszetevők kíséretében:

Általános követelmények

400 MHz (x86/x64) processzor
256 MB memória (512 MB ajánlott)
100 MB szabad merevlemez kapacitás

Támogatott platformok

WINDOWS: Win7/Vista/XP/2000/Me/98 | Win2008/2003/2000srv
LINUX: GLIBC 2.2.5, kernel 2.2.x

A program működése

A VirusBuster Scanners alkalmazások parancssori kereső funkciót látnak el, parancssorból indítva őket, a kapcsolókkal és a konfigurációs fájlban meghatározott beállításokkal víruskeresést végeznek a rendszerben. A konfigurációs állományban lehetőség van az általános keresési beállítások eltárolására, hogy szükség esetén parancssorból csak az ettől eltérő értékeket kelljen meghatározni. A többszálú keresés funkció használatával a keresési időt lehet rövidíteni az átlapolható feladatok párhuzamos feldolgozásával.

A VirusBuster Scanners program moduljai egy egyszerű tömörített állományban találhatóak, melyek kicsomagolás után válnak használhatóvá. A program a következő modulokból áll:

vbscan.exe | vbscan

Fő futtatható fájl (Windows | Unix rendszereken)

vbeng*.dll | libvbengine.so

Keresőmotor betöltő modul (Windows | Unix rendszereken)

vbscan.ini

Konfigurációs fájl

vdb/

A vírusadatbázis fájlokat és víruskereső core fájlokat tartalmazó könyvtár.

docs/<nyelv>/

A könyvtár a következő szöveges fájlokat tartalmazza:

- A program leírása
(szöveges fájl és man page (Unix) formátumban)
- Végfelhasználói szerződés

A víruskeresés a vbscan.exe vagy vbscan program indításával lehetséges, a keresési beállításokat a program konfigurációs fájljában, illetve a parancssori kapcsolókkal lehet meghatározni.

Figyelem!

A VirusBuster korábbi verzióinak jelenléte befolyásolhatja a keresőprogram működését, ezért sikertelen indítás esetén megoldás lehet a korábbi verzió(k) eltávolítása!

Ha a program indításakor a parancssorban nincs meghatározva a konfigurációs fájl elérhetősége, akkor a program automatikusan megpróbálja betölteni ezt az aktuális könyvtárból, illetve abból a könyvtárból, ahol maga a főprogram található. Ha a konfigurációs fájl ezeken a helyeken nem található, akkor csak a parancssorban megadott kapcsoló-beállítások lesznek érvényesek.

Keresés csak abban az esetben indítható, ha a mindenképpen szükséges kapcsolók - akár a konfigurációs fájlban, akár a parancssori kapcsoló-listában - beállítása megtörtént.

Mindenképpen meg kell adni a karantén könyvtárat (-y kapcsolóval), az átmeneti (temp) könyvtárat (-t kapcsolóval) és ajánlott a vírusadatbázis helyét is (-d kapcsolóval). E beállítások nélkül nem indítható keresés.

Kapcsolók

A könnyebb átláthatóság érdekében a kapcsolók tematikus csoportokba szedve követik egymást. A kapcsolók betűjeleinek kiválasztásakor szempont volt, hogy szabványos jeleket használjunk, és a gyakran használt funkciók elérhetőek legyenek úgynevezett rövid (egybetűs) kapcsolón keresztül is. Az alapértelmezett beállítások jelezve vannak a magyarázatnál, ezek a funkciók mindenféle külön beállítás nélkül aktívak a keresés során.

Információkérés

-V --version

Megjeleníti a program-, a használt keresőmotor- és a vdb verziószámát, a majd kilép.

-h --help

Megjeleníti az általános parancssori kapcsolók rövid összefoglalását (alapértelmezett értékeit), és a program verziószámát, majd kilép.

--full-help

Megjeleníti az összes parancssori kapcsoló rövid összefoglalását (alapértelmezett értékeit), és a program verziószámát, majd kilép.

Regisztrációs adatok megadása

-k --registration-key

A regisztrációs kulcs megadása, ahogy azt a licencszerződésben megtalálja. A program kezeli a kötőjelekkel tagolt formát is (XXXXX-XXXXX-XXXXX).

-u --registered-user

A regisztrált felhasználó nevének megadása, ahogy azt a licencszerződésben megtalálja.

Regisztráció hiányában, vagy érvénytelen regisztrációs adatokkal a program 30 másodpercet várakozik indítása után, utána teljes funkcionalitásban használható. A sikeres regisztráláshoz a regisztrációs kulcsot és a felhasználónevet együtt kell megadni.

Működési beállítások

-T --terse

Tömörebb naplózási forma bekapcsolása.

Tömör naplózás:

```
/mnt/test/eicar.zip//eicar1.com: found: EICAR skipped.
```

Eredeti forma:

```
/mnt/test/eicar.zip//eicar1.com
```

```
virus found: EICAR_test_file (NOT killable) ... skipped.
```

-TT --terse --terse

Csak a találati információk kerülnek be a napló fájlba, illetve ha nem kerülne semmi a naplóba, létre sem jön a fájl.

-q --quiet

Csendes üzemmód bekapcsolása, a program csak a vírustalálatokat írja ki a képernyőre, illetve a napló fájlba, és a keresés végén az eredményről egy összefoglaló táblázatban is tájékoztat.

A kapcsoló kétszeri megadása esetén:

-qq vagy --quiet --quiet

Ekkor a program nem ír ki semmit a stdout-ra csak a találatokat (a keresés végén a tájékoztató táblázat sem jelenik meg).

A kapcsoló háromszoros megadása esetén:

-qqq vagy --quiet --quiet --quiet

Hatása megegyezik a --terse és -qq opciók együttes hatásával.

FIGYELEM! A quiet kapcsoló csak a stdout-ra vonatkozik, stderr-en még megjelenhetnek hibaüzenetek!

-qqqq vagy --quiet --quiet --quiet --quiet

Ha nincs kiírandó üzenet (nem történt károsító találat), nem keletkezik bejegyzés a napló fájlba.

--summary

Letiltja a keresési folyamatról készült összefoglaló statisztikai táblázatok, illetve egyéb keresési információk megjelenését.

Ha a -qq (vagy ezek erősebb hatású formái) is meg vannak adva, akkor hatása pont ellentétes: engedélyezi az összefoglaló megjelenítését.

-o --old

A program nem figyelmeztet, ha a használt adatbázis már két hétnél régebbi.

-c --config=FILE

Konfigurációs állomány beolvasása, helyének meghatározása. Ha ez a kapcsoló nincs megadva, akkor a program az aktuális könyvtárban, ill. a saját könyvtárában keresi a fájlt vbuster.ini néven. A parancssorból nem megadott, általánosan használt, ezért a konfigurációs fájlban rögzített opciók (kapcsolók) értékét innen próbálja meg kiolvasni a program. A fájlban megadott opciók a parancssorból felülbírálhatók. Ügyeljen arra, hogy a konfigurációs fájlban relatív útvonallal megadott állományokat és könyvtárakat a program az aktuális könyvtárhoz képest keresi!

--show-config

Megjeleníti az opciók aktuális beállítását.

-E --engine=FILE

Lehetőség van a használni kívánt víruskereső motor fájl megadására. Alapértelmezetten a fájlt a program a saját könyvtárában keresi.

--debug=FILE

Az opció megadásakor a program működése közben egy - a működéssel kapcsolatos - részletes információs fájlt hoz létre (a megadott helyen és névvel), mely a későbbiekben a keresési folyamat részletes elemzésére is felhasználható.

Keresési terület meghatározása

-Z --skip-archive

A tömörített állományok nem kerülnek átvizsgálásra.

Alapértelmezetten a tömörített állományok is vizsgálat alá kerülnek, e kapcsolóval ezek mellőzése állítható be.

-b --boot

A számítógép boot szektorait is vizsgálja. Nincs lehetőség boot szektorokat külön-külön vizsgálni. A kapcsoló csak Windows rendszereken hatásos.

-M --skip-mail

MIME típusú állományok nem kerülnek ellenőrzésre.

Alapértelmezetten a keresés az ilyen típusú fájlok átvizsgálását is magában foglalja.

--symlink=ACTION

Szimbolikus hivatkozások kezelésének beállítása (csak unix rendszereken használatos). Lehetséges értékek (akciók):

follow - a hivatkozásként megadott névvel azonosítja a fájlt

resolve - a hivatkozott fájl saját nevével azonosítja a fájlt

(ezekben az esetekben a hivatkozott fájlokat is ellenőrzi, mintha szokványos fájlok lennének)

skip - szimbolikus hivatkozások figyelmen kívül hagyása

(ebben az esetben a hivatkozott fájlokat nem ellenőrzi)

-R --skip-subdir[=PATH]

Alapértelmezetten a keresés az alkönyvtárakat is bejárja, ha könyvtár van megadva célként (rekurzív keresés). Ezzel a kapcsolóval lehetőség van a megadott könyvtárak,

vagy könyvtár részletek kihagyására a keresésből, a többi könyvtáron végrehajtódik rekurzívan a keresés. Ha a kapcsolót paraméter nélkül használja, akkor a célterület összes alkönyvtárát kihagyja a keresésből.

-f --file=FILE

Lehetőség van egy szöveges fájlban meghatározni azokat a könyvtárakat és fájlokat, melyeket át szeretnénk vizsgáltatni. E kapcsoló értékeként kell meghatározni ennek a fájlnek a nevét. Az ellenőrizendő objektumokat külön sorokban kell feltüntetni egymás alatt.

Speciális érték: '-' kötőjel ('--file=-'): ilyenkor STDIN-ről olvassa be az átvizsgálandó fájl- vagy könyvtár nevét (csak automatikus módban működik).

Figyelem!

Ez a kapcsoló nem használható karanténelemek és bootszektorok átvizsgálásához!

Ellenőrizendő fájltypusok

Alapértelmezésben csak a keresőmotorban eltárolt fájltypusok (alapértelmezett kiterjesztések) kerülnek vírusellenőrzésre a keresés során. Az alapértelmezett fájltypusok a következők:

Program fájlok: *.exe|*.com|*.ov?|*.sys|*.386|
.bin|.dll|*.drv|*.lnk|*.ocx|*.prg|*.scr|
.vxd|.crt|*.prc|*.xml|*.swf
Szkript fájlok: *.bat|*.ht*|*.js|*.jse|*.vbs|
.ini|.csc|*.hlp|*.shs|*.pif|*.ade|*.adp|
.bas|.chm|*.cmd|*.cpl|*.inf|*.ins|*.isp|
.zl|*.mde|*.msc|*.msi|*.msp|*.mst|*.pcd|
.reg|.scr|*.sct|*.url|*.vb|*.vbe|*.ws*|
.ans|.tmp|*.mpp|*.mpt|*.
Dokumentációs fájlok: *.do?|*.rtf|*.wiz|*.eml
Táblázatok: *.xl?
Access fájlok: *.mdb
Prezentációs fájlok: *.ppt|*.pot
Tömörítvények: *.arj|*.a??|*.zip|*.rar|*.cab|
.gz|.bz2|*.tgz|*.tar|*.dbx

A következő opciók segítségével felüldefiniálhatja ezen fájltypusok csoportját:

--all-files

Kikapcsolja a fájltypus alapján történő vírusellenőrzést, így minden fájl átvizsgálásra kerül.

-p --pattern=PATTERN

A program csak a megadott fájlnev-mintára illeszkedő fájlokat ellenőrzi.

--include=PATTERN

További fájltypusok meghatározása, melyeken szintén végre fog hajtódni a keresés.

--exclude=PATTERN

Keresésből kizárandó fájltypusok meghatározása. E kapcsoló precedenciája nagyobb, mint a fenti opcióké.

-m --match-in-archive

A tömörítvényeken belüli fájlnev-mintaillesztés alapértelmezésben be van kapcsolva, ha keresőmotor mintáit használjuk ('--include' és/vagy '--exclude' kapcsolókkal akár). Minden más esetben pedig kikapcsolt állapotban van ('--pattern' vagy '--all-files' használatakor). A '--match-in-archive' kapcsoló az alapértelmezett beállítást változtatja meg.

Összefüggések:

- '--all-files', '--pattern', '--include' egymást kölcsönösen kizáró kapcsolók
- ha a fenti opciók közül egyik sincsen megadva, akkor a program az alapértelmezett kiterjesztésű fájlokat ellenőrzi

PATTERN szintaxis:

A PATTERN-on belül pipe-jellel (|) elválasztva több mintát is meg lehet adni. A minta '?' és '*' metakaraktereket is tartalmazhat (a ? -t (kérdőjelet) egy tetszőleges karakternek veszi a program, a * -t (csillagot) tetszőleges karaktersorozatnak). A program kezeli a karakterosztályokat is, melyekkel a ?-nél szűkebb feltételek megadása lehetséges. Karakterosztályokat szögletes zárójelek között (például [abc]) kell megadni. Ha a felkiáltójel '!' a kezdő szögletes zárójel '[' után áll, az a tagadás jele. Karakterosztályokon belül hosszabb felsorolás helyett tartományokat is meg lehet határozni úgy, hogy a tartomány első és utolsó karaktere közé kötőjelet '-' kell tenni. Ha a '-'-t vagy a '!'-t, mint figyelembe veendő karaktert akarja megadni, akkor azok a bezáró szögletes zárójel ']' elé írandó. A program nem tesz különbséget a kis- és nagybetűk között.

A '*' és '?' metakarakterek és a karakterosztályok soha nem illeszkednek a könyvtárelválasztó jelre, erre a speciális '**' sorozat használható, amivel teljes elérési utakat lehet kiváltani több szint mélységben, mint pl.: 'Program Files**\.exe' - minden .exe kiterjesztésű állomány a Program Files könyvtár alatt (az alkönyvtárakban is)

Figyelem!

Könyvtárelválasztó karaktert vagy a speciális jelentéssel bíró '**' sorozatot tartalmazó mintákat (PATTERN) a fájlok teljes nevére (könyvtárrésszel együtt) illeszti a program, míg minden más mintát csak a fájl tényleges nevére - könyvtárrész nélkül. A könyvtárelválasztó karakter Unix ill. GNU/Linux rendszereken '/', Windows-on '\', ami ugyanaz, mint ami a metakarakterek literálissá alakításához használható. A program általában könyvtár elválasztóként ismeri fel a '\'-t ezeken a rendszereken, és csak akkor kell megduplázni ('\\', ha utána valamelyik speciális jelentésű metakarakter áll, azaz a | * ? [] . valamelyike.

Keresési módok és akciók vírustalálalat esetén

-e --heuristics = (o | off | n | normal | h | high)

A heurisztikus analízis szintjének beállítása. Alapértelmezetten a 'normal' szint aktív.

o / off - heurisztika kikapcsolva
n / normal - normál szintű heurisztika
h / high - magas szintű heurisztika

-s --scanning = (fa | fast | s | strict | fu | full)

A keresés módjának beállítása. Alapértelmezetten a 'regular' szint aktív.

fa / fast - Szigorúan csak a fájl azon részeiben keres vírust, ahol az előfordulhat, néhány olyan vírustípust nem ismer fel, melyek megkeresése nagy erőforrást igényel (pl.: Excel FORMULA vírusok)

s / strict - Optimalizált keresési mód, mely minden - az adatbázisban regisztrált - vírust felismer, a fájl azon részeiben keres vírust, ahol az előfordulhat.

fu / full - Minden - az adatbázisban regisztrált - vírust felismer, a teljes fájlt leellenőrzi, azokat a részeket is, ahol normális esetben nem fordulhat elő vírus.

--thread=NUM

A kereséshez nyitható programszálak maximális száma, alapértelmezett érték: 1. Többszálú alkalmazások általában jobb teljesítménnyel futnak, de ez nagyban függ a rendszer beállításaitól is.

--timeout=NUM

A keresőszálak időtúllépési korlátja (másodpercekben). A program leállítja önmagát, ha - '--timeout-abort' kapcsolótól függően - mindegyik vagy akár csak egy kereső szál túllépi ezt az időkorlátot, és nem indul újra a megadott időintervallumon belül. Nagy méretű archívumok, vagy erősen terhelt rendszer esetén érdemes lehet ezt a korlátot megemelni.

--timeout-abort

A '--timeout-abort' kapcsoló befolyásolja, hogy melyik esetben szakítja meg a program a futást. Ha a kapcsoló meg van adva, akkor az első időtúllépés esetén a program félbehagyja a megadott területek keresését, és megszakítja a futását. Alapértelmezésben ki van kapcsolva, ami azt jelenti, hogy amíg legalább egyetlen szál az időkorláton belül végez, addig a program tovább fut. A --thread alapbeállítása azonban csak egy szál indítását engedélyezi, így ha az túllépi az időkeretet, akkor a program alapesetben így is kilép.

-a --action=ACTION

A kapcsoló megadásával automatikus módban fut a program, azaz minden vírustalálatra a megadott akció(ka)t próbálja meg végrehajtani. A kapcsoló értékeként a végrehajtandó akció(ka)t kell megadni. Több akciót is előírhat a kapcsoló ismételt megadásával, ebben az esetben, ha az első műveletet nem sikerül elvégezni, akkor sorban a többit próbálja meg végrehajtani a fertőzött állományon. Ha ez a kapcsoló egyáltalán nincs megadva, akkor minden vírustalálathoz a felhasználónak kell meghatározni a végrehajtandó műveletet (interaktív mód).

A lehetséges akciók jelentése:

k - irtás az állományból (kill)

s - változatlanul hagyja a fertőzött objektumot (skip)

r - átnevezés (rename)

q - karanténba helyezés (quarantine)

d - vissza nem állítható törlés (delete)

--remove-macro

Automatikusan törli a Microsoft Office dokumentumokból az összes makrót az interaktív üzemmódtól függetlenül, rákérdezés nélkül.

--sfx[=ENUM]

Az SFX (önkicsomagoló) felismerés ki-, illetve bekapcsolása. Értéke lehet: on vagy off. Alapértelmezetten be van kapcsolva (on).

--archive-max-size=NUM

Alapértelmezett érték: 0 (ilyenkor az engine-ben meghatározott default értéket használja).

Ha a vizsgált állomány kitömörített mérete meghaladja az ebben az opcióban meghatározott méretkorlátot, a program exploit vírustalálathoz ad vissza az adott tömörítvényre. (a beállítás MBájt-ban határozandó meg).

--archive-max-ratio=NUM

Alapértelmezett érték: 0 (ilyenkor az engine-ben meghatározott default értéket használja).

Példa érték: 50

Ha a tömörítvényben található fájl mérete a kitömörítés után (az itt megadott érték szerint) 50-szer nagyobb, vagy még nagyobb, akkor a program exploit vírustalálathoz jelez.

Az érték értelmezése százalékban: $1/n \cdot 100$, ahol n az opció értéke.

A példában: $1/50 \cdot 100 = 2\%$, tehát ha a tömörítés hatásfoka 2%, vagy annál jobb (ez már gyanúsán "jó" érték), akkor a program exploit vírustalálathoz ad vissza.

--memory-limit=NUM

Keresés során engedélyezett memóriahasználat MB-ban (ebben nincs benne a vírusadatbázis által elfoglalt memória). Alapértelmezett: 256, korlátlan: -1

--memory-block-max=NUM

Egy memória foglalás (pl. malloc) során lefoglalható terület méretét lehet korlátozni MB-ban. Célja, hogy egyes exploit-ok ne tudják hatalmas memória foglalásokkal megbénítani az engine-t. Alapértelmezett 256.

-G --greyware

A kapcsoló hatására kereséskor a program találatot jelez a greyware kategóriába sorolt termékekre és a beállított akciót hajtja végre a felismert alkalmazásokon. Greyware-ek közé soroljuk azokat a programokat, melyek egyértelmű kategorizálása nem lehetséges, mivel az változhat felhasználásuk módjától. Általában ezen alkalmazások nem károkozók, amennyiben a felhasználó jóváhagyta ezek rendszerbe való telepítését, használatukat. Ám előfordulhat, hogy kihasználva ezen programok funkcionalitásából eredő lehetőségeket, ezek ártó szándékkal, a felhasználó tudta nélkül kerülnek feltelepítésre, lehetőséget adva rosszindulatú tevékenységek végzésére (ilyen lehet pl: ftp szerver program, távoli hozzáférést lehetővé tevő alkalmazás). Vagyis magából a program jelenlétéből nem lehet egyértelműen megállapítani, hogy kárt okoz-e az adott gépen, ezt a felkerülés körülményei döntenek el.

Karantén-kezelés

Az alábbi karantén opciók mindegyike elfogad egy vagy több úgynevezett kulcsot (KEY), vagy kulcs-állománynév párt (KEY:FILE), és csak a megadott karantén elemeken hajtódnak végre a műveletek. Kulcs hiányában minden karanténban levő elem végrehajtódik a kijelölt művelet. Az egyes elemekhez tartozó kulcsokat a karantén könyvtár tartalmának kiíratásával (--list) tudja megjeleníteni.

--status = (all | clean | deleted | infected | suspicious)

Ezzel a kapcsolóval leszűkítheti/megváltoztathatja a feldolgozandó karanténelemek alapértelmezett körét azokra az elemekre, amelyeknek a fertőzöttségi státusza a megadott értékkel megegyezik.

clean: csak a tiszta (nem fertőzött) elemekre...

deleted: csak az újraellenőrzés során törölt elemekre...

infected: csak a fertőzött elemekre...

suspicious: csak a gyanús elemekre...

hajtódik végre a kívánt akció.

Az 'all' speciális érték azt jelenti, hogy mindenféle fertőzöttségű elemre a megadott akció végre lesz hajtva.

Ennek a kapcsolónak az alapértelmezett értéke minden karantén műveletre más és más:

--list: 'all'

--restore: 'clean'

--delete: 'infected'

--saveas: 'all'

-l --list[=KEY]

Kilistázza a karanténba helyezett állományokat, azok kulcsát, állapotukat (lásd --status kapcsoló), az eredeti fájl elérési helyét, méretét. Kulcs meghatározásával lehetőség van az egyes elemekre külön hivatkozni.

--rescan[=KEY]

Újra ellenőrzi a karantén összes elemét, vagy a kulccsal meghatározott objektumokat. Erre a kapcsolóra nincs hatással a --status.

--restore[=KEY[:FILE]]

Visszaállítja az előzőleg a '--rescan' paranccsal megtisztított összes elemet, vagy a kulccsal meghatározott objektumokat. A művelet nem hoz létre nem létező könyvtárakat, és meglévő állományokat csak az '--overwrite' kapcsoló megadása esetén ír felül. Ha egyes elemek esetén nem sikeres a művelet, ellenőrizze, hogy ez nem az említett okok valamelyikére vezethető-e vissza.

Fontos!

Alapértelmezésben a kapcsoló csak a tiszta, nem fertőzött állományokat állítja helyre, de a '--status' kapcsoló használatával felülbíráhatja, hogy a program az adott állapotú karanténelemeket is engedje helyre állítani. Ezt csak akkor használja, amennyiben biztos abban, hogy vakriasztás történt, azaz az adott karanténba tett állomány nem fertőzött!

--delete[=KEY]

Feltétel nélkül törli az összes elemet, vagy csak a kulccsal meghatározott objektumokat a karanténból. Alapesetben csak a fertőzött elemeket törli, de a --status kapcsolóval ezt felülbíráhatja!

--saveas=KEY:FILE

Kimentí a megadott kulcsú (KEY) karanténfájlt a megadott FILE -ba biztonságos, elkódolt formátumban, tehát az így létrejött fájl nem egyezik meg az eredetivel. Ennek a funkciónak akkor veszi hasznát, ha a VirusBuster Kft-nek vissza szeretne küldeni egy adott fájlt vizsgálatra.

-w --overwrite

Engedélyezi már meglevő állományok felülírását a '--restore' és '--saveas' műveletek számára.

Fájl- és könyvtárhivatkozások

Az alább relatív útvonallal megadott paraméterek értelmezésének kiindulópontja a program home könyvtára (amelyik a futtatható fájlokat tartalmazza):

-y --quarantine=DIR

A karantén könyvtár megadása.

-t --temp=DIR

Az átmeneti fájlok könyvtára, ahová a program írhat, alapértelmezésben a TEMP/TMP környezeti változó értékét használja.

-d --vdb=DIR

A vírusadatbázis fájl leíró XML fájl elérési útvonala, ennek megadása nem kötelező, de ajánlott. Ha nincs megadva ez a kapcsoló, akkor a program a leíró fájlt a saját könyvtárában keresi, alapértelmezetten a 'vdb' könyvtárban.

Néhány példa kapcsolókkal való indításra

vbscan.exe c:

A teljes C: meghajtót átvizsgálja, találat esetén a felhasználtól kérdezi meg, mit tegyen az objektummal.

vbscan.exe --pattern="*.exe|*.dll|*.com" --action=quarantine "C:\Program Files"

Windows binárisok vizsgálata a Program Files könyvtárban, a fertőzött fájlokat további ellenőrzésig karantén alá helyezi.

Fontos!

Windows rendszereken a speciális karaktereket (itt a példában szóközt) tartalmazó fájlneveket " " (idézőjelek) között kell megadni!

vbscan --pattern='*.exe|*.dll|*.com' --action=quarantine /mnt/windows/c/

Bináris állományok vizsgálata bemountolt Windows partíción Linux alatt. A fertőzött fájlokat automatikusan karanténba helyezi.

Fontos!

Linux/Unix rendszereken a shell értelmező elől le kell védeni a joker karaktereket ' ' (aposztrófok) közé téve őket!

vbscan.exe --rescan --action=kill --restore --delete

Újraellenőrzi a korábban karanténba tett fájlokat, és amelyiket lehet, megtisztítja (kill), majd ezeket visszahelyezi eredeti helyükre. A továbbra is fertőzötteket törli a karanténból.

vbscan --list --status=suspicious

Csak a gyanúsnak ítélt karanténelemeket listázza ki.

vbscan --saveas=0892342:examine.vbq

A 0892342 kulcsú karanténelemet az aktuális könyvtárba másolja 'examine.vbq' néven.

vbscan.exe --file=- --action=kill

Az STDIN-ről beolvasott nevű fájlokat vagy könyvtárakat ellenőrzi, a fertőzötteket megtisztítja.

vbscan c:\ --skip-subdir="Utils\Arc*" --terse

A kereső átvizsgálja a c:\ meghajtót rekurzívan, interaktív módban (a parancssorban nincs megadva akció), de nem vizsgálja át a 'Utils' könyvtár egyik 'Arc' kezdetű alkönyvtárát sem (--skip-subdir). A keresésről tömör naplózást készít (--terse).

Példa a rövid kapcsolók használatára:

vbscan -b -eh -sf --follow -ak,q /

Mindent átvizsgál (/ root könyvtárból) a legmagasabb fokozaton, amit lehet irt, a nem irthatókat pedig karanténba helyezi. A program felismeri azt, hogy a '--follow' argumentum a '--follow-symlink' rövidítése, illetve több akciót is meg lehet adni egy argumentumon belül vesszővel elválasztva.

Időzített indítás lehetősége (Linux rendszereken)

A keresés automatizálására lehetőség van a 'cron' nevű program segítségével. Időzítheti a program elindítását például minden este 8 órára. Jegyezze be a /etc/crontab-ba:

```
00 20 * * * root <elérési_út>vbscan <elérési_út>vbscan.ini
```

Visszatérési értékek

A program a visszatérési értékében is tájékoztat az elvégzett feladatok sikerességéről a képernyőre – és kérésre – a naplófájlba írt üzeneteken kívül, aminek automatikusan vagy időzített futásnál veheti hasznát.

A program a víruskeresés során 3 alapállapotot különböztet meg ('A' eset):

0

Gyanús vagy fertőzött objektumot nem talált

1

A célobjektumok között fertőzött vagy gyanús objektumokat talált.

2

A gyanús vagy fertőzött objektumokon sikerrel hajtotta végre a megadott akciókat (--action) kivéve, ha az "stop" vagy "skip" volt.

Ha az ellenőrzés során valamilyen hiba lép fel, akkor a megadott objektumok némelyikét a kereső nem tudta maradéktalanul ellenőrizni vagy megtisztítani. A fellépett hibák forrásától függően az alapértékek módosulnak.

A visszatérési értékek értelmezését az alábbi táblázat mutatja:

	0	1	2

	Sikeresen ellenőrzött objektumokban		

	nincs	van vírus, de	minden felismert
	vírus	nincs irtva	víruson akció
			végrehajtva

'A' eset			
Minden megadott cél	0	1	2
objektum sikeresen	(*)	(!)	(*)
ellenőrizve			
	=====		
'B' eset			
Nem sikerült minden	3	1	5
objektumot ellenőrizni	(?)	(!)	(?)

'C' eset			
Rendszerhiba miatt	6	1	8
nem sikerült minden	(?)	(!)	(?)
objektum ellenőrizni			

'D' eset			
Fájl-formátum			
Támogatásának hiányában	9	1	11
nem sikerült minden	(?)	(!)	(?)
objektumot ellenőrizni			

Jelölések:

szám: maga a visszatérési érték

(*): a keresés után a keresési útvonal biztosan vírusmentes

(!): a keresés után a keresési útvonal biztosan tartalmaz vírusos fájlt

(?): a keresés után a keresési útvonal tartalmazhat vírusos fájlt

'B' eset:

Az állományok némelyiket nem lehet olvasni jelszóvédelem, hibás fájlformátum vagy exploit veszély miatt. Ezek az állományok veszélyt jelenthetnek, hiszen a tartalmukat nem sikerült ellenőrizni!

'C' eset:

Rendszerhiba történt, aminek az elhárítása után érdemes ismét megpróbálni az ellenőrzést. A hiba oka lehet egyszerűen az, hogy a megadott állományok nem léteznek vagy a programnak nincs jogosultsága olvasni vagy írni azokat. Erősen terhelte rendszer esetén az erőforrások hiánya is okozhat ilyen hibát.

'D' eset:

Néhány fájl ellenőrzése sikertelen volt, amelyeknek formátumát ugyan felismerte a víruskereső motor, de az adott verziót még nem támogatja. Az ilyen fájlok tartalmát csak újabb verziójú keresőmotor tudja felismerni, tehát programfrissítés szükséges hozzá.

A magasabb hibakódok általában rossz beállítási paramétereket jeleznek:

255

Érvénytelen parancssori vagy konfigurációs állománybeli beállításokat adott meg, ellenőrizze ezeket!

254

Nem sikerült a víruskereső motort elindítani vagy nem létezik a megadott vírusadatbázis.

253

Rossz (inkompatibilis) vírusadatbázis. Ellenőrizze az adatbázis verzióját!

252

Nem sikerült elindítani a keresést, valószínűleg nem áll rendelkezésre elég rendszererőforrás.

251

Karantént nem sikerült inicializálni. Ellenőrizze, hogy jó könyvtárat adott-e meg a '--quarantine' kapcsolónál!

250

A program futása külső kérésre megszakadt. (SIGINT, SIGTERM)

A karantén műveletek sikeres végrehajtása esetén a program visszatérési értéke mindig 0.

A konfigurációs fájl kialakítása

A fájl az egyszerű vezérelhetőség miatt sororientált, minden beállítás külön sorba kerül. Kapcsolóként mind az egybetűs mind a hosszabb alak megengedett, de a bevezető kötőjeleket ('-' vagy '--') nem kell kiírni. A kapcsoló által felvehető értékek megegyeznek a parancssori kapcsolók által felvehető értékekkel. A logikai kapcsolók esetén - a parancssorhoz hasonlóan - a kapcsoló jelenléte illetve hiánya dönti el a hozzárendelt funkció iránti igényt vagy annak mellőzését. A megjegyzéseket a '#' karakter után lehet megadni, külön sorban vagy a sor végén.

Vírusadatbázis frissítése

A termék a vírusadatbázis napra készen tartásához inkrementális adatbázis frissítési mechanizmust használ. A módszer lényege és előnye, hogy frissítéskor a programnak nem kell letöltenie mindig a teljes (több megabájt méretű) vírusadatbázis csomagot, hanem általában csak egy kisebb kiegészítő adatbázis fájlt, mely az utóbbi időben megjelent és feldolgozott károkozók felismeréséhez és eltávolításához szükséges információkat tartalmazza. Ezzel a módszerrel a napi frissítések időtartama a töredékére csökken, így lehetőség van akár naponta többször is vírusadatbázis frissítés kiadására, mely növeli a vírusvédelem hatékonyságát. Az egyes újonnan megjelenő károkozók elleni védelem a károkozók feldolgozása után szinte azonnal, minimális hálózati forgalom és letöltési idő ráfordítással eljut a felhasználókhöz.

Windows rendszereken

A vírusadatbázis frissítése manuálisan hajtható végre. A vírusadatbázis-készlet több fájlból áll ezek mindegyikének frissítése szükséges. A program az adatbázis fájlokat a saját könyvtárában található 'vdb' alkönyvtárban tárolja alapértelmezetten. A frissítéshez töltsse le a következő könyvtár teljes tartalmát FTP szerverünkről:

```
update.virusbuster.hu/pub12/vbuster/vdb12/
```

A letöltött fájlokkal írja felül az eddigi adatbázis fájlokat.

Unix rendszereken

A folyamat automatizálására egy scriptet mellékelünk, mely vdbupdate.sh néven található meg a csomagban.

A script indítása után automatikusan letölti a vírusadatbázist, majd bemásolja azt a megfelelő könyvtárstruktúrába (alapértelmezetten: 'vdb'). Csak akkor hajtja végre a frissítést, ha a szerveren frissebb adatbázis található, mint az adott számítógépen. Ellenkező esetben az adatbázisok változatlanok maradnak.

A script paraméterei:

```
-h érvényes paraméterek listája  
-v megjeleníti a letöltési folyamatot  
-t használandó átmeneti könyvtár megadása (alapértelmezett $TMPDIR)  
-i könyvtár megadása, ahová az új adatbázis kerül letöltés után (alapértelmezett $LIBDIR)  
-p HTTP protokoll használata az alapértelmezett FTP helyett  
-x vdb-hez tartozó xml leíró fájl nevének megadása  
-b vdb backup könyvtár megadása  
-e engine lib könyvtár megadása
```

A script futtatásához szükség van a wget és a sed programokra!
Cron segítségével időzítheti is az adatbázis frissítéseket.

VÉGFELHASZNÁLÓI SZERZŐDÉS

A VÉGFELHASZNÁLÓI SZERZŐDÉS EGY TÖRVÉNYES MEGEGYEZÉS ÖN ÉS A VirusBuster Kft. KÖZÖTT. OLVASSA EL FIGYELMESEN, MIELŐTT FOLYTATNÁ A TELEPÍTÉST, ÉS HASZNÁLATBA VENNÉ A TERMÉKET. A SZERZŐDÉS LICENCET BIZTOSÍT A PROGRAM HASZNÁLATÁHOZ VALAMINT JÓTÁLLÁSSAL KAPCSOLATOS INFORMÁCIÓT ÉS FELELŐSSÉGI KIKÖTÉSEKET TARTALMAZ. A PROGRAM TELEPÍTÉSÉVEL ÉS HASZNÁLATÁVAL ÖN MEGERŐSÍTI A PROGRAM ÉS EZEN SZERZŐDÉS FELTÉTELEINEK ELFOGADÁSÁT. HA NEM ÉRT EGYET EZEN SZERZŐDÉS FELTÉTELEIVEL, NE TELEPÍTSE A PROGRAMOT.

FONTOS MEGJEGYZÉS: A SZOFTVER NEM HIBATÚRÓ ÉS NEM OLYAN KÖRNYEZETEKBE TÖRTÉNŐ HASZNÁLATRA LETT TERVEZVE ÉS SZÁNVÁ, AMELYEKBE HIBAMENTES MŰKÖDÉS SZÜKSÉGES. EZ A SZOFTVER EZÉRT NEM HASZNÁLHATÓ REPÜLŐGÉP-NAVIGÁCIÓS RENDSZEREK, NUKLEÁRIS LÉTESÍTMÉNYEK, KOMMUNIKÁCIÓS RENDSZEREK, FEGYVERRENDSZEREK, KÖZVETETT VAGY KÖZVETLEN ÉLETFENNTARTÓ RENDSZEREK, ILLETVE LÉGI IRÁNYÍTÁS MŰKÖDÉSÉBEN, VAGY BÁRMILYEN OLYAN ALKALMAZÁSBAN VAGY ESZKÖZBEN, AMELYBEN A MEGHIBÁSODÁS HALÁLOS KIMENETELLEL, VAGY SÚLYOS, TESTI ÉPSÉGBEN VAGY VAGYONBAN KELETKEZŐ KÁRRAL JÁRHAT.

1. Meghatározások

- (a) Az "Oktatási Verzió"-n a Program azon verziója értendő, mely kizárólagosan oktatási intézmények számára készült. Az "Otthoni Verzió"-n a Program azon verziója értendő, mely kizárólagosan magánszemélyek részére, egy gépen való felhasználásra készült. Az Oktatási és az Otthoni verzió nem használható fel üzleti célokra.
- (b) A továbbiakban VirusBuster Kft. alatt a VirusBuster Kft. valamint, és amennyiben értelmezhető, terjesztői és értékesítői értendők.
- (c) A "Nem Értékesíthető Verzió"-n a Program azon verziója értendő, mely kizárólagosan a Program bemutatására és kipróbálására használható.
- (d) A "Program"-on a VirusBuster Kft. (R) VirusBuster(TM) elnevezésű szoftvere értendő, melyet a VirusBuster Kft. szolgáltat és mely tartalmaz bármely a programhoz kapcsolódó dokumentációt, kép- és hanganyagot, nyomtatott anyagot valamint on-line és elektronikus anyagot illetve dokumentációt.

2. Licenc

Ez a Végfelhasználói SZERZŐDÉS a következőkre jogosítja fel a végfelhasználót:

- (a) A Program telepítésére és felhasználására egy különálló gépen, VAGY a Program telepítésére egy adattárolón, például egy hálózati szerveren, kizárólag abból a célból, hogy onnan futtatva telepíthető legyen a Program más gépekre egy belső hálózaton feltéve, hogy a végfelhasználó rendelkezik licenccel minden egyes számítógépre, melyre a Programot telepítik, vagy melyen futtatják annak adattároló eszközéről. A Program licence nem osztható meg vagy használható fel különböző számítógépeken.
- (b) Csak Oktatási és Otthoni verzió. Ha az Oktatási, vagy az Otthoni verzióra vásárolt licencet, a Program telepíthető egy adattárolóra vagy tárolható azon, például egy hálózati szerveren kizárólag abból a célból, hogy onnan futtatható vagy telepíthető legyen a Program a belső hálózat más gépeire felhasználás céljából legfeljebb annyi felhasználó részére, mely szám nem haladja meg a megvásárolt licencek számát; biztosítva azt, hogy ellenőrzés alatt áll a felhasználók száma annak érdekében, hogy ezt a számot ne lépjék túl. A VirusBuster Kft. bármikor megvizsgálhatja, hogy a felhasználás megfelel-e a SZERZŐDÉSben foglaltaknak.
- (c) Készíthet egy másolatot a Programról kizárólagosan biztonsági célokból. A végfelhasználó bármely másolaton köteles feltüntetni minden szerzői joggal kapcsolatos információt valamint bármely tulajdonlással kapcsolatos megjegyzést, mely a Program eredeti példányán található.

3. Licenc kikötések

- (a) A második részben leírtakon kívül a Programról nem készíthető és terjeszthető semmilyen másolat valamint a Program nem küldhető egyik gépről a másikra elektronikus formában, vagy egy hálózaton belül.
- (b) A Programot tilos részeire bontani, visszafejteni, vagy bármely más olyan állapotba hozni, amely ember által vizsgálható.
- (c) A Program nem kölcsönözhető, nem adható el, nem adható bérbe és nem licencelhető.
- (d) Tilos a Programot módosítani vagy azon alapuló munkákat készíteni.
- (e) Tilos a Programot automatikus, fél-automatikus vagy manuális eszközökben vírusszignatúrák, vírus-felismerő rutinok vagy más, káros kódot vagy adatot felismerő adat vagy kód létrehozására használni,
- (f) Abban az esetben, ha bármilyen formában megszegi a jelen SZERZŐDÉSt, a VirusBuster Kft. megszüntetheti a licencet, és Ön köteles eltávolítani a Program minden másolatát.

4. Frissítések

Ha a Program jelen másolata a Program egy korábbi verziójának frissítése, akkor a korábbi végfelhasználói SZERZŐDÉS hatályát veszti és ez a SZERZŐDÉS lép életbe. A Program korábbi verziója nem használható a továbbiakban és nem adható át más jogi személynek.

5. Tulajdonlás

A licenc korlátozott jogokat biztosít a Program használatára. A VirusBuster Kft. minden jogot, címet és érdekeltséget fenntart beleértve minden védjegyet a Programra és minden másolatára vonatkozóan. Minden jog, mely külön nem kerül kiemelésre

jelen SZERZŐDÉSben, beleértve a nemzetközi védjegyeket is, a VirusBuster Kft. kizárólagos tulajdona.

6. KORLÁTOZOTT JÓTÁLLÁS ÉS KIKÖTÉSEK

(a) KORLÁTOZOTT JÓTÁLLÁS. A VirusBuster Kft. vállalja, hogy a kézhezvételtől számított (bizonyíthatóan) kilencven (90) napig az adathordozó, melyen a Program található, mentes lesz minden anyaghibától rendeltetésszerű használat esetén.

(b) EGYÉB JÓTÁLLÁS NINCS. KIVÉVE A FENTEBB LEÍRT KORLÁTOZOTT JÓTÁLLÁST, A VirusBuster Kft. KIZÁR BÁRMELY MÁS JÓTÁLLÁST. HA AZ ALKALMAZOTT JOG BÁRMELY JÓTÁLLÁST ÍR ELŐ A PROGRAMRA, ÚGY AZ A KÉZHEZVÉTEL TŐL SZÁMÍTVA CSAK KILENCVEN NAPIG ÉRVÉNYES. Bármely szóbeli vagy írásbeli információ vagy tanács, melyet a VirusBuster Kft., forgalmazói, terjesztői, ügynökei vagy alkalmazottai adnak, nem képezhet jótállást vagy szélesítheti annak körét.

7. Kizárólagos jogorvoslat

A 6-os rész alatt foglaltak úgy nyerhetnek jogorvoslatot, ha visszaviszi a Programot az értékesítés helyére a probléma leírásával és az értékesítés igazolásával. A VirusBuster Kft. kicseréli a sérült adathordozót. A VirusBuster Kft. elhárít minden felelősséget abban az esetben, ha az adathordozó sérülésének oka: baleset, nem rendeltetésszerű használat, nem megfelelő számítógép-konfiguráció alkalmazása.

8. KORLÁTOZOTT FELELŐSSÉG.

A VirusBuster Kft. NEM TARTOZIK FELELŐSSÉGGEL SEMMILYEN KÖZVETETT VAGY KÖZVETLEN KÁRÉRT SEM ÖNNEK, SEM BÁRMELY HARMADIK SZEMÉLYNEK (BELEÉRTVE KORLÁTOZÁS NÉLKÜL MINDEN NYERESÉGVESZTÉST, ÜZLETI TEVÉKENYSÉG KÉNYSZERŰ SZÜNTELEST, INFORMÁCIÓVESZTÉST ÉS HASONLÓ KÁROKAT), AMELY A PROGRAM HASZNÁLATÁBÓL, VAGY NEM HASZNÁLHATÓSÁGÁBÓL ADÓDIK, MÉG ABBAN AZ ESETBEN SEM, HA A VirusBuster Kft.-t TÁJÉKOZTATTÁK EZEN KÁROK FELMERÜLÉSÉNEK LEHETŐSÉGÉRŐL.

9. A megegyezés alapja

A fentebb leírt korlátozott jótállás, kizárólagos jogorvoslat és korlátozott felelősség alapvető elemei a megegyezésnek, mely a VirusBuster Kft. és Ön között jön létre. A VirusBuster Kft. csak jelen alapelvek alapján értékeseíti a Programot.

10. Kizárólag fogyasztó végfelhasználók

A jelen SZERZŐDÉSben foglalt korlátozások és kizárások a jótállással és felelősséggel kapcsolatban nem befolyásolhatják a fogyasztó törvényes jogait.

11. Általános rendelkezések

Jelen SZERZŐDÉS Magyarország jogrendszerén alapul. Jelen SZERZŐDÉS tartalmazza a szerződő felek teljes megegyezését és minden más írásbeli vagy szóbeli megegyezés felett áll. A végfelhasználói SZERZŐDÉSsel kapcsolatos kérdéseket a VirusBuster Kft. címére juttassa el.

A VirusBuster a VirusBuster Kft. bejegyzett védjegye Magyarországon és/vagy más országokban. Minden más elnevezés a megfelelő tulajdonosát illeti meg.

KAPCSOLAT

Jelen dokumentáció részletesen tárgyalja vírusvédelmi programunk működését, működtetését. Ennek ellenére, ha további kérdése van termékünkkel kapcsolatban, esetleg megosztaná velünk észrevételeit, javaslatait, kérjük lépjen kapcsolatba velünk. Bizalommal forduljon hozzánk az alábbi elérhetőségek egyikén! Kéréseit, megjegyzéseit, ötleteit szívesen fogadjuk.

Cím VirusBuster Kft.
Budapest 1518,
Pf. 54.
Magyarország

Telefon (+36) 1 382-7000

Fax (+36) 1 382-7007

Web <http://www.virusbuster.hu>

Támogatás <https://support.virusbuster.hu>

E-mail sales@virusbuster.hu

support@virusbuster.hu