



VirusBuster
for Samba Servers
1.2

TARTALOMJEGYZÉK

BEVEZETŐ	2
VIRUSBUSTER FOR SAMBA SERVERS	3
Rendszerkövetelmények.....	3
Minimálisan szükséges Linux disztribúciók	3
Támogatott Samba verziók	3
Telepítés, eltávolítás	4
Vírusvédelmi modulok üzembe helyezése	4
Beállítások a konfigurációs fájlban	6
Általános beállítások.....	6
Üzenetküldés	7
Üzenetekben használható tokenek.....	8
Regisztrációs adatok	8
Külső konfigurációs fájl beillesztése	8
VIRUSBUSTER SCAN DAEMON.....	9
Futtatható fájlok.....	9
Adatbázis frissítése.....	9
Konfigurációs fájlok	11
VÉGFELHASZNÁLÓI SZERZŐDÉS	17
KAPCSOLAT	18

BEVEZETŐ

A termékcsomagban a *VirusBuster for Samba Servers* és a *VirusBuster ScanDaemon* démon program együtt található meg.

A csomag elnevezése a következő:

```
vbsambashield-<vbsambashield-verzió>-<vbscand-verzió>-<oprendszer>.tgz
```

```
pl: vbsambashield-1.2.0-1.2.0-linux-i386.tgz
```

A csomagban található 'vbinst-pkg.pl' telepítő script segítségével telepítheti a vbsambashield és vbscand termékeket.

Telepítő fájl paraméterek:

```
--no-update
```

A telepítő ne frissítse a vbscand-t.

A telepítő először a vbscand-t próbálja meg telepíteni. Ha már van telepített vbscand a rendszerben, és az régebbi, mint a telepítendő változat, akkor a telepítő a korábbi verziót eltávolítja, az új verziót feltelepíti (amennyiben ez nincs letiltva a --no-update paraméterrel). A vbscand sikeres telepítése után a script a vbsambashield terméket telepíti, illetve frissíti.

VIRUSBUSTER FOR SAMBA SERVERS

A program Linux és Solaris operációs rendszerrel működő számítógépek Samba fájlserverének vírusvédelmét látja el a VirusBuster ScanDaemon segítségével. Teljes körű védelmet biztosít a rendszer számára, a fájlok elérésekor azonnali vírusellenőrzést hajt végre (on access védelem). A felhasználó szemszögéből teljesen transzparens módon látja el a védelmet, ellenőrzi a fájlokat.

A program alapvetően két modulból áll:

- shield modul, mely az ellenőrző funkciókat látja el
- vfsemu modul, mely a különböző Samba verziókhöz történő illesztést végzi

Rendszerkövetelmények

Támogatott operációs rendszerek:

- Linux i386/amd64
- Solaris 9 (sparc), 10 (i386)

Az összes platformon követelmény:

- 256 MB szabad memória
- 100 MB szabad háttértár kapacitás
- wget (frissítéshez)
- perl5 (telepítéshez)
- VirusBuster ScanDaemon telepítve

Platformonkénti követelmények:

- Intel Pentium (vagy kompatibilis) processzor 300 MHz-en (Linux, Solaris 10)
- Ultra Sparc IIe processzor 500 MHz-en (Solaris 9)
- Linux-on minimálisan: GLIBC 2.2.5, kernel 2.2.1

Minimálisan szükséges Linux disztribúciók

SuSE 8.0
RedHat 7.3
Debian 3.0 (woody)
Mandrake 9.0
Slackware 8.1

Támogatott Samba verziók

Samba 2.2.1 - 3.4.0

Megjegyzés:

Az itt feltüntetett legutolsó verziónál újabb verziók támogatása lehetséges, amennyiben azok VFS modul interfésze kompatibilis a korábbi verziókkal.

A 2.2.1-2.2.3 verziók csak abban az esetben támogatottak, ha a Samba démon binárisa exportált szimbólumokkal lett lefordítva.

A 3.0 alpha XY verziók nem támogatottak.

Telepítés, eltávolítás

A program tgz csomagban áll rendelkezésre:

Kicsomagolás:

```
tar -xzvf vbsambashield-<verzió>-<platform>.tgz
```

Telepítés: **vbsambashield-install.pl**

Eltávolítás: **vbsambashield-uninstall.pl**

Vírusvédelmi modulok üzembe helyezése

A védelem aktiválásához a Samba konfigurációs fájljának módosítása szükséges. Ez történhet automatikusan egy script segítségével, vagy manuálisan.

Automatikus üzembe helyezés

Futtassa le a következő scriptet, mely beregisztrálja a vírusvédelmi modult a Samba konfigurációs fájljának megfelelő szekcióiba:

```
usr/lib/vbsambashield/setup.sh
```

Paraméterezés:

```
-i --install
```

Beregisztrálja a vírusvédelmet a Samba konfigurációs fájlba.

```
-u --uninstall
```

Eltávolítja a vírusvédelem bejegyzéseit a Samba konfigurációs fájlból.

```
-c --config
```

Samba konfigurációs fájl megadása. Alapértelmezett: etc/samba/samba.conf

A nem kapcsoló paraméterek (nem kötőjellel kezdődőek) azoknak a share-eknek a megnevezései, melyekhez a védelmet hozzá szeretné rendelni, vagy eltávolítani. Ha nem ad meg share nevet, akkor az adott műveletet (install vagy uninstall) az összes létező share-en végrehajtja a script.

Példák:

```
setup.sh -i
```

Az összes share-en működni fog a vírusvédelem.

```
setup.sh -i share1 share2
```

A 'share1' és 'share2' share-eken fog működni a vírusvédelem.

```
setup.sh -u share2
```

Vírusvédelem megszüntetése a 'share2' share-en.

Manuális üzembe helyezés

A különböző verziók beállítása eltér egymástól:

2.x.y Samba verziók esetén:

```
vfs object = <vfs modul neve elérési útvonallal>  
(itt abszolút útvonalat kell megadni)
```

3.x.y Samba verzió esetén:

```
vfs objects = <vfs modul neve elérési útvonallal>
```

vagy
vfs objects = <vfs modul neve>

Ha már van paraméter meghatározva ehhez az opcióhoz, akkor a SambaShield -hez tartozó bejegyzést az eddigiekhez kell hozzáfűzni.

A fenti opciók megadhatók minden megosztásra általános érvényűen, vagy külön-külön is. Az általános érvényű megadáshoz a paramétereket a [global] szekcióban kell elhelyezni. Ellenkező esetben a vírusvédelem csak azokon a megosztásokon aktív, melyekben megtalálhatók a bejegyzések.

Példák a megadásra:
vfs object = /usr/lib/samba/vfs/vbsambavfsemu.so
vagy
vfs objects = vbsambavfsemu

A vírusvédelem csak a konfigurációs beállítások módosítása után keletkező kapcsolatokon lesz aktív, az azt megelőzőket nem érinti.

Beállítások a konfigurációs fájlban

A konfigurációs fájl a `/etc/vbsambashield/general.conf` útvonalon érhető el.

Beállítható opciók a [general] szekcióban

Általános beállítások

killable_action

Vírustalálatkor, irtható vírus esetén az itt beállított akció hajtódik végre a fájlban.

Beállítható értékek:

delete - fájl törlése

kill - vírus irtása

rename - fájl átnevezése

skip - incidens figyelmen kívül hagyása

Alapértelmezett: kill

non_killable_action

Vírustalálatkor, nem irtható vírus esetén az itt beállított akció hajtódik végre a fájlban.

Beállítható értékek:

delete - fájl törlése

rename - fájl átnevezése

skip - incidens figyelmen kívül hagyása

Alapértelmezett: skip

suspicious_action

Gyanús fájl esetén az itt beállított akció hajtódik végre a fájlban.

Beállítható értékek:

delete - fájl törlése

rename - fájl átnevezése

skip - incidens figyelmen kívül hagyása

Alapértelmezett: skip

scan_method

Keresés fajtájának beállítása.

Beállítható értékek: strict/fast/full

Alapértelmezett: strict

heuristic_level

Heurisztika szintjének beállítása.

Beállítható értékek:

normal - normál szint

off - heurisztika kikapcsolva

high - erős heurisztikus keresés

Alapértelmezett: normal

access_on_error

Hozzáférés engedélyezése/tiltása, ha hiba történt ellenőrzéskor.

Értékei: allow/deny

log_level

Naplózási szint beállítása.

Beállítható értékek:

EMERG vagy 0

ALERT vagy 1

CRIT vagy 2

ERR vagy 3
WARNING vagy 4
NOTICE vagy 5
INFO vagy 6
DEBUG vagy 7
DEBUG0 vagy 7
DEBUG1 vagy 8
DEBUG2 vagy 9
DEBUG3 vagy 10
DEBUG4 vagy 11
DEBUG5 vagy 12
DEBUG6 vagy 13
DEBUG7 vagy 14
DEBUG8 vagy 15
Alapértelmezett: INFO

file_log

Használjon-e napló-fájlt a program (yes/no).
Alapértelmezett: yes

log_path

Napló fájl-, és helyének megadása. A program működése közben keletkező üzeneteket tárolja.
Alapértelmezett: /var/log/vbsambashield/general.log

virus_log_path

Vírus-napló fájl-, és helyének megadása. A víruskeresés közben keletkező üzeneteket tárolja.
Alapértelmezett: /var/log/vbsambashield/VirusScan.log

samba_log

Naplózzon-e Samba napló-rendszeren keresztül (yes/no).
Alapértelmezett: yes

syslog

Syslog használata (yes/no).
Alapértelmezett: no

Üzenetküldés

message_sender = Samba Shield

Üzenet feladójának a neve.

message_virus_killed = "Üzenet"

Vírusirtás esetén elküldött üzenet. Idézőjelek között kell megadni, tokenek használhatók a szövegben.

message_access_denied = "Üzenet"

Üzenet, ha a vírus irtása nem sikerült. Idézőjelek között kell megadni, tokenek használhatók a szövegben.

Windows operációs rendszeren az üzenetek megjelenéséhez az alábbi beállításokra van szükség:

- nt alapú Windows esetén: Üzenetküldő/Messenger szolgáltatásnak futni kell
- Windows 9x esetén: valamilyen telepített hálózati üzenetkezelő alkalmazás (pl: Winpopup)

Üzenetekben használható tokenek

%virus%

Utoljára megtalált vírus neve.

%file%

Az ellenőrzött fájl neve.

%version%

SambaShield verziószáma.

Regisztrációs adatok

registration-username

Felhasználói név megadása.

registration-key

Regisztrációs kulcs megadása.

Külső konfigurációs fájl beillesztése

Lehetőség van egyéb konfigurációs fájlok beillesztésére a fő konfigurációs állományba. Ezek a külső fájlok a fő konfigurációs fájl részeként kerülnek feldolgozásra.

A kiegészítő konfigurációs fájl felépítése meg kell, hogy egyezzen a SambaShield konfigurációs fájljával, a beillesztés a @ jel utáni fájlnev megadásával történik.

Példa:

@messages.conf

Az alapértelmezett konfigurációs állományban a virustalálatkor küldendő üzenetek nyelvének egyszerű változtathatósága is e funkció kihasználásával történik. Az üzeneteket egy külső fájl tárolja, a kívánt nyelvnek megfelelőt kell beilleszteni a fő konfigurációs fájlba.

VIRUSBUSTER SCAN DAEMON

A VirusBuster ScanDaemon (a továbbiakban scandaemon) program a VirusBuster víruskereső motor teljes funkcionalitását teszi távolról elérhetővé unix vagy internet socketen keresztül a kliens számára. A csomagban található még egy parancssori kereső kliens (vbscan) is.

A scandaemon és a kliense(i) közötti kapcsolatot közös hálózati cím meghatározásával lehet kialakítani, melyet a kliens és a daemon konfigurációs fájljában (vagy paraméter útján) kell meghatározni. A scandaemon konfigurációs fájljában az 'address' opcióban kell megadni ezt a címet.

A kliens induláskor csatlakozik a már futó kereső démonhoz, amennyiben ez nem sikerül, azt hibaüzenettel jelzi.

Futtatható fájlok

Kereső daemon

vbscand [paraméterek]

-n, --nodaemon - nem démon módban indítás
-v, --version - verzió információk megjelenítése
-b, --build - részletesebb verzió információk
-c FILE, --config=FILE - konfigurációs fájl megadásának lehetősége
-p FILE, --pid_file=FILE - pid mentése meghatározott fájlba
-d FILE, --vdb_file=FILE - vdb leírófájl megadása
-a ADDR, --address=ADDR - a megadott címhez kapcsolódás
-k SEC, --conn_timeout=SEC - kapcsolódási időkorlát másodpercben
-r SEC, --read_timeout=SEC - olvasási időkorlát
-w SEC, --write_timeout=SEC - írási időkorlát

Kereső daemon init script (az /etc könyvtárban található) paraméterek

vbscand [paraméterek]

start - kereső démon indítása
stop - kereső démon leállítása
restart - kereső démon újraindítása
cfgreload - konfigurációs fájl újra betöltése
vdbreload - vírusadatbázis újratöltése

Parancssori kereső kliens

vbscan [paraméterek]

A rendelkezésre álló parancssori kapcsolók a konfigurációs fájl (vbscan.ini) leírásánál kerülnek részletezésre.

Adatbázis frissítése

A program által használt vírusadatbázis frissítése végrehajtható manuálisan, vagy a programcsomagban megtalálható frissítő script segítségével.

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 felhasználókhoz.

Automatikus frissítés

A folyamat automatizálására mellékelünk egy scriptet, mely a /usr/bin könyvtárba települ vbs_vdbupdate.sh néven.

A script elindítása után automatikusan letölti a vírusadatbázist, majd bemásolja a fájlt a megfelelő könyvtárstruktúrába és aktivizálja. Csak akkor hajtja végre a frissítést, ha a szerveren frissebb adatbázis található, mint az adott számítógépen. Ellenkező esetben az adatbázis változatlan marad.

A script indításához írja be a vbs_vdbupdate.sh parancsot. Lehetőség van paraméterek használatára is:

```
-f, --ftp      FTP frissítési forrás használata
-h, --http,    HTTP frissítési forrás használata
-v, --verbose, megjeleníti a letöltési folyamatot
--help,       használható paraméterek kiírása
```

Pl:

```
vbs_vdbupdate.sh -v --http
```

HTTP forrásról frissíti a vírusadatbázist és megjeleníti a letöltési folyamatot.

A script futtatásához szükség van a wget nevű programra! Cron segítségével időzítheti is az adatbázis frissítéseket, például állítsa be fél órás figyelésre: Jegyezze be a /etc/crontab-ba:

```
0,30 * * * * root /usr/bin/vbs_vdbupdate.sh
```

Manuális frissítés

A vírusadatbázis-készlet több fájlból áll ezek mindegyikének frissítése szükséges. A fájlok letölthetők FTP szerverünkről, a következő könyvtár teljes tartalmát töltse le és másolja be az adatbázis könyvtárba (/var/lib/vbuster):

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

Aktivizálja az új adatbázist a "vbscand vdbreload" paranccsal.

Konfigurációs fájlok

Scan daemon konfigurációs fájlja (vbscand.conf)

A konfigurációs fájl hierarchikus szerkezetben tárolja a beállításokat, és felépítése az egységbe zárás (encapsulation) elvét valósítja meg, azaz minden összetartozó beállítás-csoporthoz meg kell határozni a tárolási útvonalat lépésenként.

A konfigurációs fájlban az útvonalat (szekciók neveit) szögletes zárójelben kell feltüntetni:
[General]

A megjegyzésként beírt szöveg elé pontosvesszőt (;) kell tenni, a pontosvessző utáni karaktereket nem veszi figyelembe az értelmező.

A konfigurációs fájl alapértelmezetten az /etc/vbuster könyvtárban 'vbscand.conf' néven található.

Beállítható opciók a [General] szekcióban:

address=unix:/var/run/vbscand

Kereső démon hálózati cím.

Kétfajta socket típus támogatott: unix és internet socket.

unix socket: unix:<útvonal>

internet socket: inet:<szervernév vagy ip cím>:<port>

Alapértelmezett érték unix:/var/run/vbscand

vdb_file=/var/lib/vbuster/vdb.xml

Vírusadatbázis-leíró fájl elérési útvonala.

Alapértelmezett érték: /var/lib/vbuster/vdb.xml

pid_file=/var/run/vbscand.pid

Pid fájl elérési útvonala.

Alapértelmezett érték: /var/run/vbscand.pid

conn_timeout=1

read_timeout=180

write_timeout=1

Socket kommunikáció időkorlát-értékei másodpercben.

conn_timeout: kapcsolódási időlimit

read_timeout: olvasási időlimit

write_timeout: írási időlimit

Alapértelmezett érték mindhárom esetben 1 másodperc.

Parancssori kereső konfigurációs fájlja (vbscan.ini)

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.

A konfigurációs fájl alapértelmezetten az /etc/vbscan könyvtárban 'vbscan.ini' néven található.

Kapcsolat

--attach

Kereső démon hálózati címe.

Kétfajta socket típus támogatott: unix és internet socket.

unix socket: unix:<útvonal>

internet socket: inet:<szervernév vagy ip cím>:<port>

Pl: attach= unix:/var/run/vbscand

--engine

--vdb

Amikor nem a scandamon-hoz kapcsolódva használjuk a terméket, a fenti két opcióban kell megadni a víruskereső motor (engine), illetve a vírusadatbázis (vdb) leíró fájljának elérhetőségét.

pl: engine=/usr/lib/libvbengine.so

vdb=/var/lib/vbuster/vdb.xml

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 funkcionalításban 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 károkozó 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 felülbírálnak. Ügyeljen arra, hogy a konfigurációs fájlban relatív útvonallal megadott állományokat és könyvtárakat a program az aktuális könyvtárhoz képest 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.

-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 végrehajtott rekurzív 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 átvizsgálendő fájl- vagy könyvtár nevét (csak automatikus módban működik).

Ellenőrizendő fájltypusok

--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 kizárható 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 vírustalálat 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)

d - vissza nem állítható törlés (delete)

--remove-macro

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

-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 károsok, 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.

Fájl- és könyvtárhivatkozások

-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.

--log[=FILE]

A program üzeneteit a megadott fájlba is elmenti amellet, hogy a képernyőre is kiírja. Ha nincs megadva külön fájlnev (FILE), akkor az esetlegesen már meglévő 'vbscan.log' fájl végére fűzi az üzeneteket.

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 értékesíti 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