Doctor Web, Ltd.

Dr.Web® viirusetõrje Windows-ile

(95/98/Me/NT/2000/XP tööjaamadele ja NT/2000/2003 serveritele)

Väike kasutusjuhend

Versioon 4.33

Tarkvaras võib esineda edasisi parandusi ning täiendusi, mida ei ole kirjeldatud käesolevas juhendis. Selle juhendi täendatud ja parandatud versioonid on saadaval internetilehel http://www.drweb.com/

Käesolev juhend on koostatud seisuga 29.05.06.

Venemaa, Moskva – Saint Petersburg
http://www.drweb.com/

Sisukord

1. Sissejuhatus

1.1 Mille kohta see juhend on

Selles kasutusjuhendis on kõik vajalikud juhendid Dr. Web viirusetõrje Windows 95/98/Me/NT/2000/XP/2003-le installeerimiseks ning selle programmi tõhusaks kasutamiseks Sinu arvutis.

Programm on saadaval kahes variandis:

- Dr.Web Windows-i tööjaamadele 95/98/Me/NT/2000/XP (Dr.Web tööjaamadele)
- Dr.Web Windows-i NT/2000/2003 serveritele (Dr.Web serveritele)

Juhend kehtib mõlemale variandile, kui ei ole märgitud teisiti. Sellistel juhtudel on kasutatud Dr. Web toote lühendatud nimetust.

Dr.Web-i komponendid ja konfiguratsioonifailid serveritele mõeldud versioonis on spetsiaalselt välja töötatud, tagamaks tõhusat viirustevastast kaitset failiserverile. Selle versiooni väljatöötamisel on silmas peetud failiserveri suurt töökoormust, ööpäevaringset kasutust ning tihedat kasutajate vahelesekkumist (serveri administraator).

Dr.Web on võimas viirusetõrje programm ning saavutab sõltumatutes võrdlustes regulaarselt parimaid tulemusi.

Viirusetõrje oluliseks tunnuseks on tema moodulite arhitektuur. Viirusetõrje kasutab programmimootorit ja viiruste andmebaase, mis on kõikidel erinevatel programmiosadel ja –versioonidel ühised. Praegusel hetkel on lisaks Dr.Web Windows-ile ka viirusetõrje versioonid DOS, OS/2, Novell NetWare jaoks ja mitmetele Unix-põhistele süsteemidele (Linux, FreeBSD, jne.).

Lisaks sellele on saadaval ka spetsiaalne programm Dr. Web Enterprise Suite – see on mõeldud viirustevastase kaitse haldamise

koondamiseks ettevõtetes. Selle programmi kohta leiad rohkem informatsiooni Lisas B.

Dr.Web kasutab mugavat ning tõhusat programmimoodulite ja viiruste andmebaaside uuendamist Interneti kaudu.

Dr.Web tuvastab ja eemaldab arvutist ka mitmeid erinevaid soovimatuid programme (reklaamvara, helistajad, naljaprogrammid, riskvara, muukprogrammid). Nende avastamiseks ning eemaldamiseks kasutatakse Dr. Web-i standardseid viirusetõrjekomponente.

Dr.Web Windows-ile sisaldab järgnevaid komponente:

- Dr.Web Skänner Windows-ile – graafilise kasutajaliidesega viirusetõrje skänner. Programm käivitub kas kasutaja nõudmisel või vastavalt ajagraafikule ning kontrollib arvutit viiruste suhtes. Samuti on saadaval käsurea versioon (Dr.Web Konsoolskänner Windows-ile)
- SpIDer Guard Windows-ile – viirusetõrje valvur (nimetatakse ka monitoorijaks). Programm töötab pidevalt arvuti mälus ning kontrollib faile "lennult", samuti tuvastab ka viirusaktiivsust.
- SpIDer Mail Windows-i tööjaamadele – e-posti viirusetõrje valvur. Programm võtab üle kõikide arvutis olevate meiliklientide pöördumised meiliserverite poole protokollidega POP3/SMTP/IMAP4/NNTP (IMAP4 on nagu IMAPv4rev1), tuvastab ja teeb kahjutuks meiliviirused enne need saabumist serverist meilikliendile või enne, kui sõnum saadetakse meiliserverisse. See komponent ei sisaldu paketis Dr.Web serveritele.
- Dr.Web Automaatse uuendamise tööriist Windowsile – võimaldab registreerunud kasutajatel saada programmimoodulite ning viiruste andmebaaside uuendusi ning installeerib need automaatselt;

registreerimata kasutajatel võimaldab tööriist registreerida või saada demo võtmefail (loe allpool).

Dr.Web tööjaamadele sisaldab ka Planeerijat Windowsile ning DOS-skännerit.

Juhend kirjeldab Dr.Web-i installeerimist ning sisaldab mõningaid näpunäiteid selle kohta, kuidas kasutada programmi viiruste poolt põhjustatud tüüpiliste probleemide lahendamisel. Enamasti on kirjeldatud programmi komponentide standardsed käitumisviisid (vaikimisi sätetes).

Lisades on välja toodud detailsem informatsioon edasijõudnud kasutajatele viirusetõrje seadistamiseks.

1.2 Terminid ja lühendid

Kasutusjuhendis kasutatakse järgnevaid termineid (Tabel 1).

Tabel 1. Leppemärkide tähendused

Leppemärk	Kommentaarid
 Pane tähele	Oluline märkus või juhend
 Tähelepanu	Hoiatus potentsiaalselt ohtliku situatsiooni või vea tegemise ohu puhul
Valvur	Termini selgitus või viide selgitusele
`Katkesta`	Nuppude, lehtede, menüüpunktide ning teiste programmi elementide nimetused
`[F1]`	Klaviatuuri klahvide nimetused
`C:\Windows\system`	Failide ja kataloogide nimetused

Juhendis kasutatakse ilma edasiste selgitusteta järgnevaid lühendeid:

- OS – operatsioonisüsteem
- GUI – graafiline kasutajaliides (Graphical User Interface), programmi GUI-versioon – versioon, mis kasutab GUI-d

1.3 Dr.Web® nõuded operatsioonisüsteemile, arvutile ning kasutaja oskustele

Sõltuvalt valitud komponentide arvust, on Dr. Web-i installeerimiseks vajaminev vaba kõvakettamaht kuni 20 MB.

Skänner (GUI-versioon ja konsoolversioon Windows-ile) ja SpIDer Guard valvur töötavad arvutites, mille OS-ks on Windows 95/98/Me või Windows NT/2000/XP/2003. Pane tähele, et SpIDer Guard töötab ainult 32-bitistes süsteemides.

Programmi töötamine Windows 95-ga on võimalik alates Windows 95 OSR2 (v.4.00.950B). Samuti võib sellisel juhul vaja minna teatud süsteemikomponentide installeerimist, mida saab alla laadida Microsoft-i kodulehelt. Programm annab nende vajadusel info komponentide nimede ning URL-de kohta.

DOS-skänner töötab MS-DOS-is või Windows-i käsureal.

Minimaalsed nõuded süsteemile ühilduvad OS nõuetega süsteemile. Arvuti peab täielikult toetama i80386 protsessori käskude süsteemi.

Sa peaksid installeerima OS tootja poolt soovitatavad turvapaigad. Kui tootjapoolset toetust OS-le enam ei võimaldata, peaksid sa OS versiooni värskendama.

Enne Dr.Web-i installeerimist tuleb arvutist eemaldada kõik teised viirusetõrjeprogrammid, et vältida nende residentsete komponentide võimalikku sobimatust Dr.Web-iga.

Enne Dr.Web versiooni 4.32 või uuema installeerimist tuleb arvutist eemaldada versioonile 4.32 eelnenud versioonid.

1.4 Litsentsi võtmefail

Kasutaja õigused viirusetõrje kasutamisel on reguleeritud spetsiaalse faili abil, mida nimetatakse *võtmefailiks*. Võtmefail sisaldab järgnevat informatsiooni:

- Komponentide nimekiri, mida kasutajal on lubatud kasutada
- Ajavahemik, mille jooksul viirusetõrje kasutamine on litsentseeritud
- Muud piirangud (näiteks arvutite arv, milles on lubatud viirusetõrjet kasutada)

Võtmefail on laiendiga `key` ning fail peab asuma vaikimisi installeerimiskataloogis (loe p. 2.1, mis kirjeldab installeerimise viimast etappi).

Võtmefailil on kirjutuskaitstud formaat ning seetõttu ei tohi seda redigeerida. Võtmefaili redigeerimine muudab selle kehtetuks. Seetõttu ei ole soovitatav võtmefaili tekstiredaktoriga avada, mis võib põhjustada selle rikkumise.

Kasutajad, kes ostavad viirusetõrje Doctor Web-i sertifitseeritud partneritelt, saavad *litsentsi võtmefaili*. Võtmefaili parameetrid, mis määravad kasutaja õigused, on vastavuses litsentsilepinguga. Fail sisaldab ka kasutaja ning müüja andmeid.

Programmi proovikasutamiseks on olemas *demo võtmefailid*. Need failid võimaldavad põhiliste viirusetõrje komponentide täisfunktsionaalset kasutamist, kuid seda piiratud aja jooksul.

Võtmefail saadetakse `key` laiendiga failina või zip-arhiivina, milles sisaldub eelpool nimetatud fail; see võidakse saata ka spetsiaalse formaadiga failina, millel on `dwz` laiend. Seda kasutatakse uuendamise paketi saatmise puhul.

Kasutaja saab võtmefaili ühel viisil järgmistest:

- Pärast viirusetõrje registreerimist Doctor Web Ltd. kodulehel. Litsentsi võtmefail moodustub kasutaja poolt sisestatud *registreerimise seerianumbri* põhjal, mille kasutaja saab müüjalt. Kui seerianumbrit pole sisestatud, saab kasutaja ainult demo võtmefaili. Genereeritud võtmefail saadetakse e-posti kaudu; samuti saab seda alla laadida registreerimise leheküljelt.
- Interneti kaudu installeerimise viimasel etapil (loe p. 2.1) või programmi esmasel uuendamisel (loe p. 4) automaatse uuendamise tööriista abil. Tööriist registreerib programmi Doctor Web, Ltd. kodulehel ning saab ja installeerib registreerimise käigus moodustatud võtmefaili. See protseduur on võimalik ainult versiooniga Dr.Web tööjaamadele.
- See on lisatud viirusetõrje müügipakendisse.
- See saadetakse kasutajale e-posti kaudu failina laiendiga `dwz`. Sellisel juhul tuleb kasutajal võtmefaili installeerimiseks teha hiirega topeltklõps sõnumile lisatud faili ikoonil.
- See on eraldi andmekandjal `key` laiendiga failina. Sellisel juhul tuleb fail kopeerida Dr. Web-i installeerimiskataloogi.

- See on zip-arhiivina, milles on `key` laiendiga fail. Fail tuleb vastava arhiiveerijaga lahti pakkida (näiteks WinZip või Pkunzip) ning paigutada installeerimiskataloogi.

Kui kehtivat võtmefaili ei leita (litsentsi või demo), blokeeritakse kõikide programmi komponentide töö. Ainsaks võimalikuks toiminguks on automaatse uuendamise tööriista käivitamine (loe p. 4) registreerimiseks ja võtmefaili saamiseks (ainult Dr.Web tööjaamadele puhul).

Alates versioonist 4.33 on Dr.Web tööjaamadele ja Dr.Web serveritele võtmefailid erinevad. Kui kasutada teise variandi võtmefaili, blokeeritakse osade komponentide töö (näiteks SpIDer Guard XP).

Soovitatav on säilitada võtmefaili kuni selle aegumiseni. Kui viirusetõrje taasinstalleerida või installeerida see mitmesse arvutisse, pole seerianumbri uuestiregistreerimine nõutav. Sellisel juhul saab kasutada esmasel registreerimisel saadud võtmefaili. Kui võtmefail on kadunud, tuleb kasutajal uuesti registreeruda. Sel juhul sisesta esmasel registreerimisel sisestatud personaalsed andmed – muuta võib ainult e-posti aadressi – ja võtmefail saadetakse sinu e-posti aadressile.

Päringute arv võtmefaili saamiseks on piiratud – üks kasutaja saab seerianumbrit registreerida mitte rohkem kui 25 korda. Kui lubatud päringute arv on ületatud, siis võtmefaili ei saadeta. Võtmefaili saamiseks pöördu Tehnilise toe osakonna poole http://support.drweb.com/request/ (saates päringut, kirjelda täpselt tekkinud olukorda ning teata esmase registreerimise käigus sisestatud personaalsed andmed ning registreerimise seerianumber). Võtmefail saadetakse Tehnilise toe osakonna poolt e-posti kaudu.

2. Dr.Web® viirusetõrje installeerimine

Dr.Web tööjaamadele esmakordne installeerimine on kirjeldatud p. 2.1.

Dr.Web serveritele esmakordne installeerimine on kirjeldatud p. 2.2.

Installeerimise iseärasustest arvutites, kuhu on juba eelnevalt installeeritud viirusetõrje versioon 4.32 või uuemad, on lähemalt kirjutatud p. 2.3. Seal on ka soovitused vajaduse tekkimisel programmi eemaldamiseks arvutist.

2.1 Dr.Web® tööjaamadele esmakordne installeerimine

See lõik kirjeldab ainult Dr.Web tööjaamadele installeerimist; Dr.Web serveritele installeerimine on kirjeldatud p. 2.2.

Enne programmi installeerimist soovitame kindlasti:

- Installeerida arvutis kasutatavale operatsioonisüsteemile kriitilised värskendused, mis on välja lastud Microsoft-i poolt (värskendusi saab Microsoft-i kodulehelt http://windowsupdate.microsoft.com)
- Kontrollida süsteemi utiliitidega failisüsteemi ning eemaldada avastatud vead
- Sulgeda aktiivsed rakendused

Sa peaksid enne installeerimise alustamist eemaldama arvutist kõik teised viirusetõrjeprogrammid.

Enne Dr.Web versiooni 4.32 või uuema installeerimist tuleb arvutist eemaldada Dr.Web viirusetõrje versioonid 4.31 ja eelnevad.

Installeerimiskomplekt on saadaval "Dr.Web viirusetõrje" plaadina või eraldi `exe`-failina suurusega 8-10 MB.

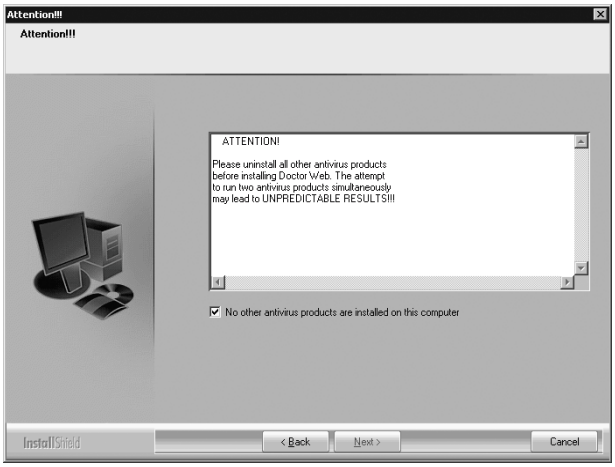
Dr.Web viirusetõrje installeerimiseks arvutisse:

- Käivita fail, kui viirusetõrje programm on eraldi failina
- Kui viirusetõrje programm on plaadil, algab installeerimise protseduur automaatselt kohe pärast plaadi sisestamist seadmesse (kui on võimaldatud automaatkäivitus). Kui automaatkäivitus on keelatud, käivita `autorun.exe` fail. Avaneb automaatkäivituse menüüga aken. Vajuta nuppu `Installeeri`

Järgi installatsiooniviisardi juhiseid. Kõikidel installeerimise etappidel (enne failide kopeerimist sinu arvutisse) saad sa naasta eelnevate etappide juurde. Selleks vajuta nuppu `Back`. Installeerimise katkestamiseks vajuta nuppu `Cancel`, jätkamiseks vajuta nuppu `Next`.

Viirusetõrje installeerimiseks arvutisse, mille OS-ks on Windows NT/2000/XP, peavad kasutajal olema administraatori õigused.

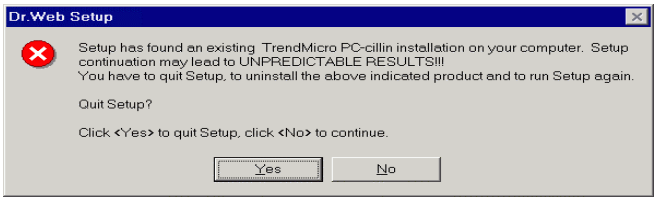
1. Vali installatsiooniprogrammi kasutajaliidese keel (see valik ei mõjuta Dr.Web viirusetõrje kasutajliidese keele valikut).
2. Installatsiooniprogramm informeerib sind Dr. Web-i sobimatuse ning ka teiste installeeritud viirusetõrjeprogrammide puhul ja soovitab need arvutist eemaldada (pilt 1).



Pilt 1. Hoiatus teise viirusetõrjeprogrammi eemaldamise vajalikkuse kohta

Juhul, kui sinu arvutisse on installeeritud mõni teine viirusetõrjeprogramm, on soovitatav vajutada nuppu `Cancel` ning lõpetada installeerimise protsess. Eemalda või deaktiveeri teine viirusetõrjeprogramm ning pärast seda võid jätkata Dr. Web-i installeerimist oma arvutisse. Installeerimise jätkamiseks märgi linnuke ruutu `No other antivirus products are installed on this computer` ees ning vajuta `Next`.

3. Installeerimisprogramm kontrollib sinu arvutit ning leides mõne talle teadaoleva viirusetõrjeprogrammi, genereerib programm vastava hoiatusteate (pilt 2).



Pilt 2. Hoiatusteade: arvutist on leitud teine viirusetõrjeprogramm

Installeerimise katkestamiseks vajuta `Yes` (sa saad installeerimist jätkata pärast tuvastatud viirusetõrjeprogrammi eemaldamist või deaktiveerimist), installeerimise jätkamiseks vajuta `No`.

Installeerimisprogramm ei tuvasta kõiki viirusetõrjeprogramme.

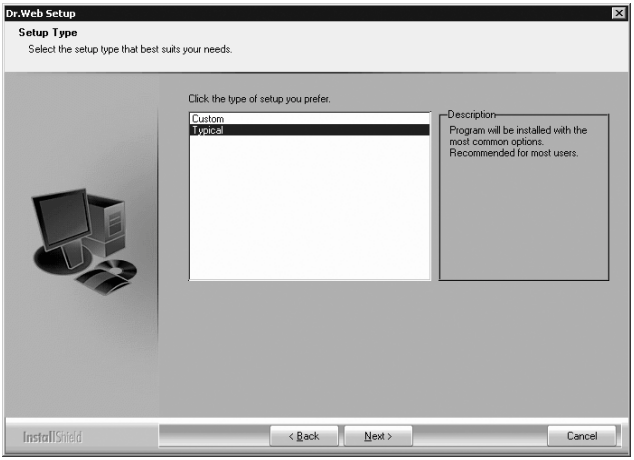
Sa võid installeerimist jätkata ainult juhul, kui sinu arvutisse installeeritud teisel viirusetõrjeprogrammil ei ole hetkel ühtegi aktiivset residentset moodulit (valvurit) ega meililiiklust töötlevat programmi.

4. Järgmisel sammul palutakse sul läbi lugeda Litsentsileping. Installeerimise jätkamiseks pead sa selle aksepteerima.
5. Järgmisel etapil kuvab installeerimisprogramm hoiatusteate võtmefaili (litsentsi- või demo-) vajalikkuse kohta. Kui võtmefail on olemas sinu arvuti kõvakettal või eemaldataval andmekandjal, vajuta `Browse` ja vali see fail avanevas failide sirvimise standardaknas. Kui sul võtmefaili pole, vajuta `Next`. Võtmefaili saamine toimub sellisel juhul hiljem, installeerimise käigus.

   Kasuta ainult Dr.Web tööjaamade jaoks mõeldud võtmefaile (loe hoiatust p. 1.4 lõpus).

   Võtmefail on `key` laiendiga. Kui võtmefail on arhiivis, paki arhiiv vastava arhiveerijaga lahti.

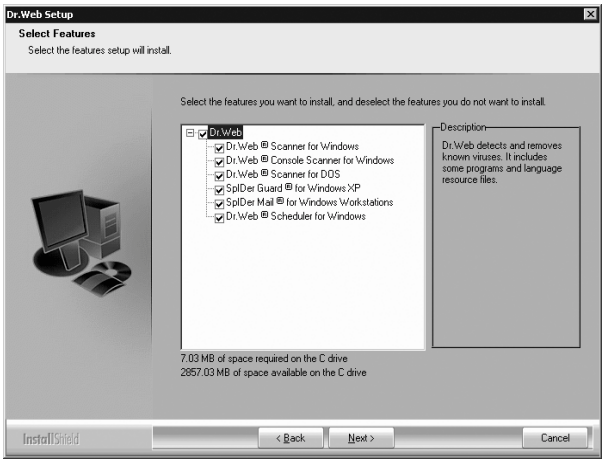
6. Järgmisel etapil tuleb valida installeerimiskataloog.
7. Programm palub valida installeerimismooduse (pilt 3). Vali nimekirjas olevast kahest moodusest üks (`Typical` või `Custom`) ja vajuta `Next`.



Pilt 3. Installatsioonimooduse valimine

Variant `Typical` installeerib viirusetõrjeprogrammi komponendid, kasutajaliidese keeled (eesti ja inglise või vene ja inglise) ning samuti ka mõned täiendavad programmid.

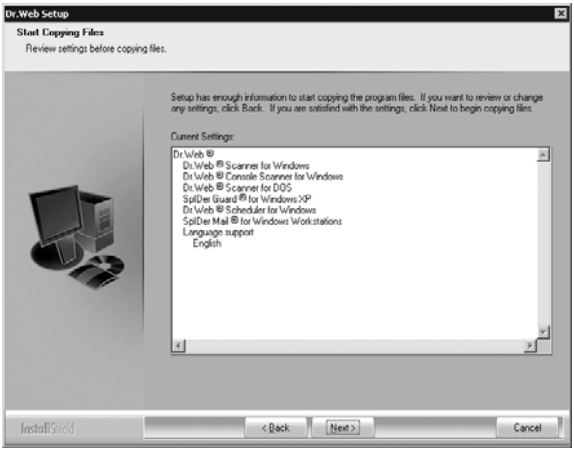
8. Kui valisid kohandatava installeerimismooduse, avaneb `Select Features` aken (pilt 4).



Pilt 4. Komponentide valimine

Märgi nimekirjas olevate komponentide kõrval asuvad ruudukesed, kui soovid vastavaid komponente installeerida. Võta märgistus maha nende komponentide kõrval olevatest ruutudest, mida sa ei soovi installeerida. Vajuta `Next`.

9. Järgmisena palutakse sul valida kataloog Windows-i peamenüü alammenüüs `Program's` (avaneb `Start` nupu vajutamisel), kuhu paigutatakse installeeritud komponentide, abifailide, logifailide ikoonid ja `Uninstall Dr.Web`, mille abiga saad hiljem vajadusel programmi arvutist eemaldada. Vaikimisi loob installatsiooniprogramm kausta `Dr.Web`. Soovitame seda mitte muuta.
10. Avaneb aken `Start Copying Files` (pilt 5). Loe läbi sätete nimekiri ning kui kõik sobib, vajuta `Next`.



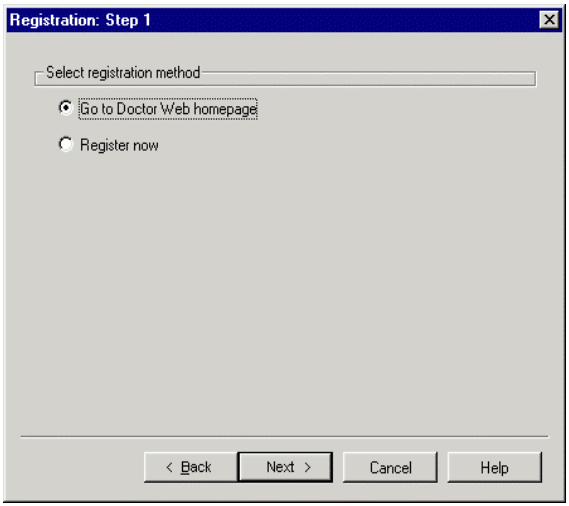
Pilt 5. Algab failide kopeerimine

11. Seejärel avaneb `Proxy server setting` aken. Kui kasutad Interneti ligipääsuks proksiserverit, täida väljad `Address`, `Name` ja `Password` ning vajuta `Next`. Muul juhul vajuta `No`.

Pilt 6. Proksiserveri sätted

12. Kui sul on võtmefail olemas ning oled täpsustanud selle asukoha (loe käesoleva peatüki punkti 5), küsitakse järgmises aknas, kas soovid viiruste andmebaase uuendada. Infot viiruste andmebaaside ning nende uuendamise kohta leiad kasutusjuhendi punktist 4. Viiruste andmebaaside uuendamiseks vajuta `Yes`. Käivitub automaatse uuendamise tööriist.

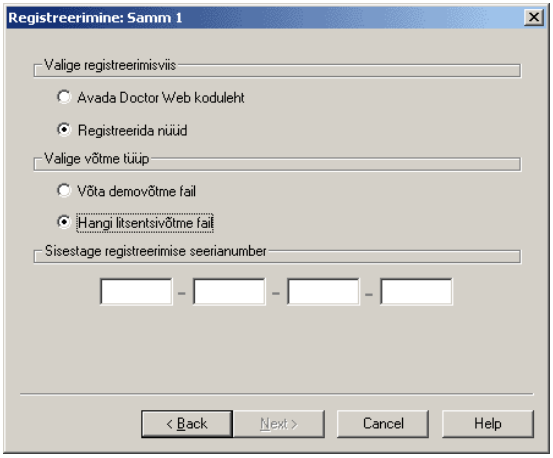
    Kui installatsioonipakett pole varustatud litsentsi võtmefailiga, informeerib automaatse uuendamise tööriist sind sellest ning üritab seda saada interneti kaudu kasutaja registreerimise protseduuri abil. Võtmefaili saamise esimesel sammul pakutakse sulle võimalust kas alustada registreerimist või minna täiendava informatsiooni saamiseks veebileheküljele www.drweb.com (pilt 7).



Pilt 7. Registreerimise alustamine

Registreerimise alustamiseks vali `Registreerida nüüd` ja vajuta `Next`.

Järgmisena vali saadava võtmefaili tüüp – demo või litsentsi võtmefail (pilt 8).



Pilt 8. Võtmefaili tüübi valimine

Kui said programmi ostmise hetkel registreerimise seerianumbri, vali raadionupp `Hangi litsentsi võtmefail` ees.

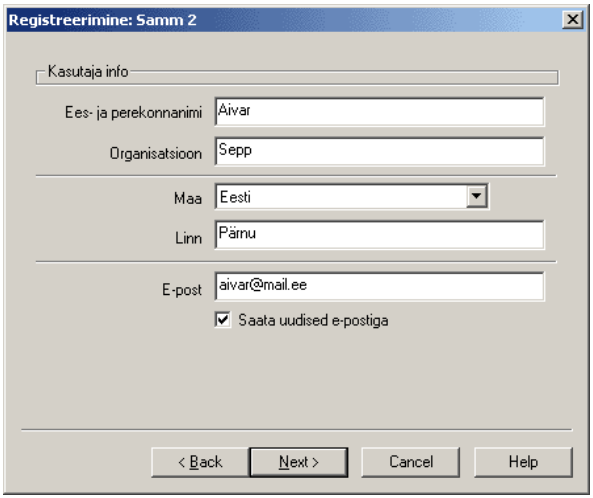
Sellisel juhul võid sa eelmisel etapil tehtud valiku viiruste andmebaaside uuendamise kohta tühistada või katkestada selle käesoleval etapil, vajutades `Cancel` ning uuendada viiruste andmebaasid hiljem, pärast litsentsi võtmefaili installeerimist.

Kui installeerisid programmi proovikasutamiseks, vali `Võta demo võtmefail`.

13. Kui valisid litsentsi võtmefaili saamise, sisesta seerianumber väljale `Sisesta registreerimise seerianumber` ning vajuta `Next`.

Sa saad registreerida ainult Doctor Web, Ltd. poolt välja antud seerianumbreid. Kõik seerianumbrid on formaadiga xxxx-xxxx-xxxx-xxxx, ehk nad koosnevad neljast sümbolite grupist ning kõik grupid on üksteisest eraldatud miinusmärgiga. Näiteks: E2E4-KH2A-7BVX-D8R6. Kui sinu seerianumber näeb välja teistsugune (näiteks OEM-xxx, DVD-xxx, 3DRWEB), on selle registreerimiseks vajalik külastada seerianumbri väljastanud firma veebilehekülge või kontakteeruda nende tehnilise toe osakonnaga. Näiteks DialogueScience, Inc. genereerib oma formaadiga seerianumbreid (http://www.antivir.ru/, reg@antivir.ru).

14. Sõltumata võtmefaili tüübi valikust (kas litsentsi või demo) avaneb kasutaja personaalsete andmete sisestamise aken (pilt 9).



Pilt 9. Kasutaja personaalsete andmete sisestamine

Täida aknas olevad väljad ning vajuta `Next`.

Algab võtmefaili allalaadimine ning installeerimine. Protseduuri kohta kuvatakse info vastavas aknas.

Pärast võtmefaili saamist uuendatakse viiruste andmebaasid ning see toiming ei nõua kasutajapoolset sekkumist.

Kui installeerimiseks valiti GUI-skänner, skaneerib programm kohe pärast installeerimise lõppemist arvuti töömälu ning käivitusfaile ja pakub võimalust teostada kogu arvuti detailne skaneerimine.

Kui installeeriti SpIDer Guard viirusetõrje monitoorija või SpIDer Mail, palub programm arvuti taaskäivitamist, mis on vajalik installeerimise lõpuleviimiseks.

Vaikimisi installeerib installeerimisprogramm ka Ülesannete planeerija Windows-ile ning koostab ajagraafikud programmi uuendamiseks igal tunnil ja lisab viirusetõrje skaneerimise ülesande. Loe sellest lähemalt punktis p. 3.6.

2.2 Dr.Web® Windows NT/2000/2003 serveritele esmakordne installeerimine

See lõik kirjeldab ainult Dr.Web serveritele installeerimist; Dr.Web tööjaamadele installeerimine on kirjeldatud p. 2.1.

Enne programmi installeerimist soovitame kindlasti:

- Installeerida arvutis kasutatavale operatsioonisüsteemile kriitilised värskendused, mis on välja lastud Microsoft-i poolt (värskendusi saab Microsoft-i kodulehelt http://windowsupdate.microsoft.com)

- Kontrollida süsteemi utiliitidega failisüsteemi ning eemaldada avastatud vead

Sa peaksid enne installeerimise alustamist eemaldama arvutist kõik teised viirusetõrjeprogrammid.

Serveritele mõeldud viirusetõrjeprogrammi installeerimiseks peavad kasutajal olema administraatori õigused.

Installeerimiskomplekt on saadaval "Dr.Web viirusetõrje" plaadina või eraldi `exe`-failina suurusega 8-10 MB.

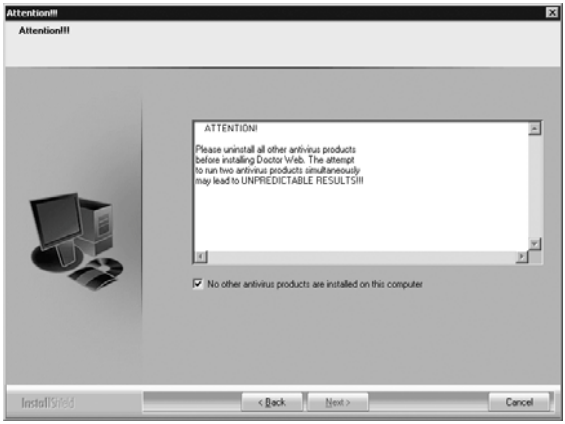
Dr.Web viirusetõrje installeerimiseks arvutisse:

- Käivita fail, kui viirusetõrje programm on eraldi failina
- Kui viirusetõrje programm on plaadil, avaneb kohe pärast plaadi sisestamist seadmesse (kui on võimaldatud automaatkäivitus) plaadi automaatkäivituse menüü. Vali `Sirvi CD` (või `Sirvi DVD`) Ning mine kataloogi `WindowsServer`. Kui automaatkäivitus on keelatud, mine kataloogi OS standardtööriistade abil. Seejärel käivita selles kataloogis asuv exe-fail.

Järgi allpool kirjeldatud installatsiooniviisardi juhiseid. Kõikidel installeerimise etappidel (enne failide kopeerimist sinu arvutisse) saad sa naasta eelnevate etappide juurde. Selleks vajuta nuppu `Back`. Installeerimise katkestamiseks vajuta nuppu `Cancel`, jätkamiseks vajuta nuppu `Next`.

1. Vali installatsiooniprogrammi kasutajaliidese keel (see valik ei mõjuta Dr.Web viirusetõrje kasutajliidese keele valikut).
2. Installatsiooniprogramm informeerib sind Dr. Web-i sobimatuse ning ka teiste installeeritud

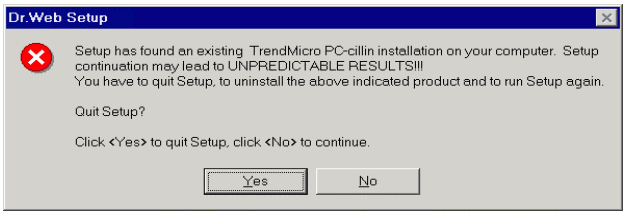
viirusetõrjeprogrammide puhul ja soovitab need arvutist eemaldada (pilt 10).



Pilt 10. Hoiatus teise viirusetõrjeprogrammi eemaldamise vajalikkuse kohta

Juhul, kui sinu arvutisse on installeeritud mõni teine viirusetõrjeprogramm, on soovitatav vajutada nuppu `Cancel` ning lõpetada installeerimise protsess. Eemalda või deaktiveeri teine viirusetõrjeprogramm ning pärast seda võid jätkata Dr. Web-i installeerimist oma arvutisse. Installeerimise jätkamiseks märgi linnuke ruutu `No other antivirus products are installed on this computer` ees ning vajuta `Next`.

3. Installeerimisprogramm kontrollib sinu arvutit ning leides mõne talle teadaoleva viirusetõrjeprogrammi, genereerib programm vastava hoiatusteate (pilt 11).



Pilt 11. Hoiatusteade: arvutist on leitud teine viirusetõrjeprogramm

Installeerimise katkestamiseks vajuta `Yes` (sa saad installeerimist jätkata pärast tuvastatud viirusetõrjeprogrammi eemaldamist või deaktiveerimist), installeerimise jätkamiseks vajuta `No`.

Installeerimisprogramm ei tuvasta kõiki viirusetõrjeprogramme.

Sa võid installeerimist jätkata ainult juhul, kui sinu arvutisse installeeritud teisel viirusetõrjeprogrammil ei ole hetkel ühtegi aktiivset residentset moodulit (valvurit) ega meililiiklust töötlevat programmi.

4. Järgmisel sammul palutakse sul läbi lugeda Litsentsileping. Installeerimise jätkamiseks pead sa selle aksepteerima.
5. Järgmisel etapil kuvab installeerimisprogramm hoiatusteate võtmefaili (litsentsi- või demo-) vajalikkuse kohta. Kui võtmefail on olemas sinu arvuti kõvakettal või eemaldataval andmekandjal, vajuta `Browse` ja vali see fail avanevas failide sirvimise standardaknas. Kui sul võtmefaili pole, vajuta `Registreeri` (nõuab aktiivse internetiühenduse olemasolu). Avaneb Doctor Web, Ltd. veebilehel asuv registreerimise aken. Täida ära kasutajavorm, sisesta viirusetõrjeprogrammi müüjalt saadud registreerimise seerianumber ning lae võtmefail alla.

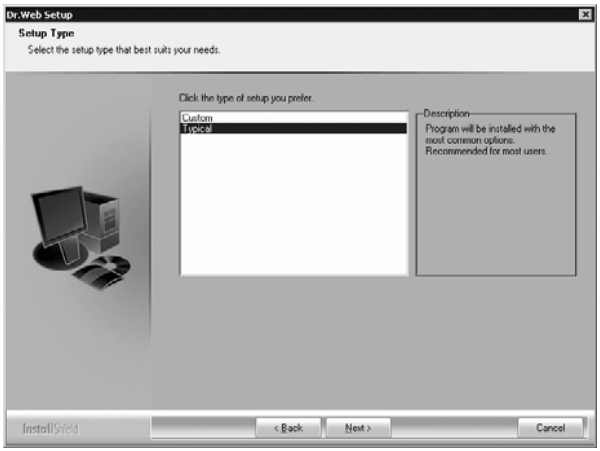
Sa saad registreerida ainult Doctor Web, Ltd. poolt välja antud seerianumbreid. Kõik seerianumbrid on formaadiga xxxx-xxxx-xxxx-xxxx, ehk nad koosnevad neljast sümbolite grupist ning kõik grupid on üksteisest eraldatud miinusmärgiga. Näiteks: E2E4-KH2A-7BVX-D8R6. Kui sinu seerianumber näeb välja teistsugune (näiteks OEM-xxx, DVD-xxx, 3DRWEB), on selle registreerimiseks vajalik külastada seerianumbri väljastanud firma veebilehekülge või kontakteeruda nende tehnilise toe osakonnaga. Näiteks DialogueScience, Inc. genereerib oma formaadiga seerianumbreid (http://www.antivir.ru/, reg@antivir.ru).

Kui registreerimine on hetkel võimatu, vajuta `Next`. Sellisel juhul pead sa võtmefaili hankima hiljem (loe p. 1.4) ning tõstma selle viirusetõrje installatsioonikataloogi.

Kasuta ainult Dr. Web serveritele jaoks mõeldud võtmefaili (loe hoiatust p. 1.4 lõpus).

Võtmefail on `key` laiendiga. Kui võtmefail on arhiivis, paki arhiiv vastava arhiveerijaga lahti.

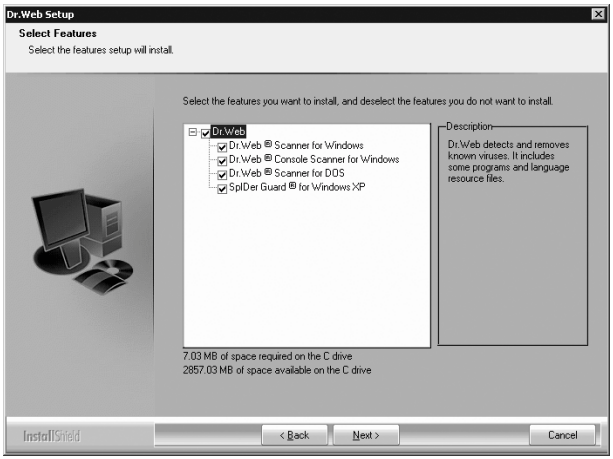
6. Järgmisel etapil tuleb valida installeerimiskataloog.
7. Programm palub valida installeerimismooduse (pilt 12). Vali nimekirjas olevast kahest moodusest üks (`Typical` või `Custom`) ja vajuta `Next`.



Pilt 12. Installeerimismooduse valimine

Variant `Typical` installeerib kõik viirusetõrjeprogrammi komponendid ja kasutajaliidese keeled.

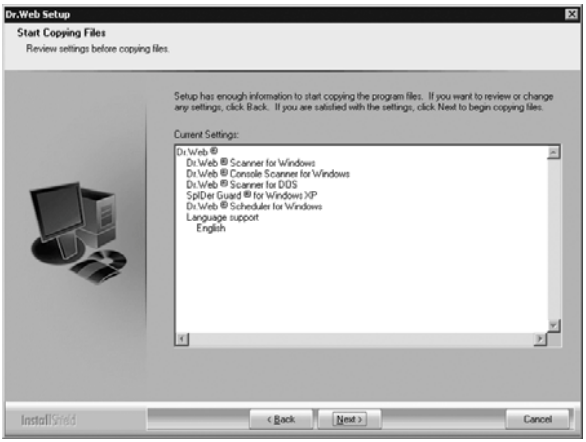
8. Kui eelmisel sammul tehti valik Custom, avaneb aken `Select Features` (pilt 13).



Pilt 13. Komponentide valimine

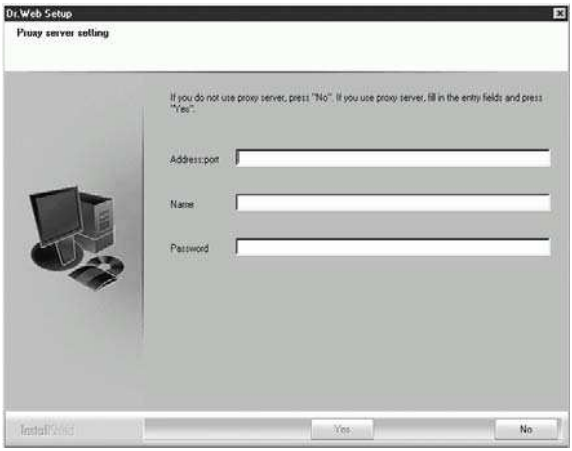
Märgi nimekirjas olevate komponentide kõrval asuvad ruudukesed, kui soovid vastavaid komponente installeerida. Võta märgistus maha nende komponentide kõrval olevatest ruutudest, mida sa ei soovi installeerida. Vajuta `Next`.

9. Järgmisena palutakse sul valida kataloog Windows-i põhimenüü alammenüüs `Program's` (avaneb `Start` nupu vajutamisel), kuhu paigutatakse installeeritud komponentide, abifailide, logifailide ikoonid ja `Uninstall Dr.Web`, mille abiga saad hiljem vajadusel programmi arvutist eemaldada. Vaikimisi loob installatsiooniprogramm kausta `Dr.Web`. Soovitame seda mitte muuta.
10. Avaneb aken `Start Copying Files` (pilt 14). Loe läbi sätete nimekiri ning kui kõik sobib, vajuta `Next`.



Pilt 14. Algab failide kopeerimine

11. Seejärel avaneb `Proxy server setting` aken. Kui kasutad Interneti ligipääsuks proksiserverit, täida väljad `Address`, `Name` ja `Password` ning vajuta `Next`. Muul juhul vajuta `No`.



Pilt 15. Proksiserveri sätted

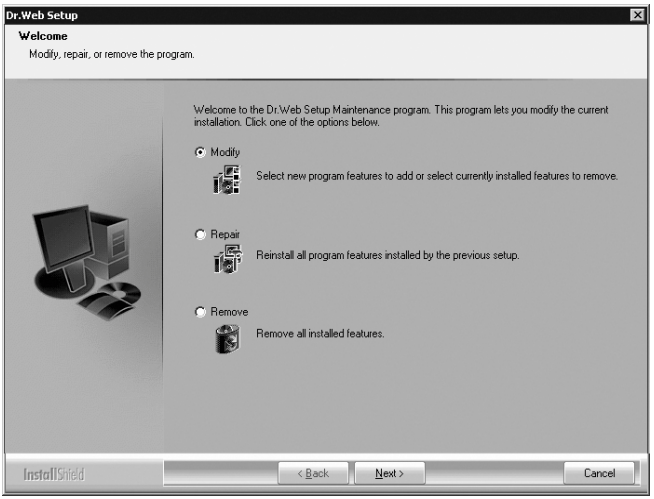
12. Järgmises aknas küsitakse, kas soovid viiruste andmebaase uuendada. Infot viiruste andmebaaside ning nende uuendamise kohta leiad kasutusjuhendi punktist 4. Viiruste andmebaaside uuendamiseks vajuta `Yes`. Käivitub automaatse uuendamise tööriist.
13. Kui installeerimiseks valiti GUI-skänner, skaneerib programm kohe pärast installeerimise lõppemist arvuti töömälu ning käivitusfaile ja pakub võimalust teostada kogu arvuti detailne skaneerimine.

Kui installeeriti SpIDer Guard viirusetõrje monitoorija, palub programm arvuti taaskäivitamist, mis on vajalik installeerimise lõpuleviimiseks.

Viirusetõrje installeerimisel arvutisse, mille OS on Windows 2000/2003 Server, loob programm süsteemi graafikusse viirusetõrje automaatse uuendamise ülesande (`Scheduled Tasks` kataloogis). Rohkem infot loe p. 3.7.

2.3 Programmi taasinstalleerimine ja eemaldamine

Kui arvutisse on Dr.Web juba installeeritud, erineb installatsiooniprogrammi käitumine mõnevõrra tavalisest. Installatsiooniprogrammi käivitamisel ilmub aken programmi tegutsemisviisi valikuks (pilt 16 näitab valikut Dr.Web tööjaamadele puhul, Dr. Web serveritele valikuaken on sarnane).



Pilt 16. Installeerimismooduse valik

Installeeritud komponentide koosseisu muutmiseks vali `Modify`. Avaneb aken `Select Features` (vt. pilt 13) ning järgnevad sammud on samasugused, nagu eelpool alates sellest aknast kirjeldatud.

Eelnevalt valitud komponentide uuesti installeerimiseks (näiteks vajadusel parandada rikutud faile) vali `Repair`. Edasine installeerimine ei nõua kasutajapoolset sekkumist.

Kõigi installeeritud komponentide eemaldamiseks vali `Remove`.

Eelpool kirjeldatud aken avaneb ka `Add/Remove Programs (Lisa/eemalda programme)` tööriistaga Windows-i Control Panel-is (juhtpaneelis).

3. Töö alustamine

3.1 Installeeritud komponentide sätted ja funktsioonid

Installatsiooniprogramm installeerib arvutisse vaikimisi järgmised viirusetõrjeprogrammi komponendid:

- Installeerides viirusetõrje tööjaamadele – skänneri Windows-keskkonnale (GUI-liidese ja konsoolskänneriga), skänneri DOS-ile, valvuri ja meilivalvuri ning Planeerija
- Installeerides viirusetõrje serveritele – skänneri Windows-keskkonnale (GUI-liidese ja konsoolskänneriga) ja valvuri

Automaatse uuendamise tööriist ning mõned teised täiendavad tööriistad installeeritakse kohustuslikus korras.

Kõik viirusetõrjeprogrammi komponendid kasutavad skaneeritavates objektides viiruste tuvastamiseks ja neutraliseerimiseks ühiseid viiruste andmebaase ning samu algoritme.

Vaatamata sellele erineb aga objektide valik skaneerimiseks; see võimaldab programmi eri komponente kombineerituna kasutades saada täiesti erilise ning üksteist täiendava kaitsevahendi arvutile.

Näiteks skaneerib *Skänner Windows-ile* (kasutaja nõudmisel või vastavalt Planeerijale) kindlaksmääratud faile (kõik failid, valitud loogilised kettad, kataloogid jne.). Vaikimisi skaneeritakse ka arvuti töömälu ning käivitusfaile. Kuna ülesande täitmise alustamine on kasutaja otsustada, ei pea muretsema arvuti jõudluse vähenemise pärast teiste tähtsate protsesside täitmisel.

Skänner DOS-ile suudab teostada detailset skaneerimist isegi siis, kui Windows pole installeeritud või selle töö on blokeeritud. Kõrgeima taseme viiruste tuvastamisel failides tagab skänneri käivitamine kaitstud kettalt arvuti käivitamisel.

Valvur püsib pidevalt arvuti töömälus ning võtab üle kõik failisüsteemi pöördumised objektide poole. Programm kontrollib viiruste suhtes ainult avatavaid faile (kui kasutada vaikimisi sätetega, siis kontrollitakse kõiki avatavaid faile eemaldatavatel andmekandjatel ning kõvakettale kirjutamiseks avatavaid faile). Tänu tasakaalustatud failisüsteemi detailse skameerimise meetodile ei sega programm peaaegu üldse teiste programmide tööd arvutis. Seetõttu küll väheneb veidi viiruste tuvastamise usaldusväärsus, kuid seda siiski tähtsusetul määral.

Programmi üheks eeliseks on kahtlemata tema katkematu töö kogu arvuti töötamise ajal. Lisaks tuvastab valvur teatud viiruseid ainuüksi nende tegevuse eripärade järgi.

Meilivalvur püsib pidevalt arvuti mälus. Programm võtab üle kõikide meiliklientide pöördumised sinu arvutist meiliserveritesse POP3/SMTPIMAP4/NNTP protokollidega ning skaneerib sissetulevaid (või väljaminevaid) sõnumeid enne nende vastuvõtmist (või saatmist) meilikliendi poolt. Erinevalt SpIDer Guard-ist ning skänneritest on SpIDer Mail kujundatud kontrollima antud hetkel sinu arvutis toimuvat liiklust. Selle tulemusena on postkastide kontrollimine tõhusam ning kulutab vähem ressursse. Näiteks võimaldab programm kontrolli all hoida viiruse poolt tehtavaid katseid ussviiruse koopiaid sisaldavate kirjade masspostituseks kasutaja aadressiraamatus olevatele meiliaadressidele. Samuti võimaldab selle programmi olemasolu arvutis blokeerida meilifailide kontrollimise SpIDer Guard-i poolt, mis säästab omakorda süsteemi ressursse.

Viirusetõrjeprogrammi maksimaalse tõhususe tagamiseks soovitame sul kasutada Dr. Web-i komponente alljärgnevalt:

- Skaneeri arvuti failisüsteemi detailse skaneerimise vaikimisi (maksimaalsete) sätetega
- Säilita valvuri automaatkäivitus ning muud vaikimisi sätted

- Lase meilivalvuril skaneerida kõiki sõnumeid
- Teosta aegajalt (vähemalt korra nädalas, kohe pärast viiruste andmebaaside uuendamist) kogu arvuti skaneerimine
- Teosta koheselt kogu arvuti skaneerimine, kui valvur oli ajutiselt blokeeritud ning arvuti oli ühendatud internetti või arvutisse laaditi faile irdketastelt

Kaitse viiruste vastu on efektiivne siis, kui pead sammu viiruste andmebaaside ning muude programmifailide uuendustega (soovitav on uuendada igal tunnil). Lähemalt loe p. 4.

Detailsemalt on Dr.Web-i komponentide kasutamisest kirjutatud järgmistes osades.

3.2 Dr.Web® Skänner Windows-ile kasutamine

3.2.1 Skänneri käivitamine. Üldine informatsioon

Skänner installeeritakse tavalise Windows-i rakendusena ning see käivitub kasutaja käsu peale (või Planeerija käsu peale, loe p. 3.6). Skänneri käivitamiseks kasuta järgnevaid vahendeid:

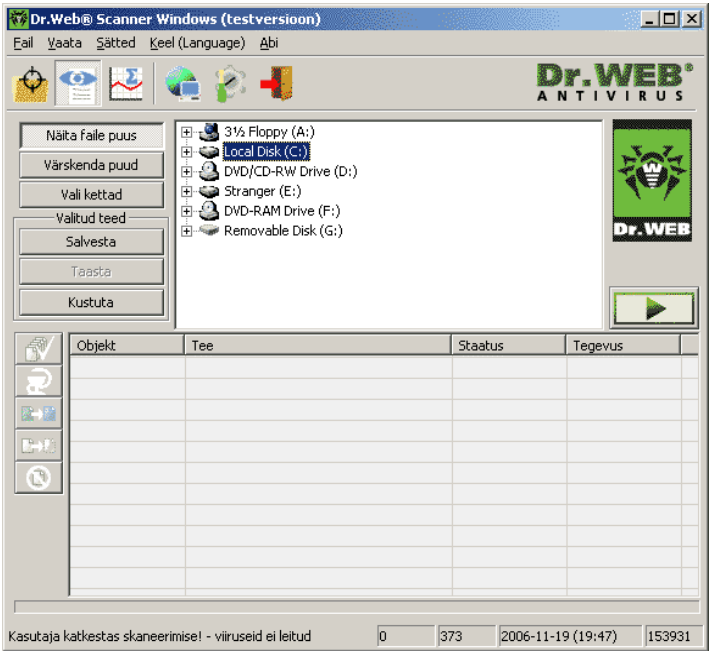
- Skänneri ikooni arvuti töölaual
- tegumiribal asuva SpIDer Guard-i ikooni kontekstmenüüd (loe p. 3.4.1)
- tegumiribal asuva SpIDer Mail-i ikooni kontekstmenüüd (loe p. 3.5.1)
- `Dr.Web Scanner` menüüpunkti `Dr.Web` kaustas, mis asub Windows-i peamenüüs (avaneb `Start` nupu vajutamisel)
- Windows-i käsurida (loe p. 3.3)

Programmi käivitamisel avaneb programmi peaaken (pilt 17).

Vaikimisi sätete kohaselt võid sa käivitada skännerit faili või kataloogi kontrollimiseks ka ühel viisil järgnevatest:

- Vali `Kontrolli Dr.Web-iga` faili või kataloogi kontekstmenüüst (Töölaual või Windows Explorer-is)
- Lohista faili või kataloogi ikoon hiirega skänneri ikooni peale või skänneri Peaaknasse

Valitud objekti skaneerimine algab koheselt.

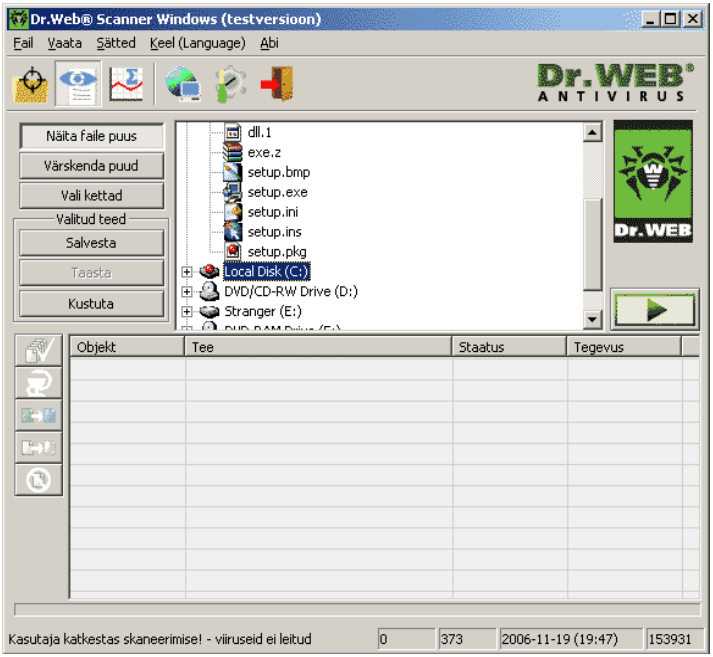


Pilt 17. Skänneri Peaaken

Vaikimisi käivitub kohe pärast programmi avamist arvuti mälu ning Windows-i käivitusfailide skaneerimine.

Teisi failisüsteemi objekte skaneeritakse kasutaja nõudmisel. Failisüsteem on näha skänneri akna keskosas hierarhilise puuna. Puud on võimalik avardada mistahes kataloogi mistahes tasemeni. Kui isegi sellest ei piisa, vajuta `Näita faile puus`.

Vali puus objektid, mida soovid skaneerida. Pildil 18 on skaneerimiseks valitud kogu loogiline ketas `C:` ja üks failidest disketil.



Pilt 18. Skänneri Peaaken skaneerimiseks valitud objektidega

Kõikide konfiguratsioonifailis märgitud ketaste valimiseks (ScanHDD, ScanFDD, ScanCD, ScanNet parameetrid, vaikimisi – kõik kõvakettad), vajuta nuppu `Vali kettad`.

Valitud objektide skaneerimise alustamiseks vajuta  peaakna paremas osas.

Skaneerimise käivitumisel ilmub nupp  akna paremasse osasse. Kontrollimise peatamiseks vajuta seda nuppu. Sel juhul

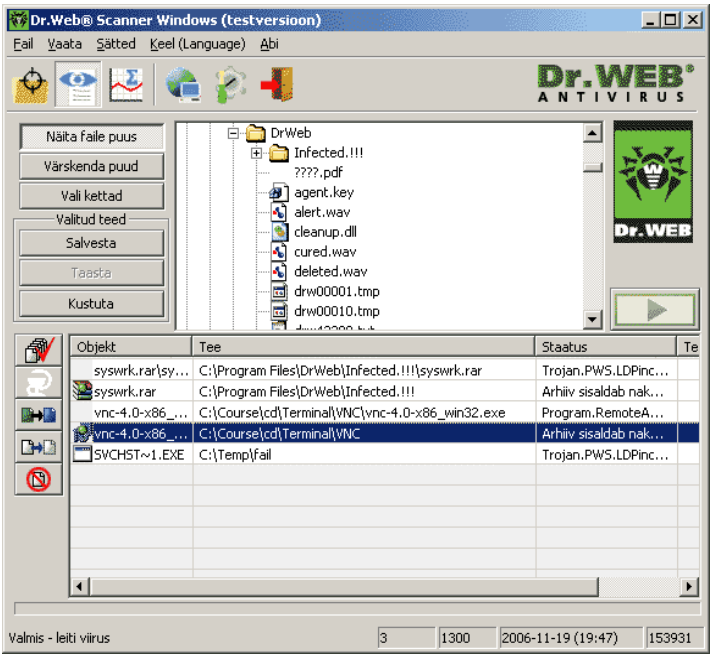
võtab nupp kuju  . Vajuta nuppu kontrollimise jätkamiseks Vajuta  kontrollimise katkestamiseks.

Vaikimisi skaneeritakse ka valitud kataloogide ja loogiliste ketaste alamkatalooge ning samuti ka nende ketaste buutsektoreid, millel valiti vähemalt üks kataloog või fail. Samuti skaneeritakse ka vastavate füüsiliste ketaste põhilisi buutsektoreid.

Skaneerimiseks tehtud valiku salvestamiseks (samade objektide kontrollimiseks tulevikus), vajuta `Salvesta` alal `Valitud teed`; varem valitud objektide valiku taastamiseks vajuta `Taasta`.

Vaikimisi skaneerib programm kõiki faile, kasutades nii viiruste andmebaase kui ka heuristilist anaalüsaatorit (meetod, mis võimaldab tuvastada programmile tundmatuid viiruseid nende loomise üldiste põhimõtete varal). Käivitatavad failid, mis on pakitud spetsiaalsete arhiveerijate poolt, pakitakse skaneerimise ajal lahti, kontrollitakse kõiki faile enimkasutatavates arhiivides (Zip, Arj, Lha, Rar jpt.), failikonteinerites (PowerPoint, RTF jt.) ja samuti meiliprogrammide postkastides (kirjade formaat peab vastama RFC822-le).

Versioon Dr.Web tööjaamadele kuvab vaikimisi kasutajale viiruse või kahtlase objekti leidmisel informatsiooni akna allosas asuvas spetsiaalses aruandeväljas (pilt 19). Dr.Web Windows serveritele teostab vaikimisi vajalikud toimingud viirusohu kõrvaldamiseks. Loe p. 3.2.3.



Pilt 19. Skänneri Peaaken koos aruandeväljaga

3.2.2 Toimingud viiruse avastamisel

Töötades vaikimisi sätetega, Dr.Web tööjaamadele ainult raporteerib nakatunud või kahtlaste objektide leidmise puhul. Sa saad programmi kasutada nakatunud objekti funktsionaalsuse taastamiseks (*paranda* see) ning selle toimingu ebaõnnestumise puhul ohu eemaldamiseks.

Selleks:

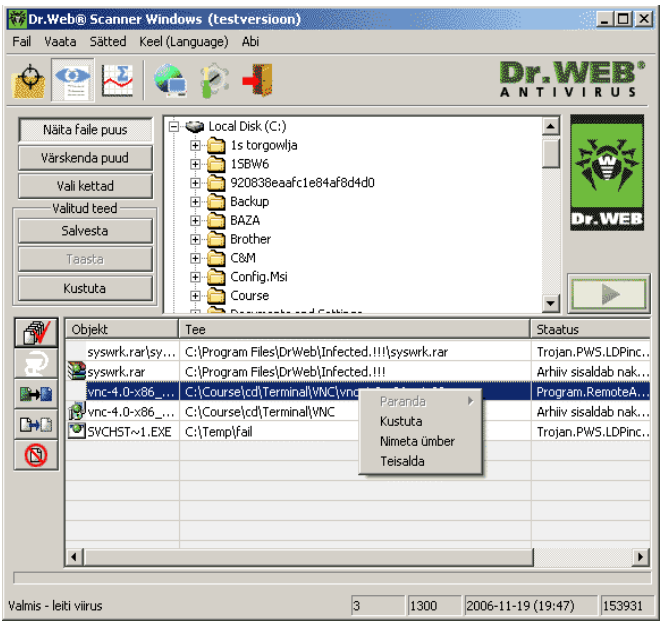
1. Klõpsi parema hiireklahviga aruandenimekirjas rida nakatunud objekti kirjeldusega.

Sa saad määrata toimingud kõikidele objektidele või ainult osadele objektidele aruandenimekirjas. Kõikide objektide valimiseks vajuta nuppu  .

Aruandenimekirjas asuvate objektide valimiseks kasuta täiendavalt järgmisi klahve või klahvide kombinatsioone:

- `Insert` – vali objekt ning liiguta kursor järgmisele positsioonile
- `Ctrl+A` – vali kõik
- nupp `*` numbriklaviatuuril – inverteeri valik

2. Vali avanenud kontekstmenüüs toiming, mida soovid teostada või vajuta vastavale nupule, mis asub aruandeväljast vasakul: (pilt 20).



Pilt 20. Toimingute valik nakatunud objektidega

3. Kui valid toimingu `Paranda`, tuleb valida veel üks toiming, mis teostatakse juhul, kui parandamine peaks ebaõnnestuma.

Ümbernimetamine tähendab faililaiendi asendamist teisega. Vaikimisi asendatakse laiendi esimene sümbol sümboliga `#`.

Teisaldamise puhul tõstetakse fail kausta, mis on määratud programmi sätetes; vaikimisi on see `infected.!!!` alamkataloog programmi installeerimiskataloogis.

Kahtlased failid, mis tõsteti karantiini, tuleks saata analüüsimiseks Doctor Web, Ltd. viirusetõrje laborisse. Seda saab teha läbi spetsiaalse veebivormi, mis asub http://support.drweb.com/sendnew/. Sellele veebilehele kiiresti minemiseks vali `Saada kahtlane fail` programmi menüüs `Abi` avanevas nimekirjas `Tugi`.

Kahtlaste objektide puhul on parandamine võimatu.

Objektide, mis ei ole failid (buutsektorid), teisaldamine, ümbernimetamine ning kustutamine ei ole võimalik.

Ükski toiming ei ole teostatav failidele, mis asuvad arhiivides, konteinerites või meilisõnumite manustena.

Kui toiming `Kustuta` on vaikimisi võimaldatud failiarhiividele, konteineritele või postkastidele, kuvab programm enne nende kustutamist hoiatuse andmete kadumise võimalikkuse kohta.

Pärast valitud toimingu teostamist kuvatakse aruandeakna tulbas `Tegevus` toimingu teostamise tulemus.

Kui leitakse nakatunud või kahtlane fail, mida kasutab mõni teine 32-bitine Windows-i rakendus, ei saa valitud toimingut koheselt teostada. Aruandeakna tulbas `Tegevus` kuvatakse sõltuvalt valitud toimingust tekst `Parandatakse pärast arvuti taaskäivitamist` või `Kustutatakse pärast arvuti taaskäivitamist`. Toiming teostatakse pärast järgmist arvuti taaskäivitamist e. toiming on edasi lükatud. Seetõttu on selliste objektide leidmisel soovitatav teostada kohe pärast skaneerimist arvuti taaskäivitamine.

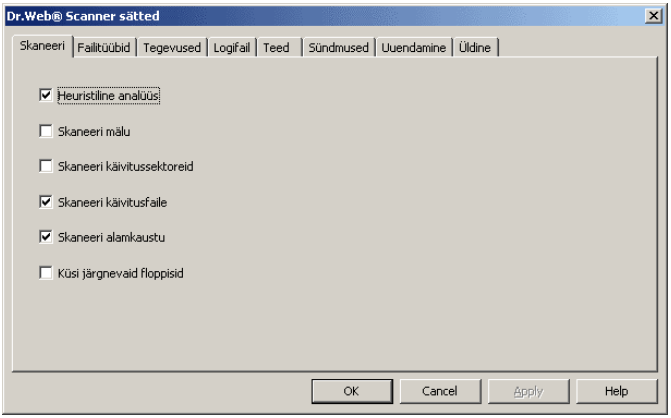
Detailne aruanne programmi tööst salvestatakse logifailina; vaikimisi asub see fail programmi installeerimiskataloogis ning selle nimi on `drweb32w.log`.

3.2.3 Programmi parameetrite seadistamine

Programmi vaikimisi sätted on enamuste rakenduste jaoks optimaalsed ning ilma vastava vajaduseta ei tasuks neid muuta.

Programmi sätete muutmiseks:

1. Vali punkt `Sätted` programmi põhimenüüs ning seejärel vali avanevas menüüs `Muuda sätteid`. Avaneb aken mitmete lehtedega, kus saab muuta sätteid (pilt 21).



Pilt 21. Sätete aken

2. Tee vajalikud muudatused ning vajuta `Apply` järgmisel lehel muudatuste tegemiseks.
3. Igal lehel kirjeldatud sätete kohta rohkema informatsiooni saamiseks kasuta nuppu `Help`. Enamikel lehtedel määratavatel sätetel on ka kiire abiteksti võimalus – selleks tuleb hiire parema klahviga klikkida vastaval sättel ning seejärel kuvab programm lühida abiteksti.
4. Kui oled redigeerimise lõpetanud, vajuta `OK` muudatuste salvestamiseks või `Cancel` tehtud muudatuste salvestamise katkestamiseks.

Vaikimisi sätetes kõige sagedamini tehtavad muudatused on kirjeldatud allpool.

Dr.Web tööjaamadele vaikimisi sätted on optimaalsed skaneerimiseks kasutaja nõudmisel. Programm teostab valitud objektide täis- ning detailse skaneerimise, teavitab kasutajat kõikidest nakatunud ning kahtlastest objektidest, jättes kasutajale õiguse otsustada, milliseid toiminguid peaks programm nende avastamisel ette võtma. Eelnev ei kehti ainult objektide kohta, mis

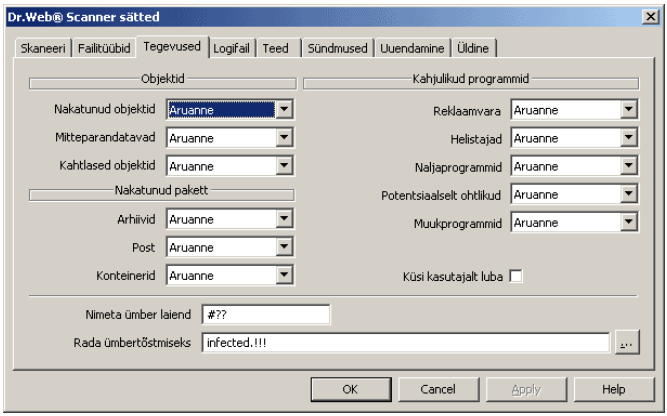
sisaldavad naljaprogramme, riskvara või muukvara: nende jaoks on vaikimisi määratud `Ignoreeri`.

Skaneerimise läbiviimiseks ilma kasutaja osavõtuta saab määrata sätteid programmi automaatseks reageerimiseks nakatunud objektide avastamisel.

Dr.Web Windows-i serveritele teostab vaikimisi toimingud viirusohu ärahoidmiseks automaatselt.

Programmi reaktsioonide määramiseks nakatunud objektide avastamisel:

1. Vali sätete aknas leht `Tegevused` (pilt 22).



Pilt 22. Tegevuste leht (Dr.Web tööjaamadele)

2. Vali rippmenüüs `Nakatunud objektid` programmi tegevus nakatunud objekti avastamisel.

Valik `Paranda` on automaatse reziimi puhul kõige parem. See toiming on vaikimisi määratud programmis Dr.Web serveritele.

3. Vali rippmenüüs `Parandamatud objektid` programmi tegevus ravimatu objekti avastamise puhul. Toimingu valikud

nende objektide puhul on samasugused, nagu eelpool kirjeldatud; erinev on ainult see, et toimingut `Paranda` ei saa valida.

Valik `Teisalda` on enamikel juhtudel parim. See toiming on vaikimisi määratud programmis Dr.Web serveritele.

4. Vali rippmenüüs `Kahtlased objektid` programmi tegevus kahtlase objekti avastamisel (sama, nagu eelpool kirjeldatud).

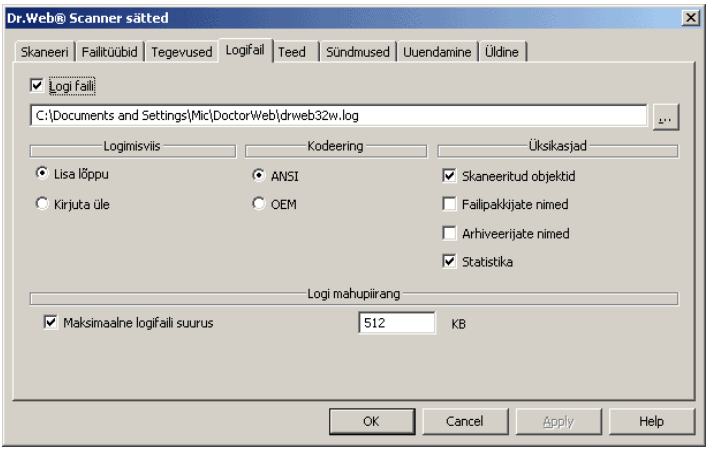
Dr.Web tööjaamadele puhul on soovitatav jätta tominguks `Aruanne`. Dr.Web serveritele puhul on soovitatav jätta toiminguks vaikimisi määratud toiming `Teisalda`.

5. Samasugused toimingud tuleks ka määrata reklaamvara, helistajaid, naljaprogramme, riskvara ning muukvara sisaldavate objektide avastamise puhul.
6. Samamoodi seadistatakse programmi automaatsed toimingud viiruste või kahtlaste koodide avastamisel ka failiarhiivides, konteinerites ning postkastides. Sellistel puhkudel rakendab programm toimingud kogu objektile. Programmis Dr.Web tööjaamadele on vaikimisi määratud toiming `Aruanne`. Programmis Dr.Web serveritele on vaikimisi kõikidel sellistel juhtudel määratud toiming `Teisalda`.
7. Võta märgistus maha `Küsi kasutajalt luba` eest, et võimaldada programmil teostada määratud toiminguid ilma eelnevalt luba küsimata.
8. Kui programmi toiminguks on määratud ümbernimetamine, asendab programm vaikimisi faili laiendi esimese sümboli

sümboliga #. Vajadusel saad sa seda muuta. Selleks sisesta vajalik väärtus sisestusväljale `Nimeta laiend ümber`.

9. Kui programmi toiminguks on määratud teisaldamine, tõstab programm faili vaikimisi programmi installeerimiskataloogi alamkataloogi `infected.!!!`. Vajadusel saad määrata mõne teise kataloogi sisestusväljal `Tee ümbertõstmiseks`.

Lehel `Logifail` (pilt 23) saad seadistada logifaili parameetreid.



Pilt 23. Leht Logifail

Enamus vaikimisi seadistatud parameetreid tuleks säilitada. Siiski võid hiljem muuta logifaili detailsuse astet (vaikimisi logitakse kogu informatsioon nakatunud või kahtlaste objektide kohta; informatsioon pakitud failide või arhiivide skaneerimise ning edukalt lõppenud skaneerimise kohta jäetakse logimata).

Sa saad määrata kõikide failide skaneerimise tulemuste logimise, sõltumata skaneerimise tulemustest. Selleks märgi ruuduke `Skaneeritud objektid` ees (see säte suurendab märgatavalt logifaili suurust).

Sa saad ka määrata arhiveerijate nimede logimise (märgi ruuduke `Arhiveerijate nimed` ees), või käivitatavate failide pakkijate nimede logimise (märgi ruuduke `Failipakkijate nimed` ees).

Sa võid tühistada vaikimisi seatud piirangu logifaili maksimaalsele suurusele (võta märgistus maha `Maksimaalne logifaili suurus` eest), või määrata sinu enda poolt soovitud logifaili suuruse piirangu, sisestades selle märkeruudu kõrval asuvasse sisestusvälja.

Vaikimisi asub logifail Windows 95/98/Me puhul programmi installatsioonikataloogis, Windows NT/2000/XP/2003 puhul kataloogis `%USERPROFILE%\DrWeb`

3.3 Skaneerimine käsurealt

Sa saad käivitada Dr.Web Skänneri Windows-ile ka käsurealt. See meetod võimaldab määrata käesoleva skaneerimise sätteid ning skaneeritavate objektide loendit nende parameetrite järgi. See meetod võimaldab ka skänneri automaatse väljakutse vastavalt ajagraafikule.

Käsurealt käivitamise süntaks on järgmine:
`[path_to_program]drweb32w [objects] [keys]`

Dr.Web Skänner Windows-ile asemel võib kasutada Dr.Web Konsoolskännerit. Sellisel juhul kirjuta `drweb32w` asemele käsunimi `drwebwcl`.

Sama on võimalik ka Dr.Web Skänner DOS-ile puhul (käsunimi `drweb386`). Kõik failinimed ning teed tuleb kirjeldada vormingus, mis on arvutis olevale OS-le vastav (näiteks on lubatud ainult lühikesed failinimed). See komponent ei kuulu Dr.Web serveritele koosseisu.

Nimekiri skaneeritavate objektide kohta võib olla tühi või sisaldada mitut üksteisest tühikutega eraldatud elementi.

Kõige levinumad variandid objektide määramisel skaneerimiseks on kirjeldatud allpool:

- `*` – skaneeri kõiki kõvakettaid
- `C:` – skaneeri ketast `C:`
- `D:\games` – skaneeri kataloogis olevaid faile
- `C:\games\*` – skaneeri kõiki faile kataloogis `C:\games` ja selle alamkataloogides

Parameetrid – käsurea võtmed, mis kirjeldavad programmi sätteid. Kui ühtegi võtit pole määratud, viiakse skaneerimine läbi eelnevalt määratud sätetega (või vaikimisi sätetega, kui sa pole neid muutnud).

Iga parameeter algab sümboliga `/`, võtmed eraldatakse üksteisest tühikutega.

Mitmed enamkasutatavad võtmed on kirjeldatud allpool. Kõikide võtmete kirjeldused leiad Lisast D.

`/cu` – nakatunud objektide parandamiseks.

`/icm` – parandamatute failide teisaldamiseks (vaikimisi määratud kataloogi),
`/icr` – ümbernimetamiseks (vaikimisi).

`/qu` – skänneri akna sulgemiseks pärast sessiooni lõppu.

`/go` – programmi poolt esitatavate küsimuste keelamiseks.

Kaks viimast parameetrit on eriti kasulikud skänneri automaatsel käivitamisel (näiteks ajagraafiku järgi).

Vaikimisi kasutab skänneri konsoolversioon Windows-ile samu sätteid, nagu skänneri GUI-versioon. Kui võtmetena ei ole määratud teisi parameetreid, kasutatakse skaneerimisel käsurealt samu parameetreid, mis on seadistatud skänneri graafilise kasutajaliideses (loe p. 3.2.3). Mõningaid skänneri sätteid saab määrata ainult programmi konfiguratsioonifailis. Loe selle kohta rohkem Lisast E.

3.4 SplDer Guard® Windows-ile

3.4.1 Üldine informatsioon

Sõltuvalt OS-st installeeritakse üks kahest valvuri versioonist:

- SpIDer Guard Me – Windows 95/98/Me puhul (SpIDer Guard Me)
- SpIDer Guard XP – Windows NT/2000/XP või Windows NT/2000/2003 Server puhul (SpIDer Guard XP)

Vaikimisi laetakse valvur igakordsel Windows-i käivitamisel. Aktiivset valvurit ei saa käesoleval Windows-i tööseansil maha laadida. Kui tekib vajadus valvuri ajutiseks blokeerimiseks (näiteks juhul, kui mõne ülesande täitmiseks läheb reaalajas vaja palju protsessori resurssi), vali SpIDer Guard XP kontekstmenüüst menüüpunkt `Peata`. Kui kasutad SpIDer Guard Me-d, pead keelama valvuri automaatse laadimise (toiming on kirjeldatud allpool, loe p. 3.4.2) ja seejärel taaskäivitama Windows-i.

Vaikimisi sätete kohaselt skaneerib valvur avatavaid faile "lennult" (failid kõvakettal – nende avamisel kirjutamiseks, failid

eemaldatavatel andmekandjatel – alati) ning teostab nende skaneerimist samal viisil, nagu skännergi (ehkki "kergemate" tingimustega). Lisaks sellele jälgib valvur pidevalt aktiivsete protsesside toiminguid, mis võivad olla iseloomulikud viirustele ning nende avastamisel blokeerib valvur ohtlikud protsessid ja teavitab sellest ka kasutajat.

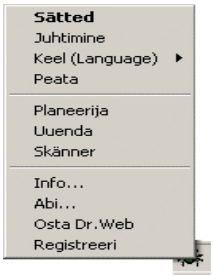
Nagu skännergi, informeerib vaikimisi Dr. Web tööjaamadele valvur nakatunud objektide avastamisel kasutajat ning pakub kasutajale võimalust otsustada, millist toimingut teostada. Dr.Web serveritele puhul teostatakse vaikimisi tuntud viiruse või nakkuskahtlusega objekti avastamisel viirusohu vältimiseks vajalikud toimingud automaatselt.

Sa saad vastavate sätete muutmisega määrata programmi käitumist viirusohtude avastamisel; sellisel juhul teostab valvur toimingud taustal. Kasutaja saab programmi toiminguid kontrollida statistikaakna abil (loe selle akna kohta allpool) ja logifailis.

Pärast installeerimist ilmub tegumiribale ämblikusarnane SpIDer Guard-i ikoon. Kui kasutatakse SpIDer Guard XP-d, ilmub hiirekursori liigutamisel üle ikooni hüpikaken, milles kuvatakse SpIDer Guard-i statistika. Kui on võimaldatud säte `Acknowledge=Yes` (vaikimisi on see võimaldatud), võib ilmuda veel teisigi hüpikaknaid, kui

- Toimub uuendamine
- Teostati mõni toiming nakatunud või kahtlase objektiga (ainult juhul, kui SpIDer Guard-i juhtpaneelil on võimaldatud `Millal saata teadaanded`)

Peamised tööriistad valvuri haldamiseks ning sätete muutmiseks asuvad valvuri ikooni kontekstmenüüs (pilt 24).



Pilt 24. SpIDer Guard XP kontekstmenüü

Menüüpunkt `Sätted` võimaldab ligipääsu programmi põhilistele parameetritele (loe detailsemalt p. 3.4.3).

Punkt `Juhtimine` (ainult SpIDer Guard XP-l) võimaldab avada Windows SpIDer Guard-i juhtpaneeli akna (ainult administraatori õigustega kasutajatel).

Menüüpunkt `Keel(Language)` võimaldab muuta programmi liidese keelt.

Punkt `Peata` võimaldab ajutiselt blokeerida programmi toimingud (ainult SpIDer Guard XP-l).

`Planeerija`, `Skänner` ja `Uuenda` menüüpunktid käivitavad vastavad komponendid.

Windows NT/2000/XP kasutajal peavad Dr.Web versiooni uuendamiseks olema adminstraatori õigused.

Kui kasutatakse SpIDer Guard Me-d, sisaldab kontekstmenüü menüüpunkti `Statistika`, mis avab akna informatsiooniga valvuri toimingute kohta alates selle viimasest laadimisest (skaneeritud, nakatunud või kahtlaste objektide arv, viirustele sarnased tegevused ning teostatud toimingud). SpIDer Guard XP kasutamisel kuvatakse lühidalt statistika (skaneeritud, nakatunud või kahtlaste objektide arv ja teostatud toimingud) hüpikaknas,

mis ilmub hiirekursori liigutamisel üle valvuri ikooni. Andmed valvuri töö kohta kuvatakse lehel `Statistika` SpIDer Guard-i sätete aknas.

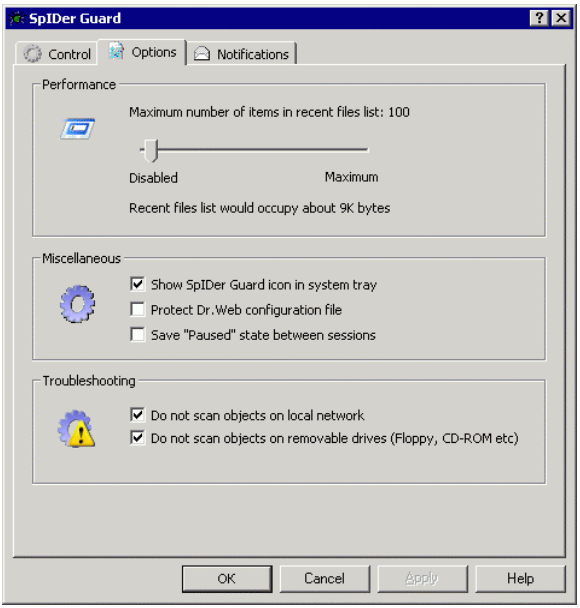
Punkt `Registreeri` käivitab kasutaja registreerimise protseduuri võtmefaili saamiseks Doctor Web, Ltd. serverist. Kui võtmefaili kehtivuse lõpuni on jäänud 10 või rohkem päeva, on see punkt blokeeritud või üldse mitte saadaval.

Punkt `Osta Dr.Web` avab Doctor Web, Ltd. veebilehekülje (või selle piirkondliku esindaja veebilehe), kus on selgitatud litsentsi omandamise ning uuendamise tingimused (internetiühenduse olemasolu korral).

SpIDer Guard XP installeerimisel lisatakse Windows-i tegumiribale element nimega `SpIDer Guard`. See sisaldab programmi spetsiifilisi sätteid, mis on seotud Windows NT/2000/XP-ga. Neid sätteid saab muuta üksnes administraatori õigustega kasutaja; näiteks saab administraator keelata valvuri ikooni kuvamise tegumiribal.

Valvuri ikooni eemaldamiseks tegumiribalt peab Windows NT/2000/XP OS-ga arvuti administraator tegema järgmist:

1. SpIDer Guard-i juhtpaneeli avamiseks kasuta üht viisi järgmistest:
   - Vali Windows-i peamenüüs (vajuta `Start` nuppu) `Settings`. Vali avanevas allmenüüs punkt `Control panel`. Vali avanevas Control panel-i aknas `SpIDer Guard`
   - Vali SpIDer Guard XP kontekstmenüüs punkt `Juhtimine`.
2. Mine lehele `Võtmed` (pilt 25).



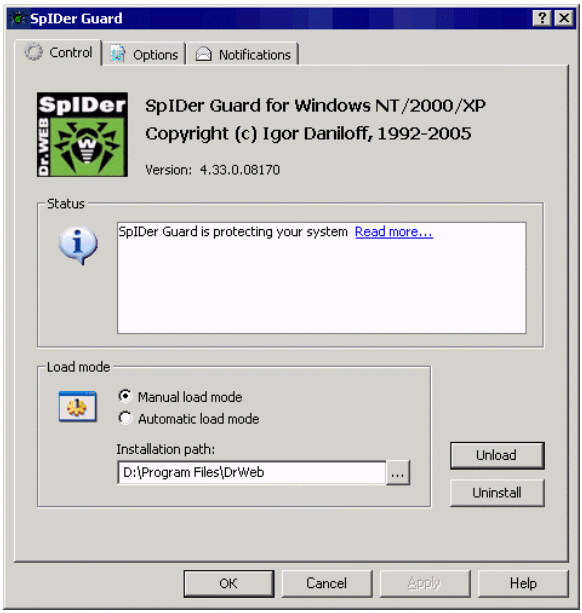
Pilt 25. SpIDer Guard-i juhtpaneeli element. `Leht Võtmed`

3. valvuri ikooni eemaldamiseks võta märgistus maha `Näita SpIDer Guard-i ikooni tegumiribal` eest; valvuri ikooni kuvamiseks tegumiribal märgi ruuduke selle ees.
4. Vajuta `OK`.

3.4.2 Valvuri käivitusreziimi häälestamine ning töö peatamine

SpIDer Guard XP automaatse laadimise keelamiseks:

1. Ava leht `Juhtimine` SpIDer Guard-i juhtpaneelil (pilt 26).



Pilt 26. SpIDer Guard-i juhtpaneeli element. `Leht Juhtimine`

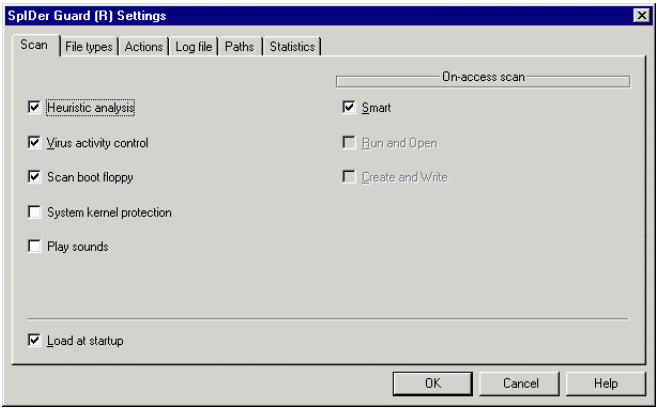
2. `Laadimisreziim` raadionuppude grupis vali `Käsitsilaadimine`.
3. Vajuta `OK`.

Järgmisel Windows-i käivitamisel ei laeta programmi automaatselt. Vajadusel saab programmi käivitada käsitsi. Selleks vajuta ülalkirjeldatud aknas nuppu `Lae`. Käsitsi käivitatuna saab valvuri töö lõpetada, vajutades nuppu `Lae maha`.

SpIDer Guard Me on alati seadistatud automaatse laadimise reziimile, kuid seda reziimi saab samuti blokeerida.

Selleks:

1. Vali tegumiribal asuva valvuri ikooni kontekstmenüüst punkt `Sätted`. Avaneb aken programmi sätetega, kuvatakse leht `Skaneeri` (pilt 27).



Pilt 27. SpIDer Guard Me sätted. `Leht Skaneeri`

2. Võta märgistus maha `Lae käivitamisel` eest.
3. Vajuta `OK`.

Järgmisel Windows-i käivitamisel valvurit automaatselt ei käivitata.

SpIDer Guard Me käivitamiseks käsitsi vali Windows-i peamenüüs (vajuta `Start` nuppu) menüüpunkt `Programs`, seejärel vali `Dr.Web`; avanevas allmenüüs vali `SpIDer Guard`. Valvuri käivitamisel taastab see automaatselt automaatse laadimise reziimi.

3.4.3 Valvuri põhilised parameetrid

Mõlema versiooni valvuri põhilised reguleeritavad parameetrid asuvad SpIDer Guard Me (vaata pilt 27) ja SpIDer Guard XP (pilt 28) lehel `Sätted`. Ükskõik millisel lehel kuvatavate parameetrite kohta abi saamiseks mine vastavale lehele ning vajuta nuppu

Help. Detailset informatsiooni iga parameetri kohta saab ka vastava elemendi peal hiire paremat nuppu klikkides.

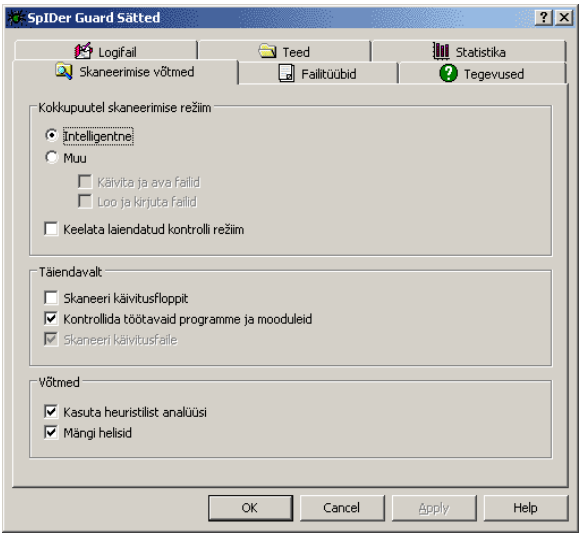
Kui sätete redigeerimine on lõpetatud, vajuta OK muudatuste salvestamiseks või Cancel tehtud muudatuste katkestamiseks.

Mõned kõige sagedamini muudetavad programmi sätted on kirjeldatud allpool.

Vaikimisi on programm seadistatud skaneerima faile kõvaketastel, mis avatakse kirjutamiseks ning faile eemaldatavatel andmekandjatel, mis avatakse lugemiseks või kirjutamiseks.

Vaikimisi on keelatud reziim *laiendatud kontroll*. Selles reziimis kontrollib SpIDer Guard XP viivitamatult kõiki faile, mille skaneerimine on määratud programmi sätetes ning kõik ülejäänud avatavad failid asetatakse kontrollimise järjekorda (failid, mis avatakse lugemiseks Smart ja Create and write files reziimides). Kui arvutil on ressurssi piisavalt, kontrollib valvur ka neid faile.

Selle reziimi võimaldamiseks võta SpIDer Guard XP Sätete aknas (pilt 28) lehel Skaneerimise võtmed märgistus maha Keelata laiendatud kontrolli reziim eest.



Pilt 28. SpIDer Guard XP Sätted. **`Leht Skaneerimise võtmed`**

Teatavaid väliseid andmekandjaid (näiteks kaasaskantavad USB-liidesega Winchester kettad) saab määratleda süsteemi kõvaketastena. Seepärast peaks selliseid seadmeid kasutama ülima ettevaatlikkusega ning nende ühendamisel arvutiga peaks neid viiruste suhtes kontrollima viirusetõrje skänneriga.

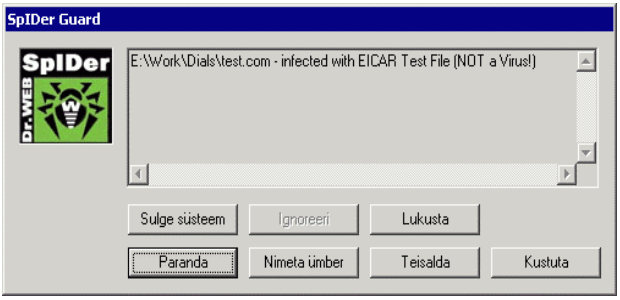
Arhiivide skaneerimise keelamine püsivalt aktiivse valvuriga ei tähenda seda, et viirused saavad arvutisse tungida – nende tuvastamise moment lükatakse lihtsalt edasi. Nakatunud arhiivi lahtipakkimisel (või nakatunud sõnumi avamisel) üritatakse nakatunud objekt kirjutada kõvakettale ning valvur tuvastab selle katse tingimata.

Dr.Web tööjaamadele puhul on vaikimisi määratud programmi käitumiseks arvatavasti parandatavate ning parandamatute viiruste ja kahtlaste objektide tuvastamisel teostatavatest toimingutest kasutaja informeerimine. Valvur genereerib infoakna, milles küsitakse edaspidi teostatavate toimingute kohta (pilt 29).

Dr.Web serveritele valvuri versioon teostab ohtlike objektide tuvastamise puhul toimingud viirusohu vältimiseks vaikimisi automaatselt (loe täpsemalt allpool).

Kui tuvastatakse objekt, mis sisaldab naljaprogramme, riskvara või muukvara, teostatakse vaikimisi toiming `Ignoreeri`.

Reklaamvara ning helistajate tuvastamisel on valvuri vaikimisi reaktsioon erinev: Dr.Web serveritele – teisaldamine, Dr.Web tööjaamadele – kasutaja teavitamine.



Pilt 29. Nakatunud objekti tuvastamisel kasutaja poolt soovitava toimingu küsimine

Teostatavate toimingute valik sõltub viirusjuhtumi tüübist.

`Paranda`, `Nimeta ümber`, `Teisalda` ja `Kustuta` toimingud on sarnased skänneri samade toimingutega.

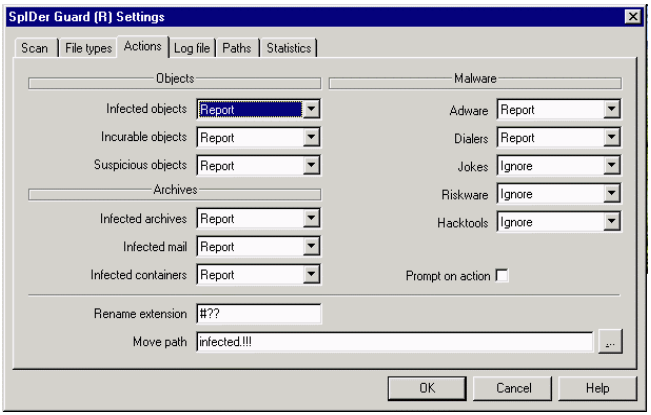
Nupu `Lukusta` vajutamisel märgitakse nakatunud fail Windows-ile ligipääsmatuks.

Nupu `Lõpeta töö` vajutamisel üritab programm Windows-i korrektselt sulgeda.

Sa saad valvuri sätteid muuta, lubamaks sellel automaatselt, ilma kasutaja vahelesekkumiseta teostada nakatunud objektide leidmisel vastavaid toiminguid.

Selleks (SpIDer Guard Me puhul):

1. Mine aknas `SpIDer Guard sätted` lehele `Tegevused` (pilt 30).



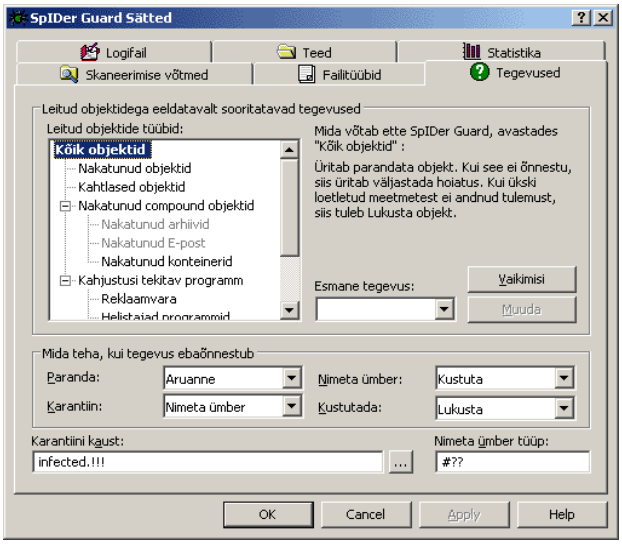
Pilt 30. Toimingute seadistamine viiruste avastamisel (SpIDer Guard Me)

2. Vali rippmenüüs `Nakatunud objektid` soovitav programmi käitumine nakatunud objekti tuvastamisel (soovitatav toiming `Paranda`).

3. Vali rippmenüüs `Parandamatud objektid` soovitav programmi käitumine parandamatu objekti tuvastamisel (soovitatav toiming `Teisalda`). Edaspidised toimingud teisaldatud objektidega on kirjeldatud p. 3.2.2.
4. Vali rippmenüüs `Kahtlased objektid` soovitav programmi käitumine kahtlase objekti tuvastamisel (soovitatav toiming `Ignoreeri` või `Teisalda`).
5. Samu programmi toiminguid saab määrata ka reklaamvara, helistajaid, naljaprogramme, riskvara ning muukvara sisaldavate objektide leidmise puhul.
6. Vajuta `OK`.

SpIDer Guard XP puhul:

1. Mine aknas `SpIDer Guard sätted` lehele `Tegevused` (pilt 31).



Pilt 31. Toimingute seadistamine viiruste avastamisel (SpIDer Guard XP)

2. Vali akna vasakus osas asuvas puus `Nakatunud objektid`. Akna paremas ülemises osas kuvatakse programmi toiming tuntud viirusega nakatunud objekti avastamise puhul. Seal kirjeldatakse käesolevate sätetega määratud programmi toiming ning samuti ka alternatiivne toiming, mis teostatakse juhul, kui esmane toiming ebaõnnestub. Allpool on kirjeldatud esmase toimingu sätete muutmine; alternatiivse toimingu sätete muutmine on kirjeldatud sammus 5.
3. Vaikimisi määratud toimingute võimaldamiseks antud tüüpi objektide tuvastamisel vajuta `Vaikimisi`. Nakatunud objektidele (v.a. objektid, mis sisaldavad naljaprogramme, riskvara ja muukvara) on vaikimisi määratud toiming `Ignoreeri`, serverite versioonis – nakatunud objektide parandamine, naljaprogrammide, riskvara ja muukvara ignoreerimine ning reklaamvara ja helistajate teisaldamine, voomane teostatakse ka kahtlaste ning nakatunud objektidega.
4. Vali rippmenüüs `Esmane tegevus` programmi esmane toiming nakatunud objekti avastamisel. Vajuta `Muuda`, kui soovid, et programm teostaks sinu poolt määratud toimingu.
5. Väljadel `Mida teha, kui tegevus ebaõnnestub` seadistatakse alternatiivsed toimingud puhuks, kui esmane toiming peaks ebaõnnestuma. Need sätted on eraldi määratavad järgnevate variantidena: parandamine, karantiini teisaldamine, kustutamine. Sa saad igas rippmenüüs valida toimingu, mis teostatakse esmase toimingu ebaõnnestumisel.
6. Programmi käitumine kahtlaste objektide, nakatunud failiarhiivide, meiliarhiivide ning konteinerite ning samuti ka reklaamvara, helistajaid, naljaprogramme, riskvara ja muukvara sisaldavate objektide avastamisel määratakse samal viisil.
7. Vajadusel täpsusta tesialdatavate failide kataloogi nimi ning tee selleni väljal `Karantiini kaust`.

8. Vajadusel määra mask faililaiendi ümbernimetamiseks.
9. Vajuta `OK`.

Lehel `Logifail` saad määrata logifaili parameetreid (sarnaselt skänneri parameetritele).

Kui SpIDer Guard töötab ja skänner on avastanud nakatunud objekti ning skänneri toiming (nakatunud objekti avamine) kutsub esile SpIDer Guard-i reageerimise, kohaldatakse nendele objektidele toiminguid, mis on määratud SpIDer Guard-i, mitte skänneri sätetes. Selle vältimiseks (ning samuti skaneerimise kiiruse suurendamiseks) tuleks säilitada SpIDer Guard-i sätetes vaikimisi määratud `Intelligentne` reziim. Kui valvuri või skänneri vaikimisi seadistatud teisaldatavate failide katalooge on muudetud ning need ei ühti omavahel, tuleb skänneri teisaldatavate failide kataloogi tee lisada skaneerimisest välistatud teede nimekirja.

3.5 SpIDer Mail® Windows-i tööjaamadele

See component ei sisaldu versioonis Dr.Web Windows-i serveritele.

3.5.1 Üldine informatsioon

Sisaldab vaikimisi koos teiste installeeritavate komponentidega ka SpIDer Mail Guard-i Windows-i tööjaamadele (meilivalvurit), mis püsib arvuti töötamisel töömälus ning see käivitatakse Windows-i käivitamisel.

Vaikimisi võtab program automaatselt üle kõik mistahes meiliprogrammide kutsed POP3-serveritele pordiga 110, SMTP-

serveritele pordiga 25, IMAP4-serveritele pordiga 143 ja NNTP-serveritele pordiga 119.

Kõik sissetulevad meilisõnumid võetakse e-posti kliendi asemel vastu viirusetõrje valvuri poolt ning sõnumeid skaneeritakse viiruste suhtes maksimaalse detailsuse tasemel. Kui viiruseid ning kahtlaseid objekte ei leitud, antakse sõnum "märkamatult" edasi meiliprogrammile, nagu oleks see vastu võetud otse serverist. Samasugune protseduur teostatakse enne sõnumite saatmist serveritesse.

Programmi reaktsioon sisenevatele nakatunud sõnumitele ja ka sõnumitele, mille skaneerimist ei teostatud (näiteks nende keerulise struktuuri tõttu) on vaikimisi järgmine:

- Viirusega nakatunud sõnumeid ei võeta vastu, meiliprogramm saab teate selle sõnumi kustutamise kohta – server saab teate sõnumi vastuvõtmise kohta (seda toimingut nimetatakse sõnumi *kustutamiseks*)
- Kahtlaseid objekte sisaldavad sõnumid teisaldatakse eraldi failidena karantiini kataloogi, meiliprogramm saab selle kohta teate (toimingut nimetatakse sõnumi *teisaldamiseks*)
- Kontrollimata sõnumid jäetakse vahele nagu ka mitte nakatunud sõnumid
- Kõik kustutatud või teisaldatud sõnumid kustutatakse ka POP3 või IMAP4 serverist

Väljuvaid sõnumeid, mis on nakatunud või kahtlased, ei saadeta serverile; kasutajat teavitatakse sõnumi saatmata jätmisest (reeglina meiliprogramm säilitab sõnumi).

Kui arvutis tuvastatakse tundmatu e-posti teel leviv viirus, suudab programm selle tuvastada selliste viiruste tüüpilise "käitumise" järgi (masspostitus). Vaikimisi on selline tuvastusmeetod võimaldatud.

Programmi vaikimisi sätted on piisavad algajale arvutikasutajale ning võimaldavad arvutile maksimaalse tasemega kaitset, nõudes seejuures kasutaja vähest sekkumist. Samas on mõned meiliprogrammide suvandid blokeeritud (näiteks võib program pidada paljudele aadressidele saadetavat sõnumit pidada masspostituseks), samuti ei ole võimalik saada kasulikku informatsiooni automaatselt kustutatavatest kirjadest (nakatumata tekstiosa). Edasijõudnud kasutajad saavad meilide skaneerimise parameetreid ning programmi käitumist viiruste avastamisel muuta.

Teatud juhtudel on POP3-, SMTP-, IMAP4- ning NNTP-ühenduste automaatne ülevõtmine võimatu; sellisel juhul võimaldab programm ühenduste ülevõtmise käsitsi.

Nii SpIDer Guard kui ka skänner suudavad mõlemad tuvastada viiruseid erinevate formaatidega postkastides, kuid meilivalvuril on siiski mitmeid eeliseid:

- Valvur ning skänner ei toeta mitte kõiki populaarseid postkastide formaate; meilivalvurit kasutades ei saabu nakatunud kirjad postkasti
- SpIDer Guard ei kontrolli vaikimisi postkaste. Kui see võimaldada, kahandab see märgatavalt arvuti tööjõudlust
- Skänner kontrollib postkaste ainult kasutaja nõudmisel või ajagraafiku järgi, mitte sõnumi vastuvõtmise hetkel. See toiming raiskab arvuti ressursse ning võtab ka rohkem aega.

Seega on meilivalvur kõikidest komponentidest esimene, kes tuvastab meili teel levivad viirused ning kahtlased objektid ega lase neil sattuda arvutisse. Valvuri töö on resursse säästev- meilide kontrollimine viiakse läbi programmi teiste komponentide abita.

3.5.2 Meilivalvuri haldamine. Käivitusreziimi seadistamine

Pärast programmi installeerimist genereerib see tegumiribale ikooni ümbrikuga ämbliku taustal. See ikoon näitab, et programm on aktiivne.

Programmi juhtimine ning seadistamine toimub ikooni kontekstmenüü abil (pilt 32).

Pilt 32. Meilivalvuri ikooni kontekstmenüü

Menüüpunkti `Statistika` valimisel avaneb aken informatsiooniga programmi töö kohta käimasoleval sessioonil (skaneeritud, nakatunud, kahtlaste objektide arv ning teostatud toimingud).

Menüüpunkti `Sätted` valimisel avaneb aken programmi sätetega (loe p. 3.5.3).

Menüüpunkt `Keel` võimaldab valida programmi kasutajaliidese keele.

Menüüpunktid `Uuenda`, `Skänner` ja `Planeerija` käivitavad vastavad komponendid.

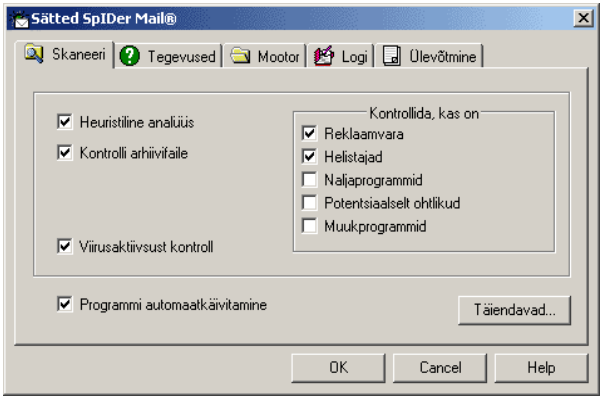
Windows NT/2000/XP kasutaja peab Dr.Web versiooni uuendamiseks omama administraatori õiguseid.

Kui programm töötab vaikesätetega, ei saa meilivalvurit Windowsi töösessiooni ajal blokeerida; sa saad ainult blokeerida valviuri

automaatse käivitamise. Sellel juhul ei käivitata programmi pärast Windowsi taaskäivitamist automaatselt.

Selleks:

1. Vali programmi kontekstmenüüs punkt `Sätted`. Avaneb aken programmi sätetega ning kuvatakse leht `Skaneerimine` (pilt 33).



Pilt 33. Meilivalvuri sätted. Leht `Skaneerimine`

2. Võta märgistus maha `Programmi automaatkäivitamine` eest.
3. Vajuta `OK`.

Meilivalvuri käsitsikäivitamiseks:

1. Vali Windows-i põhimenüüs (`Start`-nupu menüü) punkt `Programs`.
2. Vali avanevas menüüs `Dr.Web`.
3. Avanevas alamenüüs vali `SpIDer Mail`.

3.5.3 Programmi teatud sätete redigeerimine

Meilivalvuri sätete redigeerimise vajadusel ava sätete aken eelpool kirjeldatud viisil. (loe p. 3.5.2).

Sätete redigeerimisel kasuta programmi abisüsteemi (üldine abi iga lehe jaoks genereeritakse `Help` nupu vajutamisel; teatud liidese elementide kohta on võimaldatud ka kiire abiteksti kuvamine).

Kui redigeerimine on lõpetatud, vajuta `OK`.

Enamustel juhtudel on enamik vaikesätteid siiski optimaalsed. Allpool on kirjeldatud kõige sagedamini muudetavate parameetrite seadistamine.

Vaikimisi tuvastab meilivalvur lisaks nakatunud objekte sisaldavatele sõnumitele ka sõnumid, mis sisaldavad teisi tüüpe soovimatuid programme:

- reklaamvara
- helistajad

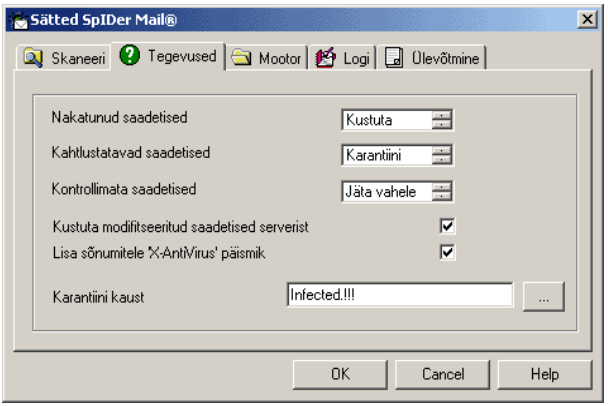
Meilivalvur suudab tuvastada ka järgnevad soovimatud programmid:

- riskvara
- muukvara
- naljaprogrammid

Tuvastatavate soovimatute programmide nimekirja muutmiseks märgista lehel `Skaneerimine` (vaata pilt 33) alal `Kontrollida, kas on` ruudukesed nende soovimatute programmitüüpide kõrval, mida soovid tuvastada ja võta märgistus maha nende programmitüüpide eest, mille tuvastamist sa ei soovi.

Meilivalvuri käitumine soovimatute programmide avastamisel on sama, nagu nakatunud sõnumite puhul, täpsemalt loe allpool.

Programmi sätted viiruste avastamisel sissetulevas postis asuvad lehel `Tegevused` (pilt 34).



Pilt 34. Meilivalvuri sätted. Leht `Tegevused`

Vaikimisi on nakatunud sõnumite (sisaldavad viiruskoodiga programme) puhul määratud toiminguks kustutamine, näiteks sõnumi vastuvõtmisest keeldumine (reeglina kustutatakse sellised sõnumid POP3/IMAP4-serverist). Kogenumad kasutajad võivad nimekirjas `Nakatunud sõnumid` valida toimingu `Karantiini`. Sellisel juhul tõstetakse sõnumid edaspidiseks analüüsimiseks spetsiaalsesse kataloogi (*karantiini*).

Kui kasutaja on kindel, et vastuvõetud "kahtlased" sõnumid ei sisalda viiruseid, võib väljal `Kahtlased sõnumid` valida toiminguks `Jäta vahele`.

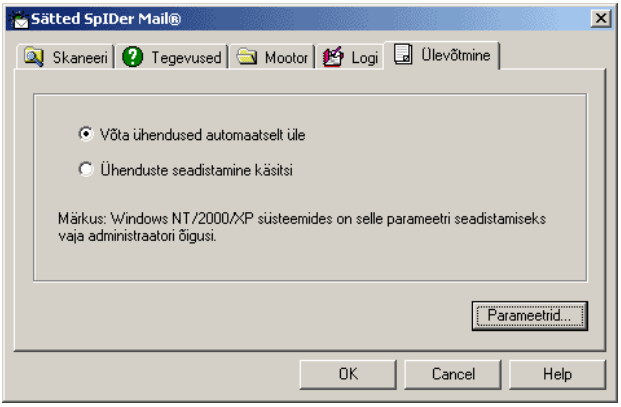
Kaitse kahtlaste sõnumite vastu võib välja lülitada, kui arvuti on täiendavalt kaitstud pidevalt töötava SpIDer Guard-iga.

Sa saad ka suurendada viirusetõrje programmi töö usaldusväärsust, valides väljal `Kontrollimata sõnumid`

toiminguks Karantiini. Teisaldatud sõnumite faile tuleks kontrollida skänneriga.

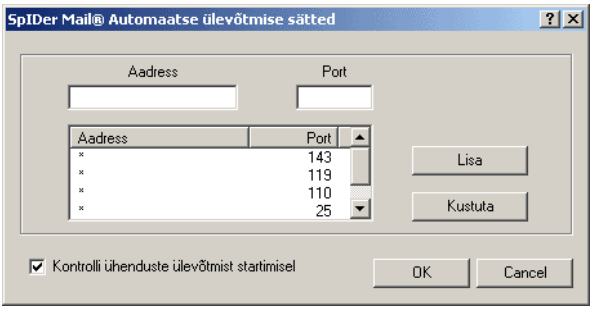
Kogenumad kasutajad võivad keelata programmi poolt kustutatud või teisaldatud sõnumite kohese kustutamise POP3/IMAP4-serverist ja kustutada need sõnumid käsitsi või kasutada meiliprogrammi mõnda paindlikkumat sätet. Selleks võta märgistus maha Kustuta modifitseeritud sõnumid serverist eest.

Ühenduste ülevõtmise parameetrid on määratud lehel Ülevõtmine (pilt 35).



Pilt 35. Ülevõtmise viisi määramine

Vaikimisi võetakse ühendused üle automaatselt. Ülevõetavate aadresside nimekiri on näha täiendavas aknas. Selle akna avamiseks vajuta Parameetrid (pilt 36).



Pilt 36. Automaatse ülevõtmise seadistamine

Vaikimisi sisaldab ülevõetavate aadresside nimekiri kõiki IP-aadresse (määratletud `*`) ja porte: `143` (standardne IMAP4 port), `119` (standardne NNTP port), `110` (standardne POP3 port) ja `25` (standardne SMTP port).

Nimekirjast mõne elemendi eemaldamiseks vali see ning vajuta `Kustuta`.

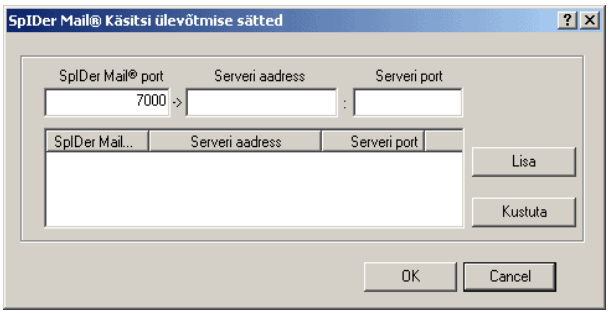
Nimekirja mõne serveri või serverite grupi lisamiseks sisesta selle aadress (IP-aadress või domeeni nimi) väljale `Aadress` ning pordi number väljale `Port` ja vajuta `Lisa`.

Aadressi `localhost` ei võeta üle, kui on määratletud `*`. Vajadusel saab selle aadressi ülevõetavate aadresside nimekirjas eraldi määrata.

Kui automaatne ülevõtmine on võimatu (programm annab sellest teada, kui ruuduke `Kontrolli ühenduste ülevõtmist startimisel` ees on märgitud), tuleb ülevõtmine seadistada käsitsi.

Selleks:

1. Vali ülalmainitud ülevõtmise seadistamise lehel (pilt 35) raadionupp `Ühenduste seadistamine käsitsi` ja vajuta `Parameetrid`. Avaneb ühenduste käsitsi seadistamise aken (pilt 37).



Pilt 37. Ülevõtmise seadistamine käsitsi

2. Koosta nimekiri ühendustest (POP3/SMTP/IMAP4/NNTP-serverid), mis tuleks üle võtta. Nummerda need üksteise järel, alustades 7000-st. Neid numbreid nimetatakse edaspidi *SpIDer Mail-i portideks*.
3. Sisesta iga kirje jaoks vastav number väljale `SpIDer Mail port` ja väljale `Serveri aadress` domeeni nimi või IP-aadress ning väljale `Serveri port` pordi number, läbi mille ühendus luuakse. Vajuta nuppu `Lisa`.
4. Korda neid toiminguid iga kirjega.
5. Vajuta `OK`.

Määra meiliprogrammi sätetes POP3/SMTP/IMAP4/NNTP-server-i aadressi asemel aadress `localhost:port_SpIDer_Mail`, kus `port_SpIDer_Mail` asendab POP3/SMTP/IMAP4/NNTP-server-i aadressi.

3.6 Planeerija Windows-ile

See komponent ei sisaldu versioonis Dr.Web Windows-i serveritele.

Vaikimisi sialdab Dr.Web tööjaamadele ülesannete automaatse käivitamise haldamise tööriista – Planeerija Windows-ile. See on täiendav programm ning selle funktsioone saab täita ka mõni teine planeerija, mis on kasutajale sobivam. Siiski on just see programm loodud viirusetõrje programmi skaneerimise ning uuendamise administreerimiseks ning pakub kasutajale täiendavaid võimalusi.

Windows NT/2000/XP kasutajal peavad olema Dr.Web-i uuendamiseks administraatori õigused. Seepärast peaks süsteemiadministraator tavakasutaja kontodega arvutites uuenduste vastuvõtmiseks keelama Dr.Web-i Planeerija ning võimaldama Windows-i standardse planeerija.

Kui programm on installeeritud, genereerib see tegumiribale rohelise ümmarguse sihverplaadile sarnaneva ikooni.

Peamised Planeerija seadistamise ning haldamise tööriistad asuvad selle ikooni kontekstmenüüs (pilt 38).

Pilt 38. Planeerija kontekstmenüü

Kui valida menüüpunkt `Ava`, avaneb Planeerija põhiaken (loe edaspidi).

Menüüpunkt `Keel` võimaldab valida programmi kasutajaliidese keele.

Menüüpunkt `Valikud` kordab põhiakna sama menüüpunkti ning võimaldab käivitada järgnevaid toiminguid:

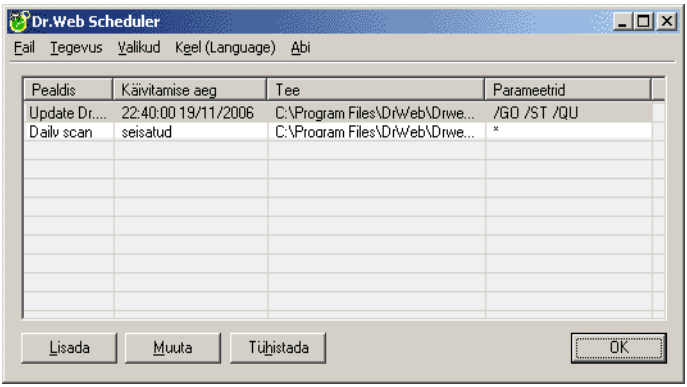
- peatada (taastada) programmi automaatne käivitamine
- peita (näidata) Planeerija ikooni tegumiribal
- keelata (võimaldada) logi kirjutamine

Vaikimisi püsib programm pidevalt arvuti töömälus ning on aktiivne. Kui soovid programmi mälust maha laadida, vali menüüpunkt `Lae maha`.

Planeerija käsitsi käivitamiseks:

1. Vali Windows-i peamenüüs (`Start`-nupu menüü) puntk `Programs`.
2. Vali avanevas menüüs `Dr.Web`.
3. Avanevas allmenüüs vali `Scheduler`.

Programmi administreerimise vahendid asuvad programmi põhiaknas. Põhiakna avamiseks (pilt 39) tee hiirega topeltklõps tegumiribal asuval programmi ikoonil või vali kontekstmenüüs punkt `Ava`.



Pilt 39. Planeerija põhiaken

Programmi mälust mahalaadimiseks vali menüüs `Fail` punkt `Lae maha`.

Programmi automaatse laadimise peatamiseks (taastamiseks) võta märgistus maha (märgista) menüü `Valikud` punkti `Laadida käivitamisel` eest.

Planeerija ikooni peitmiseks (näitamiseks) tegumiribal võta märgistus maha (märgista) menüüs `Valikud` punkti `Näita ikooni tegumiribal` eest.

Logi kirjutamise keelamiseks (lubamiseks) võta märgistus maha (märgista) menüüs `Valikud` punkti `Kirjuta logifail` eest.

Põhilised tööriistad ülesannete nimekirjaga töötamiseks asuvad menüüs `Tegevus`. Need tööriistad on saadaval ka ülesannete nimekirja kontekstmenüüs ning akna allosas asuvate nuppudega. Vaikimisi lisatakse programmi installeerimisel nimekirja kaks ülesannet:

- Igal tunnil "kriitiliseks" märgitud uuenduste saamine Internetist (loe edaspidi)

- Igapäevane kõvaketaste skaneerimine vaikimisi parameetritega kell 3

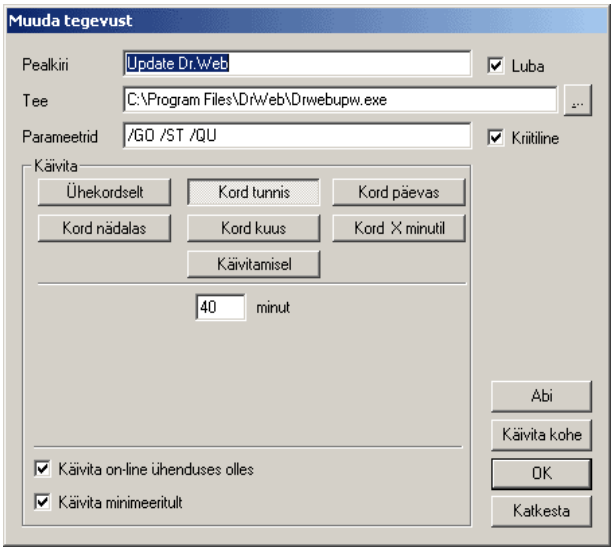
Teise ülesande käivitamise ajaks on märgitud "peatatud", mis keelab ülesande täitmise.

Ülesande täitmise lubamiseks ava see redigeerimiseks allpool kirjeldatud viisil.

Ülesande vaatamiseks ning vajadusel redigeerimiseks:

1. Tee üks toiming järgnevatest:
   - Topeltklõps ülesandel
   - Vali nimekirjas ülesanne ning seejärel kontekstmenüüs või menüüs `Tegevus` punkt `Muuta`
   - Vali nimekirjas ülesanne ning seejärel vajuta akna allosas asuvat nuppu `Muuta`

   Avaneb ülesande redigeerimise aken (pilt 40).



Pilt 40. Ülesande redigeerimine

2. Kui ülesande täitmine on peatatud, saad sa selle uuesti võimaldada. Selleks märgi ruuduke `Luba` ette. Seejärel on võimalik redigeerida ülesande parameetreid.

   Kui sa ei soovi, et ülesannet täidetaks, kuid samas ei soovi ülesannet ka kustutada (näiteks soovid ülesannet hiljem võimaldada), saad sa samal viisil aktiivse ülesande täitmise peatada.

3. Vajadusel muuda ülesande käivitamise graafikut (vajutades erinevaid nuppe väljal `Käivita`, võib akna välimus mõnevõrra muutuda).

4. Kui soovid, et ülesanne täidetakse ainult Internetiühenduse loomisel, märgi ruuduke `Käivita on-line ühenduses olles` ees.

5. Kui soovid, et vahelejäetud ülesanne täidetakse kohe, kui võimalik, märgi ruuduke `Kriitiline` ees.

6. Kui soovid rakenduse käivitamist minimeeritult, märgi ruuduke `Käivita minimeeritult` ees.

7. Vajuta `OK`.

Ülesande koheseks käivitamiseks vajuta nuppu `Käivita kohe`.

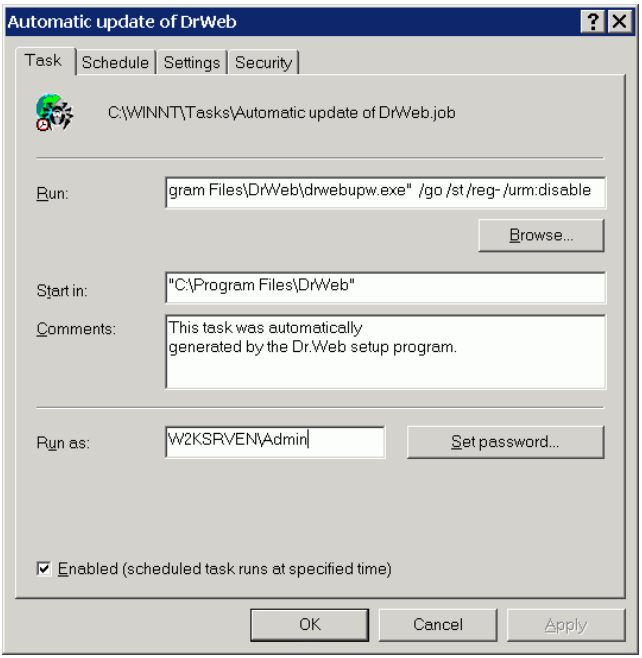
Kogenumad kasutajada võivad ka redigeerida käivitatava ülesande parameetreid ning teed.

Uue ülesande lisamiseks vali kontekstmenüüs või menüüs `Tegevus` punkt `Lisada`, või vajuta põhiakna allosas olevat nuppu `Lisada`. Avaneb eelpool kirjeldatud aknale (vt. pilt 40) sarnane aken uue ülesande parameetrite sisestamiseks. Edaspidised toimingud on samad, nagu ülesande redigeerimiselgi.

3.7 Skaneerimise ja uuendamise automaatne käivitamine programmis Dr.Web® Serveritele

Kui Dr.Web serveritele installeeritakse arvutisse, mile operatsioonisüsteemiks on Windows 2000/2003 Server, luuakse süsteemi planeerijasse automaatselt ülesanne viiruste andmebaaside ning muude failide uuendamiseks (kataloogi `Scheduled Tasks`).

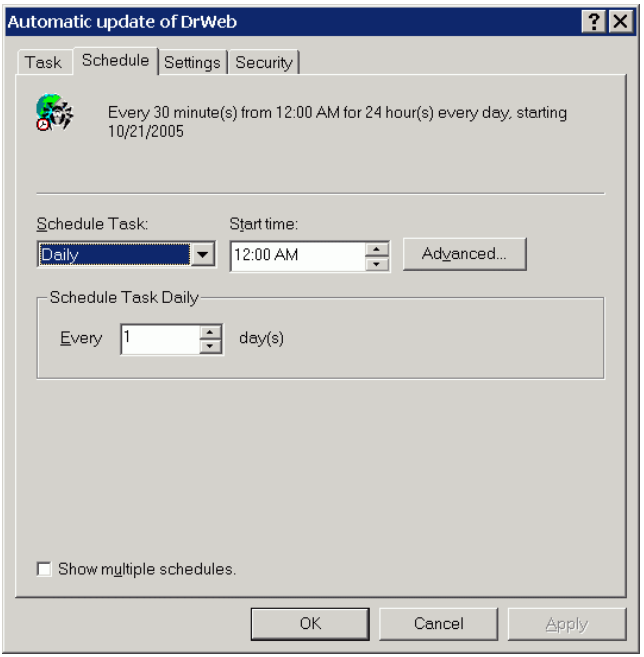
Selle ülesande parameetrite vaatamiseks vali menüüs `Programs` punkt `Accessories`. Seejärel vali `System Tools` ja `Scheduled Tasks`. Avaneb sama nimega kataloog. Tee selles kataloogis topeltklõps ikoonil `Automatic update of DrWeb`. Avaneb ülesande seadistamise aken (pilt 41).



Pilt 41. Uuendamise ülesande parameetrid

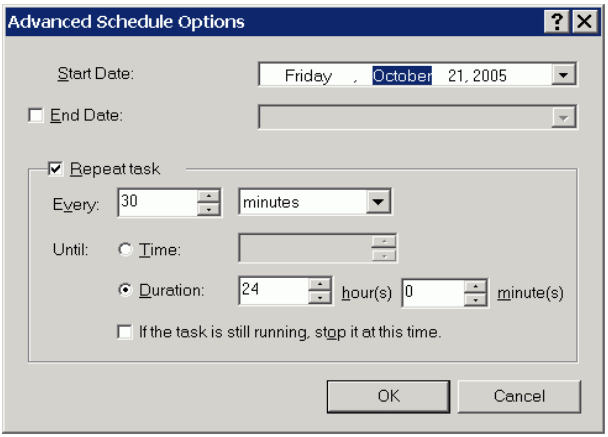
Lehel **`Ülesanne`** on kirjeldatud käivitatava faili täispikk nimi ning käsurea parameetrid. Märkeruut **`Lubatud`** võimaldab ülesande teostamist (märgistamata ruudu puhul säilitatakse ülesande andmed kataloogis, kuid ülesannet ei täideta).

Lehel **`Planeerija`** koostatakse graafik, mille järgi hakatakse ülesannet automaatselt käivitama (pilt 42).



Pilt 42. Graafiku tegemine

Vajuta **Advanced**. Avaneb aken **Advanced Schedule Options** (pilt 43).



Pilt 43. Graafiku täiendavad parameetrid

Sa saad ise lisada, kustutada või redigeerida uuendamise ja skaneerimise ülesandeid. Süsteemi planeerija töö kohta rohkema info saamiseks tutvu Help-süsteemiga ja Windows-i dokumentatsiooniga.

4. Viiruste andmebaaside ning muude programmiosade automaatne uuendamine

4.1 Üldine informatsioon

Kaasaegseid arvutiviiruseid iseloomustab nende kiire levimine. Äsja väljatulnud viirused võivad paari päeva või isegi tunni jooksul nakatada miljoneid arvuteid üle maailma.

Viirusetõrje arendajad täiendavad viiruste andmebaase pidevalt uute kirjetega. Pärast selliste uuenduste installeerimist suudab viirusetõrje tuvastada uusi viiruseid, blokeerida nende levimist ning osadel juhtudel ka parandada nakatunud faile.

Aeg-ajalt uuendatakse ka viirusetõrje algoritme, käivitatavaid faile ja programmimooduleid. Kogemused viirustega võitlemisel aitavad parandada avastatud vigu programmis; täiendatakse ka abisüsteemi ning dokumentatsiooni.

Viiruste andmebaaside uuenduste vastuvõtmise ja installeerimise kiirendamiseks ning hõlbustamiseks on loodud Dr.Web Automaatse uuendamise tööriist Windows-ile.

Uunedamise tööriista töö on reguleeritud viiruste andmebaaside struktuuri, viiruste andmebaaside uuendamise viisi ning kogu programmi poolt:

- Programm sisaldab *põhilist viiruste andmebaasi* (`drwebase.vdb`) ning selle laiendusi (failid drw43300.vdb ja drw43301.vdb). Nad kõik sisaldavad antud programmiversiooni väljalaskmise momendil teadaolevate viiruste kirjeldusi (versioonide kohta detailsemalt loe edaspidi)
- Üks kord nädalas väljastatakse *nädalased lisad* – need on failid viiruste kirjetega, millega saab tuvastada ja neutraliseerida viiruseid, mis on avastatud pärast eelmiste nädalaste lisade väljastamist. Nädalased lisad on failid,

mis näevad välja järgnevalt: `drwXXXYY.vdb`, kus `XXX` on käesoleva viirusetõrje programmi versiooni number (ilma erladusmärkideta) ja `YY` ion nädalase lisa number. Nädalaste lisade nummerdamine algab 02, näiteks viirusetõrje versiooni 4.33 esimene lisa on nimega `drw43302.vdb`

- Vajadusel (tavaliselt mitmel korral päevas), väljastatakse *kuumi lisasid* viiruste kirjetega, millega saab tuvastada ja neutraliseerida viiruseid, mis on avastatud pärast eelmiste nädalaste lisade väljastamist. See lisa on fail nimega `drwtoday.vdb`. Sellise faili vastuvõtmisel kustutatakse eelmine fail. Järgmisel nädalase lisa installeerimisel lisatakse sellesse kõik viiruste kirjed, mida sisaldas viimane kuuma lisa fail; allalaetav kuuma lisa fail ise sisaldab null viiruste kirjet.
- Programm sisaldab täiendavaid *kahjulike programmide andmebaasi* `drwnasty.vdb` ja `drwrisky.vdb`. Viiruste andmebaasis `drwnasty.vdb` sisalduvad kirjed reklaamvara ja helistajate tuvastamiseks. Naljaprogrammide, riskvara ja muukvara tuvastamiseks vajalikud kirjed sisalduvad viiruste andmebaasis `drwrisky.vdb`
- Aeg-ajalt väljastatakse ka kumulatiivseid lisasid kahjulike programmide andmebaasile. Nendele baasidele ei ole võimalik väljastada kuumi lisasid nii tihti, kui seda saab teha peamise viiruste andmebaasi puhul
- Aeg-ajalt väljastatakse sõltumatult viiruste andmebaaside uuendustest uuendusi ka teistele failidele
- Aeg-ajalt väljastatakse olulisi uuendusi viirusetõrje programmile. See on *uue viirusetõrje versiooni väljastamine*. Kõik sellel hetkel teadaolevate viiruste kirjed lisatakse uude peamisesse viiruste andmebaasi.

Uue versiooni installeerimisel vanad viiruste andmebaasid kustutatakse

Niisiis versiooni numbriga 4.33 installeerimisel ning mitmete nädalaste lisade vastuvõtmisel on viiruste andmebaaside struktuur järgmine:

- `drwebase.vdb` peamine viiruste andmebaas
- laiendused `drw43300.vdb` ja `drw43301.vdb` peamisele viiruste andmebaasile
- nädalased lisad (`drw43302.vdb`, `drw43303.vdb` jne.)
- `drwtoday.vdb` kuum lisa
- täiendavad kahjulike programmide andmebaasid `drwnasty.vdb` ja `drwrisky.vdb`
- kumulatiivsed lisad kahjulike programmide andmebaasile (`dwn43301.vdb`, `dwn43302.vdb` jne. ja `dwr43301.vdb`, `dwr43302.vdb` jne.)
- kuumad lisad täiendavatele kahjulike programmide andmebaasidele `dwntoday.vdb` ja `dwrtoday.vdb`

Viiruste andmebaaside lisasid väljastatakse tasuta ning neid saab installeerida, tõstes need programmi instaleerimiskataloogi.

Reeglina salvestatakse lisad serverites Zip-arhiividena, mis sisaldavad uuendamise faile ja tekstkirjeldusi. Need failid tuleb lahti pakkida ning asetada installeerimiskataloogi.

Kasutaja saab viirusetõrjet ostes tellida müüjalt regulaarse uuenduste saatmise e-posti kaudu või mõnel andmekandjal. Neid uuendusi väljastatakse failidena, millel on laiend `dwz`. Nende uuenduste installeerimiseks tee Explorer-is topeltklõps ikoonil või sõnumile lisatud failil.

Kõige mugavam viis programmi ja viiruste andmebaaside uuenduste saamiseks ja installeerimiseks on kasutada allpool kirjeldatud automaatse uuendamise tööriista (loe p. 4.2).

Automaatse uuendamise tööriista kasutamiseks peab sinu arvutil olema Internetiühendus.

4.2 Automaatse uuendamise tööriista käivitamine ning sellega töötamine

Automaatse uuendamise tööriista saab käivitada ühel viisil järgnevatest:

- Automaatselt, vastavalt ajagraafikule (loe p. 3.6)
- Käsurealt, nõudes programmi installeerimiskataloogis asuva faili `drwebupw.exe` täitmist
- Valides valvuri ikooni kontekstmenüüs punkti `Uuenda` (loe p. 3.4.1) või sama punkti meilivalvuri ikooni kontekstmenüüs (loe p. 3.5.2)
- Vajutades skänneri peaaknas  (loe p. 3.2.1)

Kui kasutaja käivitab automaatse uuendamise tööriista, kontrollib programm võtmefaili olemasolu installeerimiskataloogis ja selle mitte leidmisel üritab seda saada Interneti kaudu aadressilt www.drweb.com (see toiming on kirjeldatud p. 2.1 lõpus). Kui võtmefaili ei leita, on automaatne uuendamine võimatu.

Võtmefaili leidimisel kontrollib program, selle kehtivust aadressil www.drweb.com (kui fail on diskrediteeritud, võidakse see blokeerida, nt. selle illegaalse levitamise vältimiseks). Kui võtmefail on blokeeritud, ei toimu uuendamist ja programmi komponentide töö võidakse blokeerida; selle kohta genereeritakse kasutajale vastav teade.

Kui võtmefail on blokeeritud, võta ühendust müüjaga, kellelt soetasid viirusetõrje programmi.

Pärast võtmefaili edukat kontrollimist toimub uuendamine. Programm laeb automaatselt alla kõik sinu programmiversioonile vastavad uuendatud failid ning kui sinu ostutellimuses on sätestatud versiooniuuendus, siis ka uue programmiversiooni (kui see on väljastatud).

Kui uuendatakse käivitatavaid faile ja raamatukogusid, võib olla vajalik arvuti taaskäivitamine. Selle kohta kuvatakse kasutajale vastav teade. Kui uuendatakse ka automaatse uuendamise tööriista ennast, on uuendamise jooksul vajalik teha veel üks arvuti taaskäivitus.

Skänner saab uuendatud andmebaase kasutada pärast arvuti taaskäivitamist. Valvur ja meilivalvur kontrollivad perioodiliselt andmebaaside seisundit ning laevad baaside uuendused alla automaatselt. Valvur genereerib ka uuendamise kohta teate, kui `Acknowledge=Yes` on võimaldatud.

Automaatse uuendamise tööriista käivitamisel Planeerija poolt või käsurealt kasutatakse käsurea parameetreid (loe Lisa D).

Lisad

Lisa A. Erinevuste loetelu Dr.Web® tööjaamadele ja Dr.Web® serveritele vahel

Komponendid ja installeerimine

Dr.Web serveritele ei sisalda järgnevaid komponente::

- DOS-skänner
- SpIDer Mail
- Planeerija Windows-ile

Dr.Web serveritele installatsiooniprogramm ei paku kohandatava installeerimismooduse (*custom installation*) puhul nende komponentide installeerimise võimalust.

Vaikimisi sätted

Viirusetõrje kahe programmiversiooni vaikimisi sätete erinevused tulenevad programmide erinevatest kasutuskohtadest: serveritele mõeldud versioon peab töötama automaatselt koos logifailide perioodilise kontrolliga; tööjaamade versiooni tööd juhib kasutaja. Tabelis 2 on kahe versiooni erinevate vaikesätete kokkuvõte. Esimeses veerus on loetletud komponendi parameetri nimi ja konfiguratsioonifaili parameetri nimi, teises veerus on näidatud parameetri vaikeväärtus tööjaamadele mõeldud versioonis (konfiguratsioonifaili parameetri väärtus ja kirjeldus), kolmandas veerus on sama informatsioon viirusetõrjeprogrammi serveritele kohta.

Tabel 2. Viirusetõrje kahe erineva versiooni vaikesätted

Parameeter	**Versioon tööjaamadele**	**Versioon serveritele**
Skänner: toimingud nakatunud failidega InfectedFiles	Teavitada Report	Parandada Cure
Skänner: toimingud kahtlaste failidega SuspiciousFiles	Teavitada Report	Teisaldada Move
Skänner: toimingud parandamatute failidega IncurableFiles	Teavitada Report	Teisaldada Move
Valvur: toimingud nakatunud failidega InfectedFiles	Teavitada Report	Parandada Cure
Valvur: toimingud kahtlaste failidega SuspiciousFiles	Teavitada Report	Teisaldada Move
Valvur: toimingud parandamatute failidega IncurableFiles	Teavitada Report	Teisaldada Move
Skänner ja valvur: toimingud nakatunud arhiividega ActionInfectedArchive	Teavitada Report	Teisaldada Move
Skänner ja valvur: toimingud nakatunud meilifailidega ActionInfectedMail	Teavitada Report	Teisaldada Move
Skänner ja valvur: toimingud nakatunud konteineritega ActionInfectedContainer	Teavitada Report	Teisaldada Move
Skänner ja valvur: skaneeritud (mitte nakatunud) objektide logimine faili LogScanned	Ei No	Jah Yes

Parameeter	Versioon tööjaamadele	Versioon serveritele
Logifaili suurus, KB MaxLogSize	512	8182
Uuendamise lipufaili kontrollimise periood, min UpdatePeriod	1m	15m

Lisa B. Korporatiivsete võrkude kaitse Dr.Web® Enterprise Suite abiga

Dr.Web Windows-ile võimaldab usaldusväärset, paindlikku ja lihtsasti kohandatavat kaitset viiruste ning teiste soovimatute programmide vastu.

Programmiversioonid, mis on välja töötatud nii Windows-i tööjaamadele ja serveritele kui ka teistele platvormidele, võimaldavad usaldusväärset kaitset ettevõttes kasutatavatele arvutitele. Siiski on korporatiivses võrgus töötavate arvutite puhul viirusetõrje jaoks olemas teatud kitsaskohad:

- Tavaliselt installeerib tarkvara arvutitesse ettevõte süsteemiadministraator. Viirusetõrje programmide installeerimine ja nende pidev uuendamine on administraatorile lisatööks ning nõuab ka füüsilist ligipääsu arvutitele.
- Mistahes kogemusteta kasutaja poolt tehtud muudatused (kaasaarvatud viirusetõrje programmi töö blokeerimine, kuna kasutajale tundub, et selle töö tekitab ebameeldivusi arvuti kasutamisel) loovad kaitsesse "auke" – viirused hakkavad tungima ettevõtte arvutivõrku ning nende ohutuks tegemine muutub üha enam raskemaks ülesandeks
- Viirustevastane kaitse saab olla täielikult efektiivne ainult siis, kui selle tööd analüüsivad kvalifitseeritud spetsialistid

ning kui analüüs sisaldab protokollide, karantiini tõstetud failide jne. analüüse. See töö võib osutuda tingimustes, kus andmeid säilitatakse sadades või tuhandetes arvutites, väga raskeks

Nende probleemide lahendamiseks töötati välja Dr.Web Enterprise Suite (Dr.Web ES).

Dr.Web ES võimaldab järgnevat:

- Tsentraliseeritud (personali ligipääsu vajaduseta) viirusetõrje pakettide installeerimist kaitstavatesse arvutitesse (kohaliku võrgu tööjaamad ja serverid)
- Tsentraliseeritud viirusetõrje pakettide parameetrite seadistamist
- Kaitstavates arvutites olevate programmide ja viiruste andmebaaside tsentraliseeritud uuendamist
- Kõikides kaitstavates arvutites OS-i ja viirusetõrje pakettide seisundi ning viirusjuhtude monitoorimist

Dr.Web ES võimaldab jätta kasutajale õigused tema arvutis oleva viirusetõrje paketi sätete redigeerimiseks ning administreerimiseks, kasutaja õiguste paindliku piiramise või kõikide õiguste keelamise.

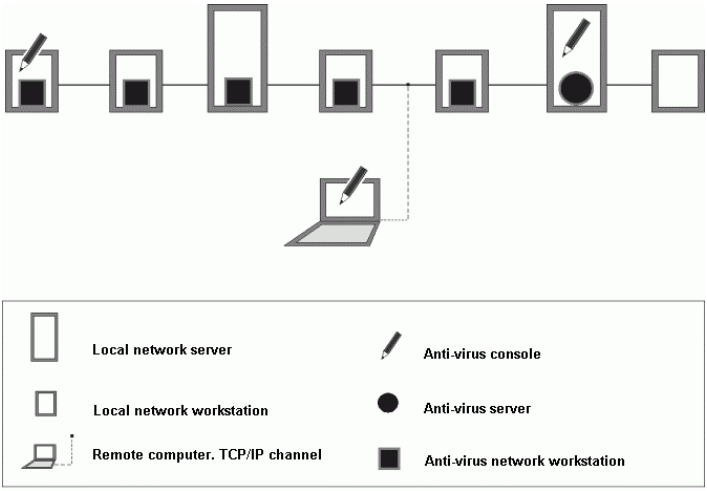
Dr.Web ES-il on "klient-server" arhitektuur. Selle komponendid on installeeritud kohtvõrgu arvutitesse ning vahetavad informatsiooni kasutades võrgu protokolle (programmi komponentide vastasmõjude detailsem kirjeldus tuleb edaspidi). Arvuteid, kuhu on installeeritud Dr.Web ES interaktiivsed komponendid, nimetame *viirusetõrje võrguks*. Viirusetõrje võrk sisaldab järgnevaid komponente:

- *Viirusetõrje agent*. See komponet on installeeritud kaitsavasse arvutisse; ta installeerib uuendusi ja juhib viirusetõrje paketi tööd vastavalt sellele, kuidas juhendab *viirusetõrje server* (loe edaspidi). Samuti saadab agent kaitstavast arvutist viirusetõrje serverisse informatsiooni viirusjuhtude ning muude sündmuste kohta

- *Viirusetõrje server*. See komponent on installeeritud ühte kohalikus võrgus asuvasse arvutisse. Viirusetõrje server säilitab kaitstavate arvutite erinevatele OS-dele mõeldud viirusetõrje programmipakette, viiruste andmebaaside, viirusetõrje pakettide ja viirusetõrje agentide uuendusi, kasutajate võtmeid ning kaitstavate arvutite pakettide sätteid ja saadab neid viirusetõrje agendi nõudmisel vastavatesse arvutitesse. Viirusetõrje server peab ühte logi sündmuste kohta kogu viirusetõrje võrgus ning iga kaitstava arvuti kohta ka eraldi logi
- *Viirusetõrje konsool*. Seda komponenti kasutatakse viirusetõrje võrgu kaugadministreerimiseks, redigeerides selle abil viirusetõrje serveri sätteid ja viirusetõrje serveris säilitatavaid kaitstavate arvutite sätteid

Viirusetõrje konsooli saab installeerida ka arvutitesse, mis ei asu kohtvõrgus; selle töötamiseks on vajalik ainult TCP/IP ühendus konsooli ja viirusetõrje serveri vahel.

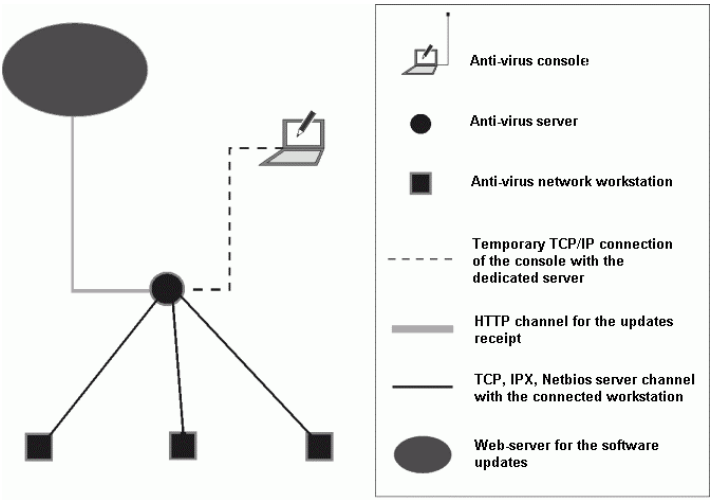
Pildil 44 on näidatud viirusetõrje võrgu poolt kaitstava kohtvõrgu fragmendi üldine skeem.



Pilt 44. Viirusetõrje võrgu füüsiline struktuur

Viirusetõrje võrgu käskude, andmete ja statistilise informatsiooni vood liiguvad läbi viirusetõrje serveri. Viirusetõrje konsool vahetab samuti andmeid ainult serveriga; muudatused tööjaama konfiguratsioonis ning käskude edastamine viirusetõrje agendile tehakse serveri poolt vastavalt konsoolilt saadud käsklustele.

Viirusetõrje võrgu fragmendi loogiline struktuur on näidatud pildil 45.



Pilt 45. Viirusetõrje võrgu loogiline struktuur

Serverist tööjaamadesse ja vastupidi (õhuke pidevjoon pildil 45) saadetakse, kasutades ühte toetatud võrguprotokolli (TCP, IPX või NetBIOS), järgnevaid päringuid:

- Agendi päringud tsentraliseeritud graafiku saamiseks ning antud tööjaama tsentraliseeritud graafiku kohta
- Agenda ja viirusetõrje paketi sätted
- Päringud teostamist vajavate graafikujärgsete ülesannete kohta (skaneerimine, viiruste andmebaaside uuendamine jne.)
- Viirusetõrje pakettide moodulid – juhul kui agent on saanud ülesande need installeerida
- Tarkvara ja viiruste andmebaaside uuendused – kui viiakse läbi uuendamist
- Agendi teated tööjaama konfiguratsiooni kohta
- Agendi ja viirusetõrje pakettide töö statistika tsentraliseeritud logifaili lisamiseks

- Teated viirusjuhtude ja muude sündmuste kohta, mida peab logima

Tööjaamade ja serveri vahelise liikluse maht on sõltuvalt tööjaamade sätetest ja nende arvust üsna mahukas ning seetõttu võimaldab Dr.Web ES liikluse mahu vähendamiseks selle pakkimise võimalust.

Liiklust serveri ja tööjaamade vahel saab krüptida. See võimaldab vältida kirjeldatud kanalis liikuva info lekkimist ja tööjaamadesse laetava tarkvara väljavahetamise võimalust.

Seega võimaldab Dr.Web ES:

- Viirusetõrje tarkvara lihtsat tsentraliseeritud installeerimist kaitstavatesse arvutitesse ning enamikel juhtudel (arvutite puhul, mille OS-ks on Windows 2000/XP) saab installeerimise läbi viia ilma füüsilise juurdepääsuta arvutile.
- Viirusetõrje tarkvara tsentraliseeritud üles seadmist, kulutades selleks minimaalselt töötunde
- Viirusevastase kaitse seisundi kontrollimist
- Vajadusel viirusetõrje tarkvara ülesannete tsentraliseeritud käivitamist või lõpetamist arvutites
- Kõikidest kaitstavatest arvutitest viirusjuhtude kohta informatsiooni kogumist ning analüüsimist
- Vajadusel mõnedele kasutajatele viirusetõrje tarkvara seadistamise õiguste andmist
- Viirusevastase kaitse administraatoril viirusetõrje võrgu haldamist ning selle kohta informatsiooni saamist kas ettevõtte kohtvõrgus asuvatest arvutites või kaugtöökohas, läbi interneti

Suurte ettevõtete võrkudes, kus asub sadu või tuhandeid arvuteid, on mõistlik luua Dr.Web ES viirusetõrje võrk mitme serveriga. Serveritevaheline hierarhiline ühendus võimaldab lihtsustada

viiruste andmebaaside ning tarkvara uuendamist ning nendelt informatsiooni vastuvõtmist viirusjuhtude kohta. Administraator saab analüüsida võrgu logisid kas eraldiasuvate serverite kaupa või kogu viirusetõrje võrgu koondlogina.

Dr.Web ES suurendab ettevõtete võrkude viirusevastase kaitse usaldusväärsust ning selle administreerimine nõuab vähem kulusid võrreldes personaalse viirusetõrje programmi installeerimisega igasse arvutisse.

Dr.Web Enterprise Suite-il on võrreldes teiste sarnaste toodetega mitmeid eeliseid:

- Rakenduslike lahenduste kõrge usaldusväärsus ja turvalisus
- Lihtne administreerimine
- Kõikide komponentide mitmeplatvormiline struktuur
- Suurepärane mastaapsus

Soovitame Dr.Web ES osta ja installeerida, kui:

- Sinu ettevõtte arvutivõrk on märkimisväärselt suur (mitukümmend või rohkem arvutit)
- Sinu arvutivõrk on väike, kuid mõnedel põhjustel (ette nähtud spetsiaalse tarkvara poolt, seadmete või personali oskuste tõttu) oled otsustanud viia ellu range poliitika tarkvara installeerimisel ja seadistamisel arvutivõrgus

Arvutites, mis ei kuulu ettevõtte arvutivõrku, kasuta personaalseid viirusetõrjeprogramme – Dr. Web Windows-ile ja Dr.Web teistele platvormidele.

Lisa C. Põhimõtted viirustele nimeandmisel

Viiruse koodi tuvastamisel informeerivad Dr. Web viirusetõrje komponendid läbi kasutajaliidese sellest kasutajat ning kirjutavad Doctor Web, Ltd. spetsialistide poolt viirusele antud nime logifaili. Need nimed on moodustatud tuginedes kindlatele põhimõtetele ja

need kajastavad viiruste mudeleid, haavatavate objektide klasse, levikeskkonda (OS ja rakendused) ning veel mõnda iseärasust. Nende põhimõtete tundmine võib tulla kasuks kaitstava süsteemi programmide ning organisatoorse haavatavuse tuvastamisel. Allpool leiad viirustele nimeandmise põhimõtete lühikirjelduse; selle täielik ning pidevalt uuendatav versioon on saadaval leheküljel http://support.drweb.com/faq/.

See rühmitamine on tinglik, teatud juhtudel omavad mõned viirused mitmeid omadusi samal ajal. Ühtlasi ei saa seda lugeda täielikuks, kuna pidevalt ilmuvad uued viiruste tüübid ja nende liigitamine tehakse veelgi täpsemalt.

Viiruse täisnimi koosneb mitmest elemendist, mis on üksteisest eraldatud punktidega. Mõned elemendid täisnime alguses (prefiksid) ja selle lõpus (sufiksid) on tüüpilised tavapärasele rühmitamisele.

Põhilised prefiksid

Operatsioonisüsteemide prefiksid

Järgnevaid prefikseid kasutatakse sellistele viirustele nimeandmisel, mis nakatavad teatud platvormide (OS-de) käivitatavaid faile:

- **`Win`** – 16-bit Windows 3.1 programmid
- **`Win95`** – 32-bit Windows 95/98/Me programmid
- **`WinNT`** – 32-bit Windows NT/2000/XP programmid
- **`Win32`** – 32-bit Windows 95/98/Me and NT/2000/XP programmid
- **`Win32.NET`** – programmed Microsoft .NET Framework operatsioonisüsteemis
- **`OS2`** – OS/2 programmid

- **Unix** – programmed erinevates Unixilaadsetes süsteemides
- **Linux** – Linux programmid
- **FreeBSD** – FreeBSD programmid
- **SunOS** – SunOS (Solaris) programmid
- **Symbian** – Symbian OS (mobiilne OS) programmid

Pane tähele, et osad viirused võivad nakatada ühe süsteemi programme, kuigi nad ise töötavad teises süsteemis.

MS Office faile nakatavad viirused

MS Office objekte nakatavate viiruste prefiksite grupp (näidatud on makro keel, mida nakatavad seda tüüpi viirused):

- **WM** – Word Basic (MS Word 6.0-7.0)
- **XM** – VBA3 (MS Excel 5.0-7.0)
- **W97M** – VBA5 (MS Word 8.0), VBA6 (MS Word 9.0)
- **X97M** – VBA5 (MS Excel 8.0), VBA6 (MS Excel 9.0)
- **A97M** – MS Access'97/2000 andmebaasid
- **PP97M** – MS PowerPoint presentatsioonid
- **O97M** – VBA5 (MS Office'97), VBA6 (MS Office'2000), viirus nakatab rohkem kui ühe MS Office komponendi faile

Programmeerimiskeelte prefiksid

HLL gruppi kasutatakse kõrgetasemelistes programmeerimiskeeltes kirjutatud viirustele nimeandmisel, nendeks keelteks on näiteks C, C++, Pascal, Basic ja teised. Modifikaatorid viitavad põhilisele funktsioneerimise algoritmile, näiteks:

- **HLLW** – ussid

- **HLLM** – e-posti ussid
- **HLLO** – ohverprogrammi koodi ümberkirjutavad viirused
- **HLLP** – parasiitviirused
- **HLLC** – satelliitviirused

Programmeerimiskeele prefiksiks võib lugeda ka järgneva prefiksi:

- **Java** – Java virtuaalmasina viirused

Trooja hobused

Trojan – üldine nimetus erinevatele Trooja hobustele (Troojalastele). Enamikel juhtudel kasutatakse selle grupi prefikseid koos prefiksiga `Trojan`.

- **PWS** – salasõna varastav Troojalane
- **Backdoor** – Trojaalane RAT-funktsiooniga (Remote Administration Tool – utiliit kaugadministreerimiseks)
- **IRC** –funktsioneerimiseks Internet Relayed Chat (IRC) kanalite keskkonda kasutav Troojalane
- **DownLoader** – Troojalane, mis laeb internetist salaja alla erinevaid kahjulikke programme
- **MulDrop** – Troojalane, mis laeb alla erinevaid tema kehas sisalduvaid viiruseid
- **Proxy** – Troojalane, mis võimaldab pahatahtlikul kasutajal läbi nakatunud arvuti anonüümselt internetis töötada
- **StartPage** (sünonüüm: **Seeker**) – Troojalane, mis muudab omavoliliselt brauseri avalehekülge
- **Click** – Troojalane, mis suunab kasutaja brauseri kindlaksmääratud leheküljele (või lehekülgedele)

- **KeyLogger** – Troojalane-nuhkvara; logib klahvivajutusi; võib saata kogutud andmeid kurjategijatele
- **AVKill** – peatab viirusetõrje programmide, tulemüüride jne. töö, võib need programmid ka ketastelt kustutada
- **KillFiles**, **KillDisk**, **DiskEraser** – kustutab mõned failid (failid mõnedes kataloogides, mõne maskiga failid, kõik failid ketastelt jne.)
- **DelWin** – kustutab Windows operatsioonisüsteemi elutähtsad failid
- **FormatC** – formaadib ketta C: . Sünonüüm: **FormatAll** – formaadib mõned või kõik kettad
- **KillMBR** – rikub või kustutab peamise käivitussektori (MBR) sisu
- **KillCMOS** – rikub või kustutab CMOS

Haavatavust kasutav vahend

- **Exploit** – vahend, mis kasutab ära mõne operatsioonisüsteemi või aplikatsiooni teadaolevaid haavatavaid kohti kahjuliku koodi või viiruse sokutamiseks sellesse või mõne omavolilise toimingu sooritamiseks süsteemis

Võrgurünnakute vahendid

- **Nuke** – vahendid, mis ründavad operatsioonisüsteemide kindlaid teadaolevaid haavatavaid kohti, põhjustades sellega rünnatava süsteemi ebanormaalse sulgemise (shutdown)
- **DDoS** – agentprogramm ”teenustest keeldumine”-tüüpi jaotatud võrgurünnakute teostamiseks (Distributed Denial Of Service)

- **FDOS** (sünonüüm: **Flooder**) – Flooder Denial of Service – programmid pahatahtlike toimingute teostamiseks WWW-s, kasutavad teenustest keeldumise ideed; erinevalt DDoS-ist mille puhul kasutatakse ühe ovhersüsteemi ründamiseks üheaegselt mitmeid agente erinevates arvutites, töötab FDOS-programm iseseisvalt, teistest sõltumatu programmina

Skriptviirused

Erinevates keeltes kirjutatud viiruste prefiksid:

- **VBS** – Visual Basic Script
- **JS** – Java Script
- **Wscript** – Visual Basic Script ja/või Java Script
- **Perl** – Perl
- **PHP** – PHP
- **BAT** – MS-DOS käsuinterpretaator

Pahatahtlikud programmid

Objektide prefiksid, mis ei ole viirused vaid muud pahatahtlikud programmid:

- **Adware** – reklaamprogramm
- **Dialer** – helistaja programm (suunab modemi helistama sisseprogrammeeritud tasulistele numbritele või tasulistele ressurssidele)
- **Joke** – naljaprogramm
- **Program** – potentsiaalselt ohtlik programm (riskvara)
- **Tool** – sissemurdmiseks kasutatav programm (hacktool)

Muud

Prefiksit **generic** kasutatakse teisele prefiksile järgnevalt, kirjeldamaks keskkonda või väljatöötamise meetodit, tähistamaks tüüpilist selle viirusetüübi esindajat. Selline viirus ei oma mingeid iseloomulikke tunnusjooni (nagu tekstiread, eriefektid jne.) mis võimaldaks sellele anda mõnda spetsiifilist nime.

Varem kasutati lihtsate tunnusjoonteta viiruste nimetamisel prefiksit **Silly** koos erinevate modifikaatoritega.

Sufiksid

Sufikseid kasutatakse mõnede eriliste viirusobjektide nimetamiseks:

- **generator** – object ei ole virus vaid viiruse generator
- **based** – erilise generaatori abiga väljatöötatud virus või muudetud viirus Mõlemal juhul on selle tüübi nimetus üldine ning võib määratleda sadu või mõnikord ka tuhandeid viiruseid
- **dropper** – object ei ole viirus vaid antud viiruse installeerija

Lisa D. Viirusetõrje täiendavad käsurea parameetrid

D1. Sissejuhatus

Programmide puhul, mis käivituvad käivitusfaili avamisel, kasutatakse täiendavaid käsurea parameetreid (*võtmeid*). See kehtib ka kõikide versioonide skännerite (loe p. 3.2 ja 3.3) ja automaatse uuendamise mooduli (loe p. 4) kohta. Võtmetega saab määrata konfiguratsioonifailis puuduvaid parameetreid; konfiguratsioonifailis näidatud parameetritele aga omistada kõrgemat prioriteeti.

Võtmed algavad sümboliga / ning nagu teisedki käsurea parameetrid, eristatakse need üksteisest tühikutega.

Alpool on loetletud eraldi nii skänneri kui ka automaatse uuendamise mooduli käsurea parameetrid (loe allpool). Kui võtmel esineb modifikatsioone, on ka need ära näidatud.

D2. Skänneri käsurea parameetrid

/@<file_name> või **/@+**<file_name> käsib skaneerida objekte, mis on loetletud määratud failis. Iga objekt määratakse loetelu-faili eraldi reana. See võib olla täielik tee koos failinimega või ainult rida ?boot, mis tähendab, et teostada tuleb käivitussektorite skaneerimine; skänneri GUI-versiooni puhul aga failinimed koos maskide ning kataloogi nimedega. Failide nimekirja võib koostada käsitsi mistahes tekstiredaktoriga; samuti saab seda koostada automaatselt, kasutades rakendusi, mis kasutavad skännerit teatud failide kontrollimiseks. Kui failide nimekirja kasutada ilma sümbolita +, kustutab skänner failide nimekirja kohe pärast skaneerimise teostamist.

/AL – antud seadme või kataloogi kõikide failide skaneerimiseks, sõltumata laienditest või formaadist.

/AR – arhiivides asuvate failide skaneerimiseks. Hetkel teostatakse sel juhul ARJ, PKZIP, RAR, LHA, GZIP, TAR 7-ZIP arhiveerijatega pakitud arhiivide, samuti ka MS CAB-arhiivide (QUANTUM-pakkimine ei ole veel toetatud) ja optiliste ketaste (CD ja DVD) ISO-kujutiste skaneerimine (ilma parandamiseta). Kui võti (/AR) on märgitud, käsib see programmil nakatunud või kahtlaste failidega arhiivi avastamisel kasutajat sellest informeerida. Võtme täiendamisel modifikaatoritega D, M või R teostatakse teised toimingud: /ARD – kustutatakse; /ARM – teisaldatakse (vaikimisi kataloogi infected.!!!); /ARR – nimetatakse ümber (vaikimisi asendatakse laiendi esimene sümbol sümboliga #). Võti

võib lõppeda ka modifikaatoriga N, sellisel juhul ei trükita arhiveeritud faili nime järel arhiveerija nime.

/CN – konteinerites asuvate objektide skaneerimiseks (HTML, RTF, PowerPoint). Kui võti (/CN) on märgitud, käsib see programmil nakatunud või kahtlaste failidega konteneri avastamisel kasutajat sellest informeerida. Võtme täiendamisel modifikaatoritega D, M või R teostatakse teised toimingud: /CND – kustutatakse; /CNM – teisaldatakse (vaikimisi kataloogi infected.!!!); /CNR – nimetatakse ümber (vaikimisi asendatakse laiendi esimene sümbol sümboliga #). Võti võib lõppeda ka modifikaatoriga N, sellisel juhul ei trükita välja konteineri tüüpi.

/CU – toimingud nakatunud failide ja ketaste käivitussektoritega. Parandatavad objektid parandatakse ning parandamatud failid kustutatakse, kasutamata täiendavat modifikaatorit D, M või R (kui parameetriga /IC ei ole määratud teisiti). Nakatunud failide puhul teiste toimingute teostamine: /CUD – kustutamine; /CUM – teisaldamine (vaikimisi kataloogi infected.!!!); /CUR – ümbernimetamine (vaikimisi asendatakse laiendi esimene sümbol sümboliga #).

/SPR, **/SPD** või **/SPM** – toimingud, mis teostatakse kahtlaste failidega, /SPR – ümbernimetamine, /SPD – kustutamine, /SPM – teisaldamine.

/ICR, **/ICD** või **/ICM** – toimingud, mis teostatakse nakatunud failidega, mida ei õnnestu parandada, /ICR – ümbernimetamine, /ICD – kustutamine,
/ICM – teisaldamine.

/MW – toimingud, mis teostatakse kõikide soovimatute programmidega. Kui võti (/MW) on märgitud, käsib see programmil kasutajat informeerida. Võtme täiendamisel

modifikaatoritega `D`, `M` või `R` teostatakse teised toimingud: `/MWD` – kustutamine; `/MWM` – teisaldamine (vaikimisi kataloogi `infected.!!!`); `/MWR` – ümbernimetamine (vaikimisi asendatakse laiendi esimene sümbol sümboliga `#`); `/MWI` – ignoreerimine. Teatud tüüpi soovimatute programmidega teostatavad toimingud määratakse võtmetega `/ADW`, `/DLS`, `/JOK`, `/RSK`, `/HCK`.

/DA – arvuti kontrollimine kord päevas. Järgmine kontrollimise kuupäev logitakse konfiguratsioonifaili ning seepärast peab sellele failile võimaldama ligipääsemise kirjutamiseks ja edaspidiseks ülekirjutamiseks.

/EX – konfiguratsioonifailis vaikimisi loetletud laienditega failide skaneerimine; kui fail on mitte saadaval, on nendeks laienditeks EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

Kui skaneeritud objektide nimekirjas on selgelt kirjeldatud laiendiga element ja see on märgitud spetsiaalsete sümbolitega `*` ja `?`, kontrollitakse mitte ainult laiendite nimekirjaga sobivaid faile, vaid kõiki faile, mis on määratud selle elemendiga.

/FN – Vene tähtede laadimine video kuvamise dekooderile (ainult Dr.Web DOS-ile puhul).

/GO – programmi pakettlaad. Kõik küsimused, mis eeldavad kasutaja vastamist, jäetakse vahele ning kõik valikut eeldavad lahendused viiakse täide automaatselt. See laad on kasulik failide

automaatsel skaneerimisel, näiteks e-kirjade 24-tunnisel kontrollimisel e-posti serverites.

/SHELL – skänneri GUI-versioonile. Võti keelab splash-akna kuvamise, mälu ja automaatkäivitusfailide kontrolli. Varem salvestatud nimekirju skaneeritavade failide ja kataaloogide teedega ei laeta skaneerimiseks. See laad võimaldab kasutada skänneri GUI-versiooni konsoolversiooni asemel, viimasega saab skaneerida ainult neid objekte, mis on määratud käsurea parameetritega.

/ST – seadistab skänneri GUI-versiooni nähtamatu töölaadi. Programm töötab, ilma, et avaneks ükski aken ja lõpetab ka iseseisvalt oma töö. Kui skaneerimise käigus tuvastatakse viiruslikke objekte, avaneb pärast skaneerimise lõppu siiski aken. See skänneri töölaad eeldab, et skaneeritavate objektide nimekiri määratakse käsureal.

/HA – failide heuristilise skaneermise võimaldamine tundmatute viiruste avastamiseks.

/INI:<path> – kasutab alternatiivset konfiguratsioonifaili määratud nime või teega.

/NI – mitte kasutada konfiguratsioonifailis `drweb32.ini` määratud parameetreid.

/LNG:<file_name> või **/LNG** – määratud nime või teega alternatiivse keeleressursi faili (`dwl`-faili) kasutamiseks, kui tee pole määratud, kasutatakse sisseehitatud (Inglise) keelt.

/ML – skaneeritakse e-posti formaadiga faile (UUENCODE, XXENCODE, BINHEX ja MIME). Kui võti (`/ML`) on määratud, käsib see programmil nakatunud või kahtlase objekti leidmisel meiliarhiivis kasutajat sellest informeerida. Võtme täiendamisel modifikaatoritega `D`, `M` või `R` teostatakse teised toimingud: `/MLD` - kustutamine; `/MLM` – teisaldamine (vaikimisi kataloogi `infected.!!!`); `/MLR` – ümbernimetamine (vaikimisi

asendatakse laiendi esimene sümbol sümboliga #). Võti võib lõppeda modifikaatoriga N, selisel juhul ei trükita teadet "Meiliarhiiv".

/NS – keelata arvuti skaneerimise katkestamine. Selle võtme kasutamisel ei ole kasutajal vajutades nupule [Esc] võimalik skaneerimist katkestada.

/OK – kuvab skaneeritud objektide täisnimekirja ning märgib nakkuseta objektide järgi Ok.

/PF – mitme disketi skaneerimisel järgneva disketi küsimine.

/PR – enne toimingu teostamist kinnituse küsimine.

/QU – skänner kontrollib käsureal määratud objekte (faile, kettaid, katalooge) ning seejärel lõpetab oma töö automaatselt (ainult skänneri GUI-versiooni puhul).

/RP<file_name> või **/RP**+<file_name> – logib võtmega määratud faili. Nime mittemääramisel logib vaikimisi nimega faili. Kui on määratud sümbol +, lisatakse uus logi eelmise lõppu, kui sümbolit ei ole määratud, luuakse uus.

/NR – mitte luua logifaili.

/SD – alamkataloogide skaneerimiseks.

/SO – helide võimaldamiseks.

/SS – käesoleval programmi käivitamisel konfiguratsioonifailis määratud sätete salvestamiseks programmi töö lõpetamisel.

/TB – kõvaketta käivitussektorite ja peamiste käivitussektorite (MBR) skaneerimiseks.

/TM – viiruste otsimiseks töömälus (kaasaarvatud Windows-i süsteemiala, võimalik ainult Windows-ile mõeldud skännerite puhul).

/TS – viiruste otsimiseks automaatkäivitusfailides (kataloogis `Autorun`, süsteemi ini-failides, Windows-i registris). Kasutatakse ainult Windows-i skännerite puhul.

/UP or **/UPN** – käivitatavate failide skaneerimiseks, mis on pakitud ASPACK, COMPACK, DIET, EXEPACK, LZEXE, jne.; failid, mis on konverteeritud BJFNT, COM2EXE, CONVERT, CRYPTCOM, jne., samuti ka failid, mis on immuniseeritud CPAV, F-XLOCK, PGPROT, VACCINE, jne. Skaneeritud failide pakkimiseks, konverteerimiseks ja vaktsineerimiseks kasutatud programmi nime kuvamise keelamiseks kasuta võtit `/UPN`.

/WA – programm ei lõpeta viiruste või kahtlaste objektide leidmisel tööd enne, kui vajtuatakse mõnda klahvi (ainult konsoolskännerite puhul).

/? – kuvab programmi abifaili.

Vaikimisi määratud töölaadid (kui konfiguratsioonifail pole saadaval või kasutusel) on kirjeldatud Tabelis 3.

Teatud parameetritele võib lõppu lisada sümboli "−". Parameetri "negatiivne" vorm tähendab töölaadi katkestamist. See valik on kasulik siis, kui töölaad on vaikimisi lubatud või konfiguratsioonifailis on varem mõni laad võimaldatud. Parameetrid, mille puhul on võimalik ka "negatiivne" vorm, on: `/ADW` `/AR` `/CU` `/DLS` `/FN` `/HCK` `/JOK` `/HA` `/IC` `/ML` `/MW` `/OK` `/PF` `/PR` `/RSK` `/SD` `/SO` `/SP` `/TB` `/TM` `/TS` `/UP` `/WA`

`/CU`, `/IC` ja `/SP` parameetrite puhul katkestab "negatiivne" vorm kõik toimingud, mis on loetletud nende parameetrite kirjelduses. See tähendab, et informatsioon nakatunud ja kahtlaste objektide kohta kajastub ainult logifailis.

Parameetrite `/INI` ja `/RP` puhul kirjeldatakse "negatiivset" laadi vastavalt `/NI` ja `/NR`.

`/AL` ja `/EX` puhul ei ole "negatiivne" vorm võimalik, kuid määrates ühe neist, lõpetab see teised kaks.

Kui käsureal on sisestatud mitu alternatiivset parameetrit, määrab programmi töölaadi viimasena sisestatud parameeter.

D3. Automaatse uuendamise mooduli käsurea parameetrid

Kui automaatse uuendamise tööriist töötab käivitatuna Planeerija poolt või käsureal, saad sa sisestada järgnevaid käsurea parameetreid:

/URL:<url of the updating server> – tunnustatakse ainult UNC-teid.

/USER:<user name of http-server> – uuenduste serveri kasutajanimi.

/PASS:<user password of http-server> – uuenduste serveri kasutaja salasõna.

/UPM:<proxy mode> – proksiserveri kasutuslaad, võib omada järgnevaid väärtuseid:

- direct – ära kasuta proksiserverit
- ieproxy – kasuta süsteemisätteid
- userproxy – kasuta kasutaja poolt määratud sätteid (Dr. Web tööriistaribal leht Uuendamine või määratud võtmetega /PURL /PUSER /PPASS)

/PURL:<proxy address> – proksiserveri aadress.

/PUSER:<proxy user name> – proksiserveri kasutajanimi.

/PPASS:<proxy user password> – proksiserveri kasutaja salasõna.

/UA – laeb alla kõik uuenduste nimekirjas olevad failid, sõltumata kasutatavast operatsioonisüsteemist ja installeeritud komponentidest. See laad on loodud Dr. Web uuenduste serverist täiskoopia saamiseks; laadi ei saa kasutada arvutisse installeeritud viirusetõrjeprogrammi uuendamiseks.

/ST – käivitab automaatse tööriista nähtamatult (varjatud laad).

/LNG:<file_name> – keeleressursside faili nimi; kui ei ole määratud, kasutatakse inglise keelt.

/GO – töötamine pakettlaadis, ilma dialoogideta.

/QU – automaatse uuendamise tööriista sulgemine pärast uuendamise lõpetamist; program suletakse sõltumata sellest, kas uuendamine õnnestus või mitte. Uuendamise õnnestumist saab kontrollida tagastatava koodiga drwebupw.exe (näiteks bat-failis errorlevel muutuja väärtus: 0 – õnnestunud, teised väärtused – ebaõnnestunud).

/DIR:<directory> – muudab kataloogi, kuhu paigutatakse uuendatud failid; vaikimisi on see kataloog, millest Tööriist käivitati.

/URM:<mode> – taaskäivitamise laad pärast uuendamist, võib omada järgnevaid väärtuseid:

- prompt – program teatab taaskäivitamise vajadusest pärast uuendusprotsessi lõpetamist
- noprompt – vajadusel toimub taaskäivitamine ilma vastava teateta
- force – taaskäivitab alati (sõltumata sellest, kas see on uuendamise protsessi lõpetamiseks vajalik)
- disable – keelab taaskäivitamise

/REG – käivitab uuendamise mooduli või registreerimise protsessi ja võtab vastu registreerimise võtmefaili.

/UPD – tavaline uuendamine; kasutatakse koos võtmega /REG: registreerimisprotsessile lisaks ka uuendamise käivitamiseks

/UVB – uuendatakse ainult viiruste andmebaasid (selle võtme määramisel keelatakse /UA).

/RP<file_name> või **/RP**+<file_name> – võtmes määratud faili logi kirjutamine. Kui nime pole määratud, logitakse

vaikimisi määratud faili. Sümboli + lisamisel lisatakse uus logi eelmise lõppu, kui sümbolit ei ole määratud, luuakse logifail uuesti.

/INI:<path> – määratud nime või teega alternatiivse konfiguratsioonifaili kasutamiseks.

/NI – mitte kasutada konfiguratsioonifailis drweb32.ini määratud parameetreid.

/NR – mitte luau logifaili.

/SO – võimaldab helid (ainult vigade puhul).

/DBG – logi detailid.

Vaikimisi määratud töölaadid (kui konfiguratsioonifail pole saadaval või kasutusel) on kirjeldatud Tabelis 3.

/SO parameteerile saab lõppu lisada sümboli "-". Parameetri "negatiivne" vorm tähendab töölaadi katkestamist. See valik on kasulik siis, kui töölaad on varem konfiguratsioonifailis määratud sätetega lubatud.

Parameetrite /INI ja /RP puhul kirjeldatakse "negatiivset" laadi vastavalt /NI ja /NR.

Kui käsureal on sisestatud mitu alternatiivset parameetrit, määrab programmi töölaadi viimasena sisestatud parameeter.

D4. Tagastatavad koodid

Tagastatavate koodide ning nendele vastavate sündmuste väärtused on järgnevad:

0 – OK, viiruseid ei leitud

1 – tuvastati tuntud viirus

2 – tuvastati tuntud viiruse modifikatsioon

4 – leiti kahtlane objekt

8 – failiarhiivis, meiliarhiivis või konteineris tuvastati tuntud viirus

16 – failiarhiivis, meiliarhiivis või konteineris tuvastati tuntud viiruse modifikatsioon

32 – failiarhiivis, meiliarhiivis või konteineris leiti kahtlane fail

64 – vähemalt üks nakatunud objekt parandati edukalt

128 – vähemalt üks nakatunud või kahtlane fail kustutati/nimetati umber/teisaldati

Programmi poolt tagastatud reaalne väärtus on võrdne skaneerimise käigus ette tulnud sündmuste koodide summaga. Summa saab lihtsalt jagada erinevate sündmuste koodideks.

Näiteks tähendab tagastatav kood 9 = 1 + 8 tuntud viiruste tuvastamist, seejuures viiruste tuvastamist arhiivides; parandamist ning teisi toiminguid ei teostatud; muid viiruslikke sündmuseid skaneermise käigus ei toimunud.

Lisa E. Dr.Web®-i komponentide reguleeritavad parameetrid

E1. Sissejuhatus

Programmi komponentide reguleeritavaid parameetreid säilitatakse põhiliselt programmi konfiguratsioonifailis (`drweb32.ini` asub installeerimiskataloogis). See on tekstiformaadiga fail ning tal on erinevate komponentide jaoks eraldi sektsioonid. Mistahes komponendi iga parameter on määratud vastavas sektsioonis tekstina

```
parameter = value
```

Parameetrite väärtuseid saab muuta ühel viisil järgnevatest:

- läbi vastava programmi kasutajaliidese (skänner, valvur, meilivalvur). Kõige tähtsam info nende sätete kohta on kirjeldatud eelpool (loe p. 3.2.3, 3.4.3,3.5.3)
- määrates parameetrid programmi käivitamisel käsurealt või ajagraafiku järgi (erinevate versioonide skänneri

puhul). Selle valiku kohta detailsema info saamiseks loe Lisa D

- redigeerides konfiguratsioonifaili mõne tekstiredaktoriga

Konfiguratsioonifaili redigeerimine on lubatud ainult kogenud kasutajatele. Faili redigeerimine ilma täieliku arusaamiseta viirusetrõje programmi struktuurist võib põhjustada viirusetõrje programmi kaitse usaldusväärsuse langemise või isegi programmi töötamast lakkamist.

Enne konfiguratsioonifaili redigeerimist deaktiveeri valvur ja meilivalvur viisil, nagu on kirjeldatud vastavates peatükkides.

E2. Windows-i versioonide skänneri, valvuri, planeerija ning uuendusmooduli parameetrid

Tabeli 3 veergudel on kirjeldatud iga parameetri kohta järgnevad andmed:

- parameetri nimi
- parameetrit kasutavate komponentide nimed
- parameetri nimi konfiguratsioonifailis
- parameetri väärtused
- käsurea võtmed

Parameetrite nimed on trükitud erinevalt – paksus kirjas on parameetrid, mis on vastavad kasutajaliidesele, ning peenes kirjas on parameetrid juhul, kui kasutajaliideses ei vasta nendele ükski parameeter.

Tabelis on kasutatud järgnevaid komponentide nimesid:

- "SpIDer" – mõlemad SpIDer Guard-i versioonid ("SpIDer-XP" ja "SpIDer-Me")
- "Skänner" – mõlemad skänneri versioonidr ("GUI-Skänner-GUI" ja "Konsoolskänner")

Kui mõnes reziimis puudub vastav konfiguratsioonifaili parameter, on parameetri väärtused kirjeldatud sulgudes ja seotud kasutajaliidese dialoogielemendiga või määratud käsurea võtmega.

Skänneri, planeerija ja uuendamismooduli vaikeväärtused on trükitud paksus kirjas, valvuri omad kaldkirjas ja kõikide komponentide omad paksus kaldkirjas.

Dr. Web Windows-i serveritele valvuri ja skänneri vaikeväärtused on alla joonitud juhul, kui nad erinevad tööjaamadele mõeldud versiooni vaikeväärtustest.

Antud parameetri vastavad käsurea võtmed on kirjeldatud lühidalt, ilma enamuste modifikaatoriteta. Detailse informatsiooni võtmete kohta leiab Lisast D.

Tabel 3. Skännerite Windows-ilversioonide, valvuri ja uuendamise mooduli reguleeritavad parameetrid

Parameeter	Komponendid	Konf. faili parameeter	Väärtused	Võtmed
"Lennult" skaneerimine	SpIDer	GuardMode	*Smart* RunAndOpen CreateAndWrite kaks viimast reziimi	
Skaneermisreziim	Skänner, SpIDer	ScanFiles	***All*** ByType ByMasks	/AL /EX
Heuristiline analüüs	Skänner, SpIDer	HeuristicAnalysis	***Yes*** / No	/HA
Viirusaktiivsuse kontroll	SpIDer	VirusActivityControl	*Yes* / No	
Käivitusdisketi skaneerimine	SpIDer	ScanBootOnShutDown	*Yes* / No	
Süsteemituuma kaitse	SpIDer-Me	DisableIDTHook	Yes / *No*	
Võrguskaneerimise keelamine	SpIDer-Me	DisableNetworkScan	*Yes* / No	
Mitte skaneerida objekte kohtvõrgus	SpIDer-XP		(Sees / *Väljas*)	
Mitte skaneerida objekte irdketastel	SpIDer-XP		(Sees / *Väljas*)	
Mälu skaneerimine	Skänner, SpIDer-Me	TestMemory	***Yes*** / No	/TM

Parameeter	**Komponendid**	**Konf. faili parameeter**	**Väärtused**	**Võtmed**
Automaatkäivitusfailide skaneerimine	Skänner, SpIDer	TestStartup	***Yes*** / No	/TS
Käivitussektorite skaneerimine	Skänner, SpIDer-Me	TestBootSectors	***Yes*** / No	/TB
Alamkataloogide skaneerimine	Skänner	ScanSubDirectories	***Yes*** / No	/SD
Järgneva disketi küsimine	Skänner	PromptFloppy	***Yes*** / No	/PF
Arhiivid	Skänner, SpIDer	CheckArchives	***Yes*** / No	/AR
Pakitud käivitatavad failid	Skänner, SpIDer	CheckPackedFiles	***Yes*** / No	/UP
E-posti failid	Skänner, SpIDer	CheckEMailFiles	***Yes*** / *No*	/ML
Maksimaalne faili suurus lahtipakkimisel, KB	SpIDer-XP	MaxFileSizeToExtract	*(tühi)*	
Arhiivi maksimaalse kokkusurumise tase	SpIDer-XP	MaxCompressionRatio	*(tühi)*	
Kontrollitava faili maksimaalne kohustuslik suurus KB	SpIDer-XP	CompressionCheckThreshold	*(tühi)*	
Laiendite nimekiri	Skänner, SpIDer	FilesTypes	***(vaata Tabelis allpool)***	
Maskide nimekiri	Skänner, SpIDer	UserMasks	***(vaata Tabelis allpool)***	
Välistatud kataloogide asukoht	Skänner, SpIDer	ExcludePaths	***(tühi)***	
Välistatud failid	Skänner, SpIDer-Me	ExcludeFiles	***(tühi)***	
Luba maskid	SpIDer-XP	AllowWildcards	Yes / *No*	

Parameeter	**Komponendid**	**Konf. faili parameeter**	**Väärtused**	**Võtmed**
Näidatud teeta failide väljajätmise lubamine	SpIDer-XP	AllowRelativeFileNames	Yes / *No*	
Kõvaketaste skaneerimine (kui skaneeritakse käsurea parameetriga * ja kui vajutatakse nuppu `Vali kettad`)	Skänner	ScanHDD	**Yes** / No	
Diskettide skaneerimine (kui skaneeritakse käsurea parameetriga * ja kui vajutatakse nuppu `Vali kettad`)	Skänner	ScanFDD	Yes / **No**	
Laserplaatide skaneerimine (kui skaneeritakse käsurea parameetriga * ja kui vajutatakse nuppu `Vali kettad`)	Skänner	ScanCD	Yes / **No**	
Võrguketaste skaneerimine (kui skaneeritakse käsurea parameetriga * ja kui vajutatakse nuppu `Vali kettad`)	Skänner	ScanNet	Yes / **No**	
Kinnituse küsimine	Skänner, SpIDer-Me	PromptOnAction	**Yes** / No	/PR
Laiendi ümbernimetamine	Skänner, SpIDer	RenameFilesTo	***#??***	
Tee ümbertõstmiseks	Skänner, SpIDer	MoveFilesTo	***infected.!!!***	
Viiruste andmebaaside asukoht	Skänner, SpIDer	VirusBase	*.vdb	
Faili poole pöördumise aja taastamine	Skänner, SpIDer	RestoreAccessDate	Yes / ***No***	

Parameeter	**Komponendid**	**Konf. faili parameeter**	**Väärtused**	**Võtmed**
Viiruste andmebaasi taaslaadimise lipufail	SpIDer	UpdateFlags	*drwtoday.vdb*	
Lipufaili kontrollimise periood, m	SpIDer	UpdatePeriod	*1m* *15m*	
Hüpikakna genereerimine	SpIDer-XP	Acknowledge	*Yes* / No	
Tee komponendi ajutiste failide kataloogini	Skänner, SpIDer	TempPath	**%TMP%, %TEMP%,** ***install. kataloog***	
Valvuri väljalülitamise võimaldamine	SpIDer	EnableSwitch	Yes / *No*	
Valvuri laadimisreziim	SpIDer-XP		Käsitsireziime *Automaatne reziim*	
"peatatud"-seisundi salvestamine sessioonide vahel	SpIDer-XP		(Sees / *Väljas*)	
Dr.Web konfiguratsioonifaili kaitsmine	SpIDer-XP		(Sees / *Väljas*)	
Täiendava kaitsereziimi keelamine	SpIDer-XP	DisableEnhancedProtection	*Yes* / No	
Skaneeritud failide nimekirja suurus	SpIDer-XP		*100*	

Parameeter	Komponendid	Konf. faili parameeter	Väärtused	Võtmed
Nakatunud objektid	Skänner, SpIDer	InfectedFiles	***Report*** ***Cure*** Delete Rename Move Lock (valvur) Shutdown (valvur)	/CU
Parandamatud objektid	Skänner, SpIDer	IncurableFiles	***Report*** Delete Rename ***Move*** Lock (valvur) Shutdown (valvur)	/IC
Kahtlased objektid	Skänner, SpIDer	SuspiciousFiles	*Report* Delete Rename *Move* Lock (valvur) Ignore (valvur) Shutdown (valvur)	/SP

Parameeter	Komponendid	Konf. faili parameeter	Väärtused	Võtmed
Nakatunud arhiivid	Skänner, SpIDer	ActionInfectedArchive	***Report*** Delete Rename ***Move*** Lock (valvur) Ignore (valvur) Shutdown (valvur)	/AR
Nakatunud e-posti failid	Skänner, SpIDer	ActionInfectedMail	***Report*** Delete Rename ***Move*** Lock (valvur) Ignore (valvur) Shutdown (valvur)	/ML
Nakatunud konteinerid	Skänner, SpIDer	ActionInfectedContainer	***Report*** Delete Rename ***Move*** Lock (valvur) Ignore (valvur) Shutdown (valvur)	/CN

Parameeter	Komponendid	Konf. faili parameeter	Väärtused	Võtmed
Reklaamvara programmid	Skänner, SpIDer	ActionAdware	***Report*** Delete Rename ***Move*** Ignore Lock (valvur) Shutdown (valvur)	/ADW
Helistavad programmid	Skänner, SpIDer	ActionDialers	***Report*** Delete Rename ***Move*** Ignore Lock (valvur) Shutdown (valvur)	/DLS
Naljaprogrammid	Skänner, SpIDer	ActionJokes	Report Delete Rename Move ***Ignore*** Lock (valvur) Shutdown (valvur)	/JOK

Parameeter	Komponendid	Konf. faili parameeter	Väärtused	Võtmed
Riskvara	Skänner, SpIDer	ActionRiskware	Report Delete Rename Move ***Ignore*** Lock (valvur) Shutdown (valvur)	/RSK
Muukvara	Skänner, SpIDer	ActionHacktools	Report Delete Rename Move ***Ignore*** Lock (valvur) Shutdown (valvur)	/HCK
Tegevus ümbernimetamise ebaõnnestumise korral	SpIDer-XP	ActionIfRenameFailed	Report *Delete* Rename Move *Lock* Shutdown	

Parameeter	Komponendid	Konf. Faili parameeter	Väärtused	Võtmed
Tegevus teisaldamise ebaõnnestumise korral	SpIDer-XP	ActionIfMoveFailed	Report Delete *Rename* Move Lock Shutdown	
Tegevus kustutamise ebaõnnestumise korral	SpIDer-XP	ActionIfDeleteFailed	Report Delete Rename Move *Lock* Shutdown	
Tegevus teatamise ebaõnnestumise korral	SpIDer-XP	ActionIfReportFailed	Report Delete Rename Move *Lock* Shutdown	
Arhiivide kustutamise lubamine kinnitust küsimata	Skänner, SpIDer	EnableDeleteArchiveAction	Yes / ***No***	
Leiti nakatunud objekt (teadete saatmine)	SpIDer-XP		(Sees / *Väljas*)	
Leiti parandamatu objekt (teadete saatmine)	SpIDer-XP		(Sees / *Väljas*)	

Parameeter	Komponendid	Konf. faili parameeter	Väärtused	Võtmed
Leiti kahtlane object (teadete saatmine)	SpIDer-XP		(Sees / *Väljas*)	
E-posti sõnumi saatmine viirusjuhtude puhul	SpIDer-XP		(Sees / *Väljas*)	
Teate saatmine viirusjuhtude puhul	SpIDer-XP		(Sees / *Väljas*)	
Faili logimine	Skänner, SpIDer, Uuendamise moodul	LogToFile	***Yes*** / No	/RP /NR
Logifaili kirjutamine	Planeerija		(**Sees** / Väljas)	
Logifaili nimi	Skänner SpIDer-Me SpIDer-XP	LogFileName	**drweb32w.log** *spider.log* *spidernt.log*	/RP
Logifaili nimi	Uuendamise moodul		**drwebupw.log**	/RP
Logifaili nimi	Planeerija		**drwebscd.log**	
Logimisviis	Skänner, SpIDer, Uuendamise moodul	OverwriteLog	Yes / ***No***	/RP
Logi kodeering	Skänner, SpIDer, Uuendamise moodul	LogFormat	***ANSI*** OEM	
Skaneeritud objektid logifailis	Skänner, SpIDer	LogScanned	***Yes*** / *No*	/OK
Failipakkijate nimed logifailis	Skänner, SpIDer	LogPacked	*Yes* / **No**	

Parameeter	**Komponendid**	**Konf. Faili parameeter**	**Väärtused**	**Võtmed**
Arhiveerijate nimed aruandes	Skänner, SpIDer	LogArchived	*Yes* / **No**	
Statistika logifailis	Skänner, SpIDer	LogStatistics	***Yes*** / No	
Logifaili maksimaalne suurus	Skänner, SpIDer, Uuendamise moodul	LimitLog	Yes / ***No***	
Logi suuruse limiit, KB	Skänner, SpIDer, Uuendamise moodul	MaxLogSize	***512*** ***8192***	
Akna sulgemine pärast sessioonide lõppu	Skänner, Uuendamise moodul	WaitAfterScan	Yes / **No**	/QU
Klahvivajutuse ootamine	Konsoolskänner		(Sees / **Väljas**)	/WA
Pakettreziimis töötamine	Skänner, Uuendamise moodul		(Sees / **Väljas**)	/GO
Kasutajapoolse katkestamise keelamine	Skänner		(Sees / **Väljas**)	/NS
Korra päevas skaneerimine	Skänner		(Sees / **Väljas**)	/DA
Ainult valitud objektide skaneerimine	Skänner-GUI		(Sees / **Väljas**)	/SHELL
Akende mitteavamine (nähtamatu reziim)	Skänner-GUI		(Sees / **Väljas**)	/ST
Alternatiivse konf.faili kasutamine. Mitte ühegi konf.faili kasutamine	Skänner, Uuendamise moodul		(Sees / **Väljas**)	/INI /NI

Parameeter	**Komponendid**	**Konf. faili parameeter**	**Väärtused**	**Võtmed**
Enda swap-faili kasutamine	Skänner, SpIDer	UseDiskForSwap	***Yes*** / No	
Edenemisriba kuvamine	Skänner	ShowProgressBar	**Yes** / No	
Helid	Skänner, SpIDer, Uuendamise moodul	PlaySounds	Yes / ***No***	/SO
Hoiatus (heli)	Skänner	AlertWav	alert.wav	
Parandatud (heli)	Skänner	CuredWav	cured.wav	
Kustutatud (heli)	Skänner	DeletedWav	deleted.wav	
Ümber nimetatud (heli)	Skänner	RenamedWav	renamed.wav	
Teisaldatud (heli)	Skänner	MovedWav	moved.wav	
Lõpetatud (heli)	Skänner	FinishWav	finish.wav	
Viga (heli)	Skänner, Uuendamise moodul	ErrorWav	error.wav	
Sätete automaatsalvestamine	Skänner	AutoSaveSettings	**Yes** / No	/SS
Ilma taaskäivituseta sätete muutmise keelamine	SpIDer-Me	DisableHotReconfigure	Yes / *No*	
SpIDer Guard ikooni näitamine tegumiribal	SpIDer-XP		(*Sees* / Väljas)	
Ikooni näitamine tegmuiribal	Planeerija		(**Sees** / Väljas)	

Parameeter	Komponendid	Konf. faili parameeter	Väärtused	Võtmed
Registri sätete kasutamine	Skänner-GUI		(**Sees** / Väljas)	
Skaneerimise prioriteet	Skänner	ScanPriority	**25** **50**	
Keel	Skänner, SpIDer, Uuendamise moodul	LngFileName	***et-drweb.dwl***	/LNG
Proksi reziim	Skänner-GUI for Uuendamise moodul	UpdateProxyMode	direct **ieproxy** userproxy	/UPM
Ainult viiruste andmebaaside uuendamine	Uuendamise moodul	UpdateVirusBasesOnly	Yes / **No**	/UVB
Uuenduste nimekirjast kõikide failide allalaadimine	Uuendamise moodul	UpdateAllFiles	Yes / **No**	/UA
Taaskäivitusreziim uuendamisel	Uuendamise moodul	UpdateRebootMode	**prompt** noprompt force disable	/URM
Detailide logimine	Uuendamise moodul		(Sees / **Väljas**)	/DBG

Faililaiendite nimekiri (parameetri `FilesTypes` väärtus) sisaldab vaikimisi järgnevaid laiendeid: EXE, COM, DLL, SYS, VXD, OV?, BAT, BIN, DRV, PRG, BOO, SCR, CMD, 386, FON, DO?, XL?, WIZ, RTF, CL*, HT*, VB*, JS*, INF, PP?, OBJ, LIB, PIF, AR?, ZIP, R??, GZ, Z, TGZ, TAR, TAZ, CAB, HLP, MD?, INI, MBR, IMG, CSC, CPL, MBP, SH, SHB, SHS, SHT*, MSG, CHM, XML, PRC, ASP, LSP, MSO, OBD, THE*, EML, NWS, SWF, MPP, TBB.

Valitud maskide nimekiri (parameetri `UserMasks` väärtus konfiguratsioonifailis) sisaldab vaikimisi väärtuseid, mis on formeeritud sümboli `*` ja punkti lisamisega faililaiendite nimekirjas oleva laiendi ette (näiteks "`*.exe`").

E3. SplDer Mail Windows-i tööjaamadele parameetrid

SpIDer Mail Windows-i tööjaamadele parameetrid on kirjeldatud Tabelis 4. Selle tabeli kujundus on sarnane Tabeli 3 omale. Parameetrite väärtuste nimekirjas on meilivalvuri vaikeväärtused trükitud kaldkirjas.

Tabel 4. Meilivalvuri reguleeritavad parameetrid

Parameeter	**Konf. faili parameeter**	**Väärtus**	**Võti**
Alternatiivse konfiguratsioonifaili kasutamine		(Sees / *Väljas*)	-ini:file_name
Alternatiivse kasutaja võtmefaili kasutamine		(Sees / *Väljas*)	-key:file_name
Keel	LngFileName	*ru-drweb.dwl*	-lng:file_name
Heuristiline analüüs	HeuristicAnalysis	*Yes* / No	
Arhiivifailide kontrollimine	CheckArchives	*Yes* / No	
Viirusaktiivsuse kontrollimine	VirusActivityControl	*Yes* / No	
Sõnumi skaneerimise timeout, s	ScanTimeout	*250*	
Lahtipakitava faili maksimaalne suurus, KB	MaxFileSizeToExtract	*30720*	
Maksimaalne kokkusurumise tase	MaxCompressionRatio	*Infinite*	
Maksimaalne arhiveerimise tase	MaxArchiveLevel	*64*	
Teatamine viirustest väljaminevas postis	ShowAlerts	*Yes* / No	
Nakatunud sõnumid	ActionInfected	*Delete* Move	

Parameeter	**Konf. faili parameeter**	**Väärtus**	**Võti**
Kahtlased sõnumid	ActionSuspicious	Delete *Move* Skip	
Kontrollimata sõnumid	ActionNotChecked	Delete Move *Skip*	
Modifitseeritud sõnumite kustutamine serverist	DeleteMessagesOnServer	*Yes* / No	
'X-AntiVirus'-päise lisamine sõnumitele	InsertXAntiVirus	*Yes* / No	
Karantiini tee	PathForMovedFiles	*infected.!!!*	
Dr.Web mootori tee	EnginePath	*(tühi)*	
Dr.Web viiruste andmebaaside tee	VirusBasesPath	*(tühi)*	
Uuendamise lipufail	UpdateFlag	*drwtoday.vdb*	
Lipufaili kontrollimise periood, s	UpdatePeriod	*300*	
Maksimaalselt laetavaid mootoreid	MaximumLoadEngines	*10*	
Eellaetavad mootorid	PreloadEngines	*1*	
Mittekasutatava mootori mahalaadimise timeout, s	UnusedEngineUnloadTimeout	*420*	

Parameeter	**Konf. faili parameeter**	**Väärtus**	**Võti**
Logimise lubamine	EnableLog	*Yes* / No	
Skaneerimise info logimise lubamine	EnableLogScanInfo	*Yes* / No	
Logi faili	LogFileName	*spiderml.log*	
Logifaili maksimaalne suurus, KB	MaximumLogSize	*500*	
Ikonnianimatsioonide lubamine	EnableIconAnimation	*Yes* / No	
Ikooni kuvamine tegumiribal	HideIcon	Yes / *No*	
Näita teateid	NoBalloons	*Yes* / No	
Võta ühendused üle automaatselt või **Ühenduste seadistamine käsitsi** raadionupud	HookModeAuto	*Yes* / No	
Kontrolli ühenduste ülevõtmist startimisel (aut.reziim)	HookCheck	*Yes* / No	
Aadress-Port (esimene element nimekirjas, aut.reziim)	Hook1	**:143* aadress:port	
Aadress-Port (järgmine nimekirjas, aut.reziim)	Hook2 Hook3 …	aadress:port aadress:port …	

Parameeter	Konf. faili parameeter	Väärtus	Võti
SpIDerMail port- Serveri aadress –Serveri port (käsitsireziim, nimekirja esimene element)	HookManual1	7000 -> aadress POP3/SMTP/IMAP4/NNTP: port	
SpIDerMail port- Serveri Aadress -Serveri Port (käsitsireziim, järgmine nimekirjas)	HookManual2 HookManual3 …	7001 -> aadress POP3/SMTP/IMAP4/NNTP: port 7002 -> aadress POP3/SMTP/IMAP4/NNTP: port …	
Luba menüüpunkt **vigane**	AllowDisable	Yes / *No*	
Luba menüüpunkt **Välju**	AllowExit	Yes / *No*	
Luba menüüpunkt **Sätted**	AllowSettings	*Yes* / No	
Luba menüüpunkt **Reinitialize**	AllowReinitialize	Yes / *No*	
Maksimaalne üheaegselt töödeldavate päringute arv ühes kohalikus pordis (käsitsireziim)	MaximumChildConnections	*20*	
Sõnumile lisatav tekst	Xbanner	*(tühi)*	
Tee komponendi ajutiste failide kataloogini	TempPath	*%TMP%, %TEMP%, installeerimiskataloog*	

Parameeter	Konf. faili parameeter	Väärtus	Võti
Reinitialize			-reinit
Keela			-disable
Luba			-enable
Uuenda			-update
Välju			-exit