F-PROT 2.25 Opas

Kääntäjän yhteystiedot

Timo Kinnunen
Särkiniementie 16 A 41
70700 Kuopio
Finland

~~+358 (9)17 2613618~~

Timo Kinnunen
~~mailto:ttokinnu@iwn.fi~~

klikkaa ylläolevaa sinistä linkkiä jos haluat lähettää sähköpostia (Linkki ei toimi enää).

Sisällys

F-PROT -asennus
F-PROT 2.25 komentorivioptiot
F-PROT 2.25 heuristinen analyysi
F-MACROW 1.02: yleistietoja
F-MACROW:n käyttö
F-MACROW käynnistysoptiot
F-MACROW automaattikäynnistys
F-MACROW tunnettuja ongelmia
F-MACROW Tunnistetut virukset
VIRSTOP komentorivikytkimet

Esitietoja

Olen suomentanut tämän juuri nyt lukemasi HTML -kielisen oppaan siitä syystä, että on monia, jotka haluavat tutustua tämäntapaisten ohjelmien ominaisuuksiin etukäteen ennen niiden käyttöönottoa.Näin on helppoa arvioida kannattaako ohjelmaa edes imuroida omalle koneelle, ja myöhemminkin tällaista opasta voi käyttää monin tavoin apuna. Valitettavasti ohjelman valmistaja ei tällaista palvelua tarjoa ainakaan suomenkielellä, ja ei ainakaan tällaisissa tutustumispainoksissa. Toinen syy tämän käännöksen olemassaololle on se, että tässä nimenomaisessa versiossa on liitteenä hyvä selvitys ohjelmien kytkimistä, mikä tieto saattaa kiinnostaa joitakin. En ole tehnyt tätä opasta kenenkään toimeksiannosta, vaan alunperin omaksi hyödykseni, ja opiksi - ja siitä syystä tämä teksti on hyväksyttävä sellaisenaan, ja kaikki esitetty kritiikki on turhaa, ja lähinnä ajanhukkaa. Tästä oppaasta ei voi aiheutua minulle mitään oikeudellisia seuraamuksia koskien F-PROT ohjelman mahdollista väärinkäyttöä, tai näiden ohjeiden virheellistä tulkintaa, tai ymmärtämättömyttä, tai painovirheitä. Tästä samasta syystä kenenkään ei myöskään tarvitse maksaa minulle tästä työstä yhtään mitään. En kuitenkaan takaa, että teen näitä automaattisesti aina kun uusia F-PROT -ohjelmaversioita ilmaantuu, sillä ei tämä sellainen automaatti ole, ja sellaisissa tapauksissa puhutaan tietenkin jo rahasta, koska olisi joku joka haluaa teettää jonkin työn, ja tämä työ toistuu useita kertoja. En usko tällaista tapahtuvan. Jos joku haluaa välttämättä lukea alkukieliset tekstitiedostot, ovat ne aina saatavilla siinä arkistotiedostossa, jossa F-PROT -ohjelmaa jaetaan.

Alkuaan tähän ympätyt tekstit olivat siis englannikielisiä, ja sellaisina niiden esittäminen vaikkapa vain tällaisessa HTML -muodossa ei palvele mitään järjellistä päämäärää, sillä ne jotka osaavat kieliä, ja F-PROT -ohjelmaa käyttävät, osaavat lukea asiat kyseisistä ASCII -tiedostoistakin. Mutta niissäkin asiat ovat sijainneet erillisissä tekstitiedostoissa, ja niiden välillä ei ole välttämättä helposti hahmotettavissa olevia yhteyksiä - sinänsä kätevää kääntämisen kannalta. En kuitenkaan ole sisällyttänyt tähän luetteloa kaikista niistä viruksista joita F-PROT kykenee joko huomaamaan, tai huomaamaan ja tuhoamaan. Saat niistä tietoa jos imuroit ohjelman itsellesi. Tämä kyseinen luettelo on lisäksi pitkä. Sitävastoin olen liittänyt tähän luettelon niistä Word -makroviruksista, jotka ohjelman 2.25 -versio [19.12.1996] tunnistaa.

Nyt luettelo voi olla pitempikin.

Yleisenä huomiona totean, että F-PROT on tavallaan saapunut eräänlaiseen tienhaaraan, josta toista tietä menee Word-makrovirusten -ja toista tietä DOS-ohjelmavirusten hyökyaalto. Molempia ei voi enää seurata samalla välineellä. Lue erityisesti kohta F-MACROW tunnettuja ongelmia. Ja kaikki kunnia islantilaiselle **Fridrig Skulanssonille**

Jää Salka Valka Islantiin

F-PROT -asennus

F-PROT -ohjelman asennus on helppoa: kopioidaan vain kaikki pakatussa tiedostossa olevat tiedostot johonkin hakemistoon. AUTOEXEC.BAT -tiedostoon voidaan lisätä komentorivi VIRSTOP ohjelman automaattiseksi käynnistämiseksi. Ohjelma voidaan myös asettaa käynnistyväksi CONFIG.SYS -tiedostosta. Huomattakoon, että Windows 95:n menestyksekäs asennus edellyttää, ettei muistissa ole toimivia viruksentorjuntaohjelmia. Toisaalta ei ole ollenkaan suositeltavaa asentaa VIRSTOP -ohjelmaa käynnistymään kun Windows 95 -järjestelmä käynnistetään. Jos F-PROT -ohjelmaa halutaan ajaa Windows 95:ssä, voidaan käyttää sen komentorivikehoite-tilaa. Sitävastoin F-MACROW soveltuu hyvin käytettäväksi Windows 95:ssä.

VIRSTOP2 on parannettu versio VIRSTOP -ohjelmasta, ja siksi sitä tulisi käyttää mikäli mahdollista. Niiden komentorivikytkimet poikkeavat toisistaan hieman. Ja vielä kerran: Näitä kumpaakaan ei ole suunniteltu toimimaan Windows 95 -ympäristössä. VIRSTOP2 toimii kuitenkin Windows 3.1 ja Työryhmä-Windows 3.11 -ympäristössä, koska niissähän pohjalla toimii aina MS-DOS -järjestelmä. Se ei kuitenkaan ole yhtä monipuolinen kuin F-PROT -ohjelma.

Jos VIRSTOP -ohjelmaa halutaan kuitenkin käyttää, voidaan CONFIG.SYS - tiedostoon kirjoittaa komentorivit:

DEVICE=C:\F-PROT\VIRSTOP.EXE

tai jos käytät DOS 5 (tai 6):

DEVICEHIGH=C:\F-PROT\VIRSTOP.EXE

Muistinhallintaohjelmien (386MAX, HIMEM) käynnistysrivien tulee sijaita ennen VIRSTOP -komentoriviä. VIRSTOP kykenee tunnnistamaan onko se ITSE saastunut "stealth" -viruksesta. Monasti se myös kykenee tunnistamaan, yritetäänkö tällaisia ohjelmia ajaa - vaikka ne sijaitsisivatkin muistissa.

F-PROT 2.25 komentorivioptiot

F-PROT.EXE -ohjelma käynnistetään tavallisesti kirjoittamalla pelkästään ohjelman nimi (F-PROT) ja painamalla ENTER -näppäintä. Tällöin ohjelma toimii vuorovaikutteisessa muodossa - eli kaikki sen valinnat tehdään valikoista, ja niiden vaihtoehdoista. Jos tämä ohjelma käynnistetään komentoriviltä, ja komento annetaan optioiden kanssa, ohjelma ei "keskustele" käyttäjän kanssa, vaan suorittaa tehtävän optioiden mukaisesti.

Saatavissa olevat komentorivioptiot ovat:

/640

Tietyissä vanhoissa koneissa ei-käytettävissä olevan muistinosan (640K-1MB) skannaus voi kaataa järjestelmän. Tämä optio varmistaa sen, että F-PROT skannaa vain [perus]muistialueen 1-640KB.

/ALL

Tämän kytkimen valinta määrää ohjelman tarkistamaan kaikki tiedostot. Tätä kytkintä ei tulisi koskaan käyttää /ANALYSE kytkimen kanssa yhdessä, vaan ainoastaan tapauksissa, joissa järjestelmästä on löydetty virus, ja halutaan tarkistaa, ettei se "piileksi" jossakin "overlay" -tiedostossa.

/ANALYSE

Tämän kytkimen vaikutuksesta ohjelma suorittaa heuristisen analyysin "Secure" -skannauksen jälkeen. Tämä lähestymistapa voi aiheuttaa vääriä hälytyksiä, ja siksi sitä tulisi käyttää varoen.

/APPEND

Käytetään /REPORT -kytkimen kanssa, ja sen vaikutus on se, että raportti liitetään olemassaolevan raporttitiedoston perään.

/AUTO

Voidaan käyttää /DELETE tai /DISINF -kytkinten kanssa, jolloin ohjelma ei kysy lupaa ennen [tiedoston] tuhoamista, tai disinfektointia. Oletusavona on se, että järjestelmä kysyy näitä jokaisen epäilyttävän tiedoston kohdalla.

/BOOT (oletusarvo) /NOBOOT

Skannaa/Ei skannaa alkulataussektoreita.

/COMMAND

Pakottaa ohjelman komentorivimoodiin.

/DELETE

Tuhoaa kaikki tartunnan saaneet tiedostot sensijaan, että vain luettelee ne.

/DISINF

Disinfektoi milloin se vain on mahdollista - tuhoaa ensimmäisen polven otokset ja myös tiedostot, jotka ovat tuhoutuneet virusten ylikirjoituksen takia. Tämän kytkimen valintaa aiheuttaa sen, ettei tiedostoa koskaan tuhota mikäli se voidaan disinfektoida.

/DOC

Skannaa Word-dokumentteja.

Huomaa tässä yhteydessä erityisesti se, mitä on sanottu F-Macrow -ohjelmasta, ja sen paremmasta kyvystä tuhota tehokkaasti makroviruksia.

/EXT=

Tällä optiolla voidaan spesifioida millä tarkentimilla varustettuja tiedsotoja skannataan oletusarvoisesti, maksimimäärä on 10.

Esimerkki: /EXT=COM.EXE.SYS.DLL.OV?

/FILE (oletusarvo) /NOFILE

Skannaa/Ei skannaa tiedostoja. Jos /NOFILE -optiota käytetään, se viittaa sekä /NOPACKED että /NOUSER -kytkimiin.

/GURU

Tarjoaa lisäinformaatiota skannauksen aikana.

/HARD

Skannaa MBR:n ja kaikki saavutettavissa olevat partitiot kiintolevyllä.

/HELP tai /?

Näyttää saatavissa olevien optioiden luettelon.

/INTER

Pakottta ohjelman interaktiiviseen muotoon.

/LIST

Tuottaa luettelon KAIKISTA tarkistetuista tiedostoista.

/MONO

Käyttää mustavalkomuotoa värinäytöillä.

/MULTI

Skannaa useita levykkeitä peräjälkeen.

/NET

Skannaa löydetyt verkkoasemat.

/NOBREAK

Poistaa ESC ja ^C pois käytöstä skannauksen ajaksi.

/NODOC

Ei skannaa Word-dokumentteja.

/NOMEM

Ei skannaa muistia.

/NOSUB

Ei skannaa alihakemistoja.

/NOWRAP

Ei sovelleta "wrap" toimintoa raportin tekstiin.

/OLD

Ei tuota näyttöön ilmoitusta:

"*This version of the program is rather old*"

Tällainen ilmoitus tulee näyttöön kun ilmaisjakeluversio saavuttaa tietyn iän. Ohjelma toimii tietenkin tämänkin jälkeen, mutta se ei ole vain enää"uusin mahdollinen".

/ONLY

Käytettäessä /ANALYSE -kytkimen kanssa, F-PROT suorittaa **PELKÄSTÄÄN** heuristisen analyysin.

/PACKED (oletusarvo) /NOPACKED

Etsii/Ei etsi pakattujen tiedostojen sisäpuolella (DIET, PKLITE, LZEXE). Tämä ei tarkoita sitä, että F-PROT etsii arkistotiedostoista (ZIP tai ARJ). PKLITE ja LZEXE ovat työkaluja, joiden avulla voidaan tiivistää ohjelmatiedostoja, sekä jopa Windows 3.0:n DLL-kirjastoja - kuten uudemmilla PKLITE-ohjelmaversioilla. Ohjelmatiedosto koodataan tiivistettäessä niin, että ohjelmassa olevat "toistuvat ja samanlaiset ilmaisut" koodataan kukin ryhmittäin lyhyemmillä koodeilla, jotka kirjastoisaan ohjelman loppuun, ja niitä varten luodaan konsepti, jonka mukaan koodit "laajennetaan" alkuperäiseen kokoonsa. Jos käytetään "äärimmäistä" tiivistystä PKLITE -ohjelman rekisteröidyssä versiossa, lisätään tiivistetyn ohjelmatiedoston alkuun "PK" -signatuuri, josta ohjelma voi käynnistyessään tarkistaa onko se yhä tiivistetyssä tilassa. LZEXE on tarkoitettu pelkästään .EXE tiedostojen tiivistämiseen, ja kyseeseen tulevat tavallisesti vain DOS-tiedostot. ZIP ja ARJ -tiedostot ovat samantapaisia tiivistettyjä tiedostoja, mutta tavallisesti niihin on "pakattu" useita erillisiä tiedostoja, jotka eivät välttämättä kaikki ole ohjelmia, tai edes missään vuorovaikutussuhteessa toisiinsa. Monasti niitä kuitenkin käytetään ohjelmistopaketin luomiseen ja lähettämiseen.

/PAGE

Pitää tauon jokaisen sivun jälkeen.

/PARANOID

Tämä kytkin tekee skannerista todella vainoharhaisen, ja se lisää uusien virusten poimituksi tulemisen mahdollisuutta, mutta samalla myös virheilmoitusten määrän kasvamista. Tätä kytkintä ei suositella muiden kuin kokeneiden ja teknisesti orientoituneiden käyttäjien työkaluksi.

/RENAME

Nimeää saastuneet tiedostot tarkentimilla *.VOM, *.VXE tai *.VVV.

/REPORT=file

Lähettää tulokset tiedostoon sen lisäksi, että tuottaa ne näytölle.

/SILENT

Aiheuttaa sen, ettei näytölle ilmaannu mitään toiminnasta huolimatta. Käyttökelpoinen kytkin mikäli haluat ajaa ohjelman eräajotiedostolla, ja pelkästään tarkistaa paluukoodin.

/USER /NOUSER (oletusarvo)

Etsii/Ei etsi käyttäjän määrittelemiä hakusanoja, tai niiden ketjuja. Tätä optiota tulisi käyttää mikäli se on ehdottoman välttämätöntä, sillä se aiheuttaa nopeuden hidastumista.

Paluutila

Ohjelma käyttää seuraavia exit-koodeja, jotka voidaan tarkistaa BAT -tiedoston ERRORLEVEL komennolla.

0 - Normaali paluu - mitään ei löytynyt.
1 - Epätavallinen lopetus - korjaamaton virhe. Tämä voi tarkoittaa jotakin seuraavista:

- DOS versio 1.x oli käytössä (F-PROT vaatii DOS 2.0 tai uudempaa)
- Raporttitiedostoa (spesif. /REPORT=) ei voitu luoda.
- ENGLISH.TX0 tai SIGN.DEF vioittuneita, tai ei lainkaan saatavissa
- Ohjelma käynnistettiin ensin levykkeeltä, jonka jälkeen levykettä on vaihdettu.

2 - Itsetakistus epäonnistui - ohjelmaa on käsitelty.

3 - Alkulataus/Tiedosto virus löydetty.

4 - Viruksenetsintä hakusanaketju löydetty muistista.

5 - Ohjelman toiminta päättynyt käyttäen ^C tai ESC.

6 - Ainakin yksi virus poistettu. Tällä koodilla on merkitystä vain jos ohjelma tutki yhtä tiedostoa.

7 - Muisti ei riitä ohjelman ajamiseen.

8 - Ainakin yksi epäilyttävä tidosto löytynyt, mutta ei infektioita.

F-PROT ja heuristinen analyysi

Virustenetsintä käyttäen hakusanoja, tai lauseita ei ole lopullinen ratkaisu virusten aiheuttamaan ongelmaan. Kun käytetään päivitettyä skanneria (tai paremminkin kahta eri valmistajien sovellusta) voidaan saavuttaa varmuus siitä, että kaikki tunnetut virukset tunnistetaan. Skannerit voivat tunnistaa vanhojen virusten variantit - tai olla tunnistamatta, mutta jos uusi virus on kirjoitettu alusta alkaen kokonaan uudelleen, voi olla, että se jää tunnistamatta, koska siinä ei ehkä ole yhtään olemassaolevaa tunnistamiseen tarvittavaa lauseketjua. Virus voidaan tunnistaa tarkkailevalla ohjelmalla aina kun virusohjelma aktivoituu - esimerkiksi sen perusteella, että se yrittää suorittaa jotakin epäilyttävää toimenpidettä, kuten esimerkiksi alustaa kiintolevyä uudelleen. Virus voidaan myös määrittää tarkistussummaohjelmalla, mikä määrittää tiedostojen tai alkulatauslohkon muutoksia senjälkeen kun ne ovat saaneet jo tartunnan. Kuitenkin on kaikkein suositeltavinta käyttää tunnistamiseen sellaista tapaa, jossa se voi tapahtua ilman, että tunnistamiseen tarvittaisiin ohjelman käynnistystä. Heuristinen analyysi on periaatteessa pieni asiantuntijasysteemi, joka on asettanut säännöt virusten kuvaukseen, ja yrittää soveltaa niitä ohjelmiin joita se analysoi. Analyysi on vielä kokeellisella asteella, ja se ei ole virheetön - joitakin viruksia ei vieläkään voida paikantaa tällä tavoin, ja satunnaisia virheilmoituksia on myös odotettavissa.

Tällä hetkellä (~~19.12.1996~~) joidenkin ohjelmien tiedetään aiheuttavan virheilmoituksia:

1. Kaikkien ohjelmien, jotka on suojattu HyperLOCK enkryptausohjelmalla ... mikä ei ole ihmekään,

koska se väittää:

"*Attemping to reverse engineer this software may result in data loss*".

2. Kaikkien ohjelmien, jotka on suojattu PROTECT enkryptausohjelmalla.

3. Joidenkin ohjelmien, jotka käyttävät usean kerroksen anti-debuggaustekniikoita - kuten XTG.EXE (Xtree Gold).

4. RXINTMGR.COM

5. Joidenkin Central-Point PC-Tools ohjelman tiedostojen.

Mikäli heuristinen raportti väittää jotakin ei-ajettavissa olevaa tiedostoa epäilyttäväksi, on kyseessä melko varmasti väärä hälytys, sillä heuristinen menetelmä on tarkoitettu ajettavissa olevien tiedostojen analyysiin. Tästä syystä sinun ei **KOSKAAN** tulisi valita tutkittavaksi kaikkia tiedostoja.

Kokeneet käyttäjät toivoisivat käyttävänsä /PARANOID -kytkintä heuristisessa analyysissä - mutta tämä vain lisää virheilmoitusten määrää, joten älä käytä sitä.

F-MACROW 1.02: yleistietoja

F-MACROW on 16-bittinen Windows-sovellus, joka soveltuu käytettäväksi seuraavissa [Microsoftin] järjestelmissä:

- Windows 3.1
- Työryhmä-Windows 3.11
- Windows 95
- Windows NT (3.51 ja 4.0 beta 2)

F-Macrow ei toimi DOS:n alaisuudessa, mutta eivätpä makrovirukset DOS-ohjelmia vaivaakaan.

F-MACROW:n käyttö

Tämä ohjelma asennetaan käyttäen asennusohjelmaa. Kun olet asentanut tarvittavat tiedostot asennusohjelmalla, voit käynnistää ohjelman kaksoisklikkaamalla ohjelman ikonia. Asennetaessa Windows 95:een käyttäjät voivat käynnistää ohjelman myös DOS-kehoitteesta. Ohjelman käyttö on yksinkertaista. Kun ohjelmaan on ensimmäisessä käynnistyksessä määritelty se hakemisto, josta makroviruksia etsitään, sekä se tiedosto, ja tapa, jolla raportti luodaan, voidaan ohjelma käynnistää. Klikataan vain scan-painiketta, jolloin näyttöön ilmaantuu ohjelman asetuksista kertova valikko. Jos etsintä tapahtuu WinWord -ohjelman hakemistosta /WINWORD, olipa se sitten jonkin toisen hakemiston alihakemistona tai ei. Hyvä vaihtoehto on asentaa WinWord -ohjelma hakemistoon MSOFFICE, ja asentaa sinne kaikki tähän ohjelmaperheeseen kuuluvat muutkin ohjelmat, kuten Microsoft Excel -esimerkkinä. Kun tämä MSOFFICE -hakemisto asetetaan oletukseksi, niin F-MACROW etsii ja löytää kaikki dokumentit, tyyli yms. -jotka saattavat sisältää makroviruksia. Jos käytössä on myös Excel -ohjelma, löytyvät myös sen dokumenttitiedostot samalla kertaa.

Seuraavat optiot ovat käytettävissä:

Scan all drives

Skannataan kaikki levyasemat (paitsi levykeasemat). CD-ROM -asemat voidaan jättää optiona skannaamatta.

Scan directory

Valitaan skannattava hakemisto.

What to scan

Valitaan skannataanko Word tai Excel -tiedostoja, (*.DOC, *.DOT, *.XL?), vai skannataanko kaikkia tiedostoja.

Scan Subdirectories

Skannataanko spesidioidun hakemiston alihakemistoja.

If a virus is found

Määritetään, mitä tehdään, kun virus on löytynyt:

Report only.

Raportoidaan viruksesta.

Ask each time.

Käyttäjältä kysytään vahvistus joka kerta kun virus tuhotaan.

Disinfect automatically.

Virus poistetaan kysymättä.

Report all scanned documents

Tavallisesti ohjelma raportoi ainoastaan ne tiedostot, joista on löydetty virus. Jos tarkistus tehdään tämän option mukaan, raporoidaan kaikki skannatut tiedostot.

Report file

Valitse tämä optio jos haluat että raportti tallennetaan tiedostoon, ja määritä se, millä tavoin tämä tapahtuu.

Vasta kun halutut optiot on valittu, käynnistetään haku, joka voidaa keskeyttää painamalla ESC -näppäintä, tai STOP -painiketta.

Lopuksi ohjelmasta poistutaan **EXIT** -painikkeesta.

F-MARCOW käynnistysoptiot

Ohjelma hyväksyy seuraavat käynnistysoptiot:

/ALLDRIVES

Skannaa kaikki levyt (paikalliset ja muualla sijaitsevat, mutta ei levykeasemia).

/HARD

Skannaa kaikki paikalliset levyt (paitse levykeasemia).

/NET

Skannaa kaikki verkkolevyasemat.

/NOCDROM

Ei skannaa CD-ROM asemia käytettäessä /ALLDRIVES tai /HARD -optioita.

/CDROM

Skannaa CD-ROM asematkäytettäessä /ALLDRIVES tai /HARD -optioita.

/DEFDIR

Skannaa siinä hakemistossa, joka on määritelty F-MACROW.INI -tiedostossa.

/DOC

Skannaa vain *.DOC, *.DOT ja *.XL? tiedostot.

/ALLFILES

Skannaa kaikki tiedostot riippumatta niiden tarkentimista.

/SUB

Skannaa spesifioudun hakemiston alihakemistot.

/NOSUB

Ei skannaa spesifioidun hakemiston alihakemistoja.

/SCAN

Kun virus on löydetty, siitä vain raportoidaan.

/DISINF

Joka kerta kun virus löydetään, kysytään käyttäjältä tuhotaanko se.

/AUTO

Virukset tuhotaan automaattisesti aina löydettäessä.

/REPORT=

Nimetään raporttitiedosto. Tiedostonimen on oltava välittömästi "=" -merkin jälkeen ilman välilyöntejä. On hyvä, jos saantipolku määritellään tarkasti. Esimerkiksi:

/REPORT=D:\FOO\BAR\REPORT.TXT

jos kenttään kirjoitetaan vain tiedoston nimi, tallentuu se samaan hakemistoon jossa ohjelma itse sijaitsee.

/APPEND

Uusi raportti lisätään olemassaoleva raporttitiedoston perään.

/OVERWRITE

Uusi raportti kirjoitetaan entisen päälle.

/LIST

Kaikki skannatut tiedostot luetteloidaan raportissa.

/NOLIST

Vain sairaat tiedostot luetteloidaan.

/MINI

Ohjelma ajetaan minimoituna.

/HIDDEN

Ohjelma ajetaan taustalla kätkettynä.

/DONTQUIT

Ohjelma päättyy automaattisesti kun se on tarkistanut määritellyn hakemiston, ja ei ole löytänyt mitään. /DONTQUIT -optio estää tämän. Jos käyttäjä tekee jotakin typerää, kuten määrittää sekä /HIDE -että /DONTQUIT -optiot vallitseviksi, ohjelma "näyttää" itsensä kun se on lopettanut skannauksen.

Tällä hetkellä vain yksi hakemisto voidaan spesifioida kerrallaan. Jos spesifioidaan vain levyaseman kirjain, skannataan se kaikkine alihakemistoineen. Ohjelma voidaan opastaa skannaamaan ainoastaan vallitseva hakemisto kirjoittamalla levyaseman jälkeen piste:

(esimerkiksi, D:.)

Mikäli hakemistonimi sisältää välilyöntejä, täytyy spesifioitu hakemisto esittää rajattuna lainausmerkein:

(esimerkiksi, "C:\My Documents")

F-MACROW automaattikäynnistys

Windows 95:ssä F-MACROW -ohjelma on nyt mahdollista käynnistää sijoittamalla linkkitiedosto:

Käynnistä-valikko/ Ohjelmat /käynnistys

kohtaan. Tällöin F-MACROW ajetaan aina kun Windows 95 käynnistetään. Tällaisen järjestelyn järkevyydestä voi tietystikin olla montaa eri mieltä, koska jos esimerkiksi oma henkilökohtainen koneesi on ollut sammutettuna välillä, ja sitä käynnistettäessä suoritetaan tällainen tarkistus, ei asiassa ole mieltä, koska ei sinne ole mitenkään voinut ilmaantua makroviruksia tällä välin, ellei joku ole niitä sinne välillä käynyt asentamassa, ja jotka voivat toimia lisäksi vain jos sellainen tiedosto, jossa niitä on, luetaan asianomaisella ohjelmalla. Järkevämpää on suorittaa ajo aina kun järjestelmään on tuotu muualta Word-dokumenttitiedostoja, tai Excel -tiedostoja.

F-MACROW tunnettuja ongelmia

F-MACROW aiheuttaa GPF:n [General Protect Fairlure = yleinen suojausvirhe] skannatessaan joitakin dokumentteja.

Nämä dokumentit ovat korruptoituneita, ja Word (tai mikä tahansa OLE 2 -sovellus) kaatuu yrittäessään avata niitä. Virhe on Microsoftin kirjastoissa **STORAGE.DLL** ja **COMPOBJ.DLL**. Tuleva F-MACROW välttää näiden kirjastojen käyttöä. F-MACROW skannaa vain OLE2 -tiedostoja. Tämän seuraamuksena se ei tunnista Word 2.0 -dokumenteissa olevia makroviruksia, tai troijalaisia hevosia. Näiden dokumenttien formaatti on erilainen kuin Word 6.0:n tuottamien tiedostojen formaatti. Jos F-MACROW löytää viruksen tiedostosta, on sen havainto **AINA** luotettavampi kuin F-PROT -ohjelman - varsinkin tapauksissa, joissa F-PROT ei virusta tunnista lainkaan. Ne OLE2 -tiedostot, joissa Word 6.0 tai uudemmat ohjelmaversiot säilyttävät dokumenttejaan, ovat uskomattoman mutkikkaita rakenteeltaan - itse asiassa ne ovat tiedostojärjestelmiä tiedostojen sisällä: Niissä on oma FAT, juurihakemisto, alihakemistot (storages), ja tiedostot (streams). F-MACROW käyttää standardeja kirjastoja (DLL), joita

on saatavissa jokaisessa Windows-installaatiossa näiden struktuurien kartoittamiseen. Microsoft on toimittanut meille lähdekoodin tärkeimpiin funktioihin näissä tiedostoissa, mutta ne ovat valtavia - noin 150 Kb kompiloituina. Kun on esitetty toiveita, että F-PROT -ohjelmaan istutettaisiin näiden ylläkuvattujen ohjelmapiirteiden hallinta, on todettava, ettei niille ole tilaa F-PROT -ohjelmassa - ja kun näitä ominaisuuksia ei siinä ole, niin F-PROT ei myöskään ymmärrä näitä tiedostoja. OLE2 -tiedosto voi olla myös fragmentoitunut samaan tapaan kuin DOS-tiedostojärjestelmä. Loogisesti toisiaan seuraavat osat voivat olla eri osissa OLE2 -tiedostoa. Jos fragmentaatio osuu keskelle jotakin F-PROT:n käyttämää koodia, ei ohjelma löydä virusta. F-PROT:n tapa käsitellä viruksia on erilainen kuin esimerkiksi Microsoftin SCANPROT -ohjelman, joka jättää "viruksen kuolleen ruumiin" OLE2 -tiedoston käyttämättömään osaan, ja merkitsee sen käyttämättömäksi. Koska F-PROT -ohjelmalla ei ole "käsitystä" OLE2 -tiedostojärjestelmästä, se ei kykene tunnistamaan näitä osia käytöstä poissa oleviksi. Tästä syystä se voi aiheuttaa virheellisiä hälytyksiä. Tästä syystä F-PROT:n makrovirusten tunnistamiskyky poistetaan ohjelmasta lähitulevaisuudessa. Käyttäjät voivat käyttää sen sijaan F-MACROW -ohjelmaa.

F-MACROW Tunnistetut virukset

FormatC (Trojan) / Switches(Trojan) / Concept.L.Drp (Trojan) / Concept.M.Drp (Trojan) / Outlaw.C.Drp(Trojan) / Reflex.Drp(Trojan) / Laroux(Excel) / Alien / Alliance / AntiConcept / Atom.A / Atom.B / Atom.C /Atom.D / Atom.E / Atom.F / Bandung.A / Bandung.B / Bandung.C / Bandung.D / Bandung.E / Bandung.F / Birthday:De / Boom:De / Buero:De / Colors.A / Colors.B / Colors.C / Colors.D / Colors.E / Colors.F / Colors.G / Colors.H / Clock:De / Concept.A / Concept.B:Fr / Concept.C / Concept.D / Concept.E / Concept.F / Concept.G / Concept.H / Concept.I / Concept.J / Concept.K:NL / Concept.L / Concept.M / Concept.N (Intended) / Concept.O:Tw / Concept.P / Concept.Q / Concept.R / Concept.S / CountTen.A / CountTen.B / Daniel.A / Daniel.B / Date / Dietzel:De / Divina.A / Divina.B / Divina.C / DMV / Doggie / Easy / Friendly:De / Gangsterz / Goldfish / Hassle / Helper / Hot / Hybrid / Imposter.A / Imposter.B / Irish / Johnny / KillDLL / Look.A:Tw / Look.B:Tw / Look.C:Tw / Look.D:Tw / Lunch.A / Lunch.B / MadDog.A / MadDog.B / Magnum / MDMA.A / MDMA.B / MDMA.C / MDMA.D / Minimal / NF / NiceDay / Niki:It / NJ-WMVCK.A / NJ-WMVCK.B / NOP.A:De / NOP.B:De / Npad.A / Npad.B / Npad.C / Npad.D / Npad.E / Npad.F / Nuclear.A / Nuclear.B / Nuclear.C / Nuclear.D / Nuclear.E / Olympic.A:Tw / Olympic.B:Tw / Outlaw.A / Outlaw.B / Outlaw.C / Paper / Phantom / Phardera / Polite / Rapi.A / Rapi.A1 / Rapi.A2 / Rapi.B / Rapi.B1 / Rapi.B2 / Rapi.C / Rapi.C1 / Rapi.D / Rapi.D1 / Rapi.D2 / Rapi.E2 / Reflex / Satanic / Saver:De / ShowOff / Smiley:De / Spooky:De / Stryx:De / Target.A:De / Target.B:De / Tedious / Tele:De / Theather.A:Tw / Theather.B:Tw / Twister / Twno.A:Tw / Twno.B:Tw (Intended) / Twno.C:Tw / Twno.D:Tw / Waverley / Wazzu.A / Wazzu.AA / Wazzu.B / Wazzu.C / Wazzu.D / Wazzu.E / Wazzu.F / Wazzu.G / Wazzu.H / Wazzu.I / Wazzu.J / Wazzu.K / Wazzu.L / Wazzu.M / Wazzu.O / Wazzu.P / Wazzu.Q / Wazzu.R / Wazzu.S / Wazzu.T / Wazzu.U / Wazzu.V / Wazzu.W / Wazzu.X / Wazzu.Y / Wazzu.Z / Wazzu.AA / Wazzu.AB / Weather.A:Tw / Weather.B:Tw / Xenixos:De.

VIRSTOP komentorivikytkimet

VIRSTOP tottelee seuraavia komentorivikytkimiä:

/DISK:X

Ei tallenna hakusanaketjuja muistiin, vaan lukee ne sensijaan levyltä. Tällainen järjestely vähentää muistintarpeen aina 3500 bittiin. "X" -viittaa siihen levyasemaan jonne kaksi "heittovaihetiedostoa":

_VIRSTOP.TMP

(johon tallentuu se osa muistia, jonka VIRSTOP itse ylikirjoittaa)

_VIRSTOP.SWP

(joka on VIRSTOP -ohjelman kopio)

Huomautus:

Jos levyasemaa ei määritellä, on se C:

Aseman tulisi olla nopea, paikallinen asema - ei verkkoasema. RAM -levyasemat ovat ihanteellisia.

/DISK

Kytkintä voidaan nyt käyttää myös ajettaessa ohjelmaa levykeasemasta, ja jos levykettä vaihdetaan. Älä kuitenkaan käytä tätä kytkintä jos käytät DEVICEHIGH -komentoa. Kuitenkin LOADHI -komento näyttäisi toimivan.

TÄTÄ KYTKINTÄ EI KÄYTETÄ VIRSTOP2 -OHJELMAA KÄYTETTÄESSÄ - KOSKA SE AINA ASETTAA LEVYLLE HEITTOVAIHETIEDOSTON.

/OLD

Ilmoitusta ohjelman "vanhuudesta" ei tule näytölle. Tämän kytkimen käyttöä ei suositella.

/REHOOK

Asetu uudelleen osoitteeseen INT 21h, jos VIRSTOP ladattiin ennen Netwarea, tai vastaavaa ohjelmaa, joka ottaa haltuunsa "lataa ja käynnistä" -toiminnon.

/NOTRACE

Tätä kytkintä käytettäessä VIRSTOP toimii oikein vaikka käytössä olisikin vanha, ja ei täysin Intel-yhteensopiva Cyrix 486SLC -prosessori. Kytkin korjaa myös joitakin 386MAX -yhteensopivuusongelmia. Tämän kytkimen käyttö tekee VIRSTOPin vastustuskyvyttömäksi "stealth" -viruksia vastaan.

VIRSTOP2 EI VÄLTTÄMÄTTÄ TUE TÄTÄ KYTKINTÄ

/NOMEM

Ei suorita muistin skannausta.

/FREEZE

Pysäyttää tietokoneen viruksen löydyttyä.

/[NO]COPY

[Älä] tarkista tiedostot kun ne löydetään/ kopioidaan. Oletusarvona on /NOCOPY.

/[NO]BOOT

[Älä] tarkista alkulataussektorit kun levyke otetaan käyttöön. Oletusarvo /BOOT.

/[NO]WARM

[Älä] tarkista levykeasemaa A: wkun käyttäjä painaa Ctrl-Alt-Del. Oletusarvo /NOWARM.