

## Das Virensuchprogramm

# VIRSCAN PLUS

(VSP)

Gegen bekannte und unbekannte DOS  
Computerviren, mit integriertem Vi-  
renkiller

---

Copyright (c) 1989-2004 by ROSE Softwareentwicklung  
(ROSE SWE)



Dipl.-Ing. Ralph Roth  
Finkenweg 24, D 78658 Zimmern o. R.  
[rose\\_swe@gmx.net](mailto:rose_swe@gmx.net)  
[http://come.to/rose\\_swe](http://come.to/rose_swe)

ALL RIGHTS RESERVED! - ALLE RECHTE VORBEHALTEN!

---

Druckdatum: Dienstag, 6. April 2004  
Revision: 28



## Disclaimer

Das in diesem Handbuch enthaltene Material dient nur Informationszwecken und kann ohne vorherige Ankündigung geändert werden.

Alle anderen in diesem Handbuch verwendeten Warenzeichen, Markennamen, Dienstleistungsmarken und Dienstleistungsbezeichnungen, die Eigentum oder eingetragene Warenzeichen anderer Unternehmen sind, sind Eigentum der entsprechenden Unternehmen.

ROSE SWE übernimmt keine Verantwortung für Fehler oder Auslassungen in diesem Handbuch und verpflichtet sich nicht, die darin enthaltenen Informationen auf den neuesten Stand zu bringen.

# 1 Inhaltsverzeichnis

<b>DAS VIRENSUCHPROGRAMM .....</b>	<b>1</b>
DISCLAIMER .....	3
<b>1 INHALTSVERZEICHNIS.....</b>	<b>4</b>
<b>2 EINLEITUNG .....</b>	<b>8</b>
2.1 ZWECK VON VIRSCAN PLUS (VSP).....	8
2.2 HINWEIS FÜR ERFAHRENE ANWENDER.....	8
2.3 KURZBESCHREIBUNG DES PROGRAMMS VIRSCAN.....	9
2.3.1 <i>Verfügbare Funktionen von VirScan</i> .....	10
2.3.2 <i>Weitere Vorteile von VirScan</i> .....	10
2.3.3 <i>Warum gerade VirScan?</i> .....	11
2.3.4 <i>Technisches zum Programm VirScan Plus</i> .....	12
2.4 DAS VIRSCAN PLUS HANDBUCH .....	12
2.5 URHEBERRECHT .....	13
2.6 SHAREWARE.....	13
2.6.1 <i>Das Sharewareprinzip</i> .....	13
2.7 WAS SIND EIGENTLICH COMPUTERVIREN? .....	14
<b>3 STARTEN VON VIRSCAN.....</b>	<b>16</b>
3.1 WÄHREND DES SUCHLAUFES.....	16
3.2 NACH DEM SUCHLAUF .....	17
<b>4 UNTERSTÜTZTE PARAMETER .....</b>	<b>18</b>
4.1 PARAMETERSYNTAX.....	18
4.2 DIE UMGEBUNGSVARIABLE ‚VIRSCAN‘ .....	18
4.2.1 <i>Zurücksetzen von voreingestellten Werten</i> .....	19
4.2.2 <i>VirScan per AUTOEXEC.BAT Datei konfigurieren</i> .....	19
4.2.3 <i>Beispiele für das Setzen der Umgebungsvariable</i> .....	19
4.3 BSP.: TÄGLICHE KURZE PRÜFUNG PER AUTOEXEC.BAT DATEI .....	20
<b>5 DIE EINZELNEN PARAMETER.....</b>	<b>21</b>
5.1 /? ODER -? (HILFESTELLUNG) .....	21
5.2 /ALL (ALLE DATEIEN ÜBERPRÜFEN) .....	21
5.3 /ANALYSE .....	21
5.4 /AUTO (AUTOPILOT AKTIVIEREN) .....	21
5.4.1 <i>Beispiele für den weiteren Einsatz des Autopiloten</i> .....	22
5.5 /BATCH (BATCHMODUS) .....	23
5.6 /BOOT (BOOTVIREN SUCHEN) .....	23
5.7 /CDROM (CD-ROM SCANNEN).....	23
5.8 /CONT (FORTLAUFENDES SCANNEN) .....	24
5.9 /D (DIRECTORY) ODER <VERZEICHNIS>.....	24
5.10 /DEL (DELETE/LÖSCHEN VON DATEIEN) .....	24
5.11 /EXTR (SIGNATUR EXTRAHIEREN) .....	24
5.12 /FSUCHMASKE ODER SUCHMASKE (EINZELNE DATEIEN UNTERSUCHEN) .....	25
5.13 /H (/HILFE ODER /HELP) .....	25
5.14 /IVT (INTERRUPT VIRENTTEST).....	26
5.15 /JN (VOR DEM LÖSCHEN ABFRAGEN).....	26
5.16 /KILL (VIRENKILLER AKTIVIEREN) .....	27
5.16.1 <i>Allgemeine Hinweise zum Virenkiller</i> .....	27
5.16.2 <i>Entfernen von Boot- und Partitionsviren</i> .....	28
5.16.3 <i>Hinweise bei Mehrfachinfektionen</i> .....	28
5.16.4 <i>Virus kann nicht entfernt werden?</i> .....	28

5.17 /LAPTOP (UNTERSTÜTZUNG FÜR LAPTOPS) .....	28
5.18 /LESEN (ANLEITUNG LESEN) .....	28
5.19 /LOG UND /LOG= (REPORTDATEI ANLEGEN) .....	29
5.20 /MEHR (MEHRERE DISKETTEN NACHEINANDER UNTERSUCHEN) .....	29
5.21 /MEM (MEMORY) .....	30
5.22 /MEMHI (HOHER ARBEITSSPEICHER) .....	30
5.23 /MUTANT (NACH MUTIERTEN VIREN SUCHE) .....	30
5.24 /NOMEM (ARBEITSSPEICHER NICHT UNTERSUCHEN) .....	31
5.25 /NOPART (PARTITIONSTABELLE NICHT SCANNEN) .....	31
5.26 /NOSCRIP (NICHT NACH SCRIPTVIREN SUCHE) .....	31
5.27 /NOTROJ (NICHT NACH TROJANISCHEN PFERDEN SUCHE) .....	32
5.28 /OFFSET (OFFSET ANZEIGEN) .....	32
5.29 /PROZ - INFORMATIONEN ZUM PROZESSOR .....	32
5.30 /PRT ODER /PRN ODER /PRINTER .....	32
5.31 /Q (QUIET) .....	32
5.32 /REG (REGISTRATION) .....	32
5.33 /REP (REPORT) .....	33
5.34 /SHOWLOG= (REPORTDATEI BETRACHTEN) .....	33
5.35 /SICHER (SICHERHEITSMODUS) .....	33
5.36 /SPEICHER (SPEICHERBELEGUNG) .....	33
5.37 /TURBOAUS (NICHT IM TURBO-MODUS SUCHE) .....	34
5.37.1 WARNUNG .....	34
5.38 /ULTRA (SCHNELLERES SUCHVERFAHREN) .....	34
5.39 /UNB (UNBEKANNTE VIREN SUCHE) .....	34
5.40 /VL (VIREN-LISTE) .....	35
5.41 /VTC .....	36
5.42 /WIN (KOMPATIBILITÄT ZU WINDOWS) .....	36
5.43 /ZEIT (NICHT AUF UNÜBLICHE ZEIT ÜBERPRÜFEN) .....	36
5.44 LW: (LAUFWERKE) .....	36
5.45 BEISPIELE FÜR AUFRUFE .....	37
<b>6 SONSTIGE FUNKTIONEN .....</b>	<b>38</b>
6.1 VIRSCAN UNTER WINDOWS .....	38
6.2 VIRSCAN UNTER WINDOWS 9X UND WINDOWS NT/2000 .....	38
6.3 VIRSCAN UNTER OS/2 .....	39
6.4 VIRSCAN UNTER NETZWERKE .....	39
6.5 HINWEISE FÜR NETZWERKADMINISTRATOREN .....	39
6.6 ZUSÄTZLICHE FEHLERMELDUNGEN .....	40
6.7 SUCHGESCHWINDIGKEIT .....	41
6.8 WIE WERDEN NEUE VIRENERKENNUNGEN IN VIRSCAN AUFGENOMMEN? .....	41
6.9 WIE ERZEUGEN SIE EINE ERKENNUNG .....	42
<b>7 FEHLALARM? JA/NEIN? .....</b>	<b>43</b>
7.1 BEKANNTE FEHLALARME (MIT DER OPTION /UNB) .....	43
7.1.1 Programme die einen Fehlalarm erzeugen .....	43
7.1.2 WARNUNG: Option /TURBOAUS UND /UNB .....	43
7.2 VIRENBEFALL VON BOOTSEKTOREN .....	44
7.3 VIRENBEFALL VON DATEIEN .....	44
7.3.1 Ein Virus in nur einer Datei .....	44
7.3.2 Mehrere Viren in einer Datei/Bootsektor .....	44
7.4 DIE AM WEITESTEN VERBREITETEN VIREN .....	44
7.5 DIE PROGRAMME GUARD.SYS, VDEFEND.SYS, DEFENDER.COM UND TSAFES.COM U.A. ....	46
7.6 MEHRERE VIREN IM ARBEITSSPEICHER .....	46
7.7 ANALYSE BEI VIRENVERDACHT .....	47
7.8 UNBEKANNTE ODER MUTIERTE VIREN .....	47
<b>8 NEUE FUNKTIONEN UND WISSENSWERTES ÜBER VIRSCAN PLUS .....</b>	<b>48</b>
8.1 VERÄNDERUNGEN DER EINZELNEN PROGRAMMVARIANTEN .....	48
8.2 VIRSCAN UND EIN UNÜBLICHES DATEIDATUM .....	49
8.2.1 62-Sekunden/100 Jahre Viren .....	49

8.3 VIRSCAN UND STEALTH VIREN .....	50
8.3.1 Der Parity_Boot, AntiExe, Ripper Virus (u. a.).....	50
8.4 SUCHVERFAHREN MITTELS PLATZHALTER .....	50
8.5 DER DATEIENDEBUGGER .....	51
8.5.1 Bedeutung von "Typ" .....	52
8.5.2 Bedeutung von "Ext" .....	52
8.6 DER INTEGRIERTE VIRENSCHUTZ .....	53
8.6.1 Der eingebaute Checksummentester.....	53
8.6.2 Hinweise für das Programm SCAN.EXE.....	54
8.6.3 Hinweise für die Programme TAV & FShield.....	54
8.7 VIRSCAN UND ARBEITSSPEICHER .....	54
<b>9 ALLES WISSENSWERTE ÜBER VIREN.....</b>	<b>56</b>
9.1 KURZBESCHREIBUNG ALLER VIREN.....	56
<b>10 REGISTRATION, BESTELLUNGEN UND SONSTIGES.....</b>	<b>57</b>
10.1 REGISTRIEREN .....	57
10.2 KEYDATEI FÜR VIRSCAN PLUS .....	57
10.3 ANFRAGEN .....	59
10.3.1 Adresse .....	59
10.3.2 Kommerzielle Anwender.....	59
10.4 SONSTIGES .....	60
10.4.1 Ein Dankeschön an.....	60
10.4.2 Garantiausschlussklärung .....	60
<b>11 ENDE DES HANDBUCHES.....</b>	<b>61</b>



## 2 Einleitung

### 2.1 Zweck von VirScan Plus (VSP)



Mit VirScan werden Dateien, Laufwerke, Netzwerke, Arbeitsspeicher, der Partitionssektor und der Bootsektor auf Virenbefall untersucht.

### 2.2 Hinweis für erfahrene Anwender

'**DOS-Power User**' und sonstige Anwender, die der Meinung sind, dass sie dieses Handbuch erst lesen müssen, wenn ein Virus die Festplatte total zerstört hat, raten wir folgendes:

- n Zuerst VirScan mit INSTALL installieren bzw. bei
- n ZIP Datei: pkunzip -d vsp\*.zip verwenden!
- n RAR Datei: rar x vsp\*.\* oder unrar vsp1270.rar
- n Anschließend die Datei VIRSHELP.TXT ausdrucken lassen. Diese Datei enthält eine '**Quick Referenz**' für die Bedienung des Programms (liegt der Vollversion ausgedruckt bei).
- n VirScan wie folgt starten (maximale Sicherheit!):

**VirScan -auto /unb /boot**

(Mit Autopilot nach bekannten, unbekanntem (/unb) und zusätzlich nach Bootviren (/boot) suchen). Minus (-) entspricht Slash (/)!

- n Wenn VirScan etwas gefunden hat, eventuell (falls es nicht zuviel Mühe ist - ja, 20 weitere Programme müssen noch ausprobiert werden-) dennoch das Handbuch lesen. Dies kann durch folgende Befehle veranlasst werden:

**Ausdrucken:** copy virscan.doc lpt1:  
**Lesen:** VirScan /lesen

- n** Wenn Sie die Sharewareversion benützen und Sie meinen, dass das Programm sein Geld wert ist, geben Sie folgendes ein:

#### **REGISTER**

und ein kompletter Bestellschein wird ausgedruckt.

## **2.3 Kurzbeschreibung des Programms VirScan**

VirScan Plus ist ein Programm zum Erkennen und Suchen von Computerviren, Würmern, Scriptviren und trojanischen Pferden auf IBM kompatiblen PC-Rechnern. VirScan kann in der aktuellen Version mehrere tausend verschiedene Viren entdecken. Die Bedienung ist denkbar einfach, so kann VirScan z. B. mit zusätzlichen Parametern gestartet werden, andernfalls fragt das Programm den Benutzer, welche der Optionen gewünscht wird. VirScan ist durch die Optimierung in Assembler und seinen eingebauten "Debugger" sehr schnell. Für die bekanntesten Viren enthält VirScan Plus zusätzlich ein Killerprogramm, welches den Virus entfernen kann. Das Programm wird mit mehreren Hilfsprogrammen und Hilfsdokumenten zur Virenerkennung ausgeliefert. VirScan Plus ist lauffähig auf PC-Rechnern (286'er oder höher).

## 2.3.1 Verfügbare Funktionen von VirScan

- Arbeitsspeicher untersuchen. Komplett (640 KB/ 1 MB) oder im Turbo-Modus.
- Datenträger im Turbo-, Ultra-Modus oder im Sicherheitsmodus untersuchen.
- Befallene Dateien löschen (wahlweise mit Bestätigen).
- Soweit wie möglich Virus entfernen (VirScan kann zurzeit die bekanntesten Viren entfernen).
- Mehrere Disketten/Festplatten nacheinander untersuchen.
- Ausgabe auf Bildschirm und/oder Drucker bzw. in eine Datei; Erstellen eines Reports.
- Lesen des Handbuches, der Kurzhilfe oder Anzeige aller Viren, die VirScan erkennt.
- Untersuchen von Laufwerken, Netzwerken, CD-ROM, Dateigruppen und einzelner Verzeichnisse manuell oder mittels '**Autopiloten**'.

## 2.3.2 Weitere Vorteile von VirScan

- Der Boot- und Partitionssektor und das Programm VirScan werden jedes Mal mit überprüft.
- Neue Virensignaturen können in die Dateien VIRSCAN.EXT und VIRSCAN.TRJ aufgenommen werden.
- Alle zeitkritischen Funktionen wurden zusätzlich in Assembler optimiert.
- Für etwaige Fragen stehen mehrere Dokumentationen zur Verfügung. Die Anleitung zu VirScan kann als Handbuch ausgedruckt werden.
- VirScan ist lauffähig auf allen Graphikkarten. Ein Laufwerk oder eine Festplatte und MSDOS ab Version 4.0, sowie ein IBM kompatibler Rechner mit 520 KB freiem Speicher sind erforderlich.
- Verschiedene Suchverfahren finden auch nicht konstante Virenstämme (z. B. VCL, PS\_MPC, Jerusalem oder Tremor) und deren Abarten. VirScan findet -wahlweise- auch neue Viren, die durch Modifizieren bestehender Viren entstehen (sog. "Mutanten")! VirScan kann auch wahlweise nach noch unbekanntem Viren suchen! Ferner werden unübliche Dateiattribute oder defekte bzw. zerstörte Programme erkannt.
- Es wird eine Textdatei (VIRBIBEL.DOC) mitgeliefert, die eine kurze Beschreibung zu ca. 4000 Viren ent-

hält. Ferner sind dem Programm weitere hilfreiche 'Antivirentools' beigelegt.

- VirScan kann teilweise noch unbekanntes im Arbeitsspeicher, Boot- und Partitionssektor und in Programmen befindliche Tarnkappenviren erkennen!
- VirScan kann regelbasierend neue Scriptviren und Würmer erkennen. So wurde beispielsweise VBS.LoveLetter und VBS.NewLove regelbasierend erkannt!
- VirScan kann Netzwerke untersuchen. Läuft auch in der 'DOS-Box' des Betriebssystem OS/2 Version 2.1 & Warp sowie in der DOS Emulation von Windows 3.1x/95/386/2000/XP und NT 4.0
- Das Programm ist komplett in deutscher Sprache. Inklusive Installationsprogramm!
- VirScan Plus wird u. a. nach dem Sharewareprinzip vermarktet. Mehrplatzlizenzen für Netzwerke sind ebenfalls erhältlich.

### 2.3.3 Warum gerade VirScan?

Sie werden sich vielleicht fragen, warum Sie gerade VirScan verwenden sollen? Folgende Gründe sprechen für VirScan:

1. VirScan ist speziell auf den deutschen Markt zugeschnitten. Was nützt Ihnen der beste Virenschanner, der nicht deutsche Viren erkennt! Zudem ist VirScan komplett in Deutscher Sprache.
2. VirScan ist einer der schnellsten Virenschanner überhaupt (eingebauter 'Turbobugger').
3. VirScan erkennt auch noch unbekanntes oder modifizierte Viren. VirScan kann hoch komplex verschlüsselte Viren erkennen.
4. VirScan hat einen intelligenten Codeanalyser integriert und kann damit (fast) alle Viren klassifizieren. VirScan verwendet im Gegensatz zu anderen Virenschannern sog. Familienerkennungen, womit VirScan oft noch veränderte (mutierte oder neue) Viren erkennen kann, wo andere Virenschanner schon lange nichts mehr finden! VirScan kann somit:
  - 'First Generation' Samples erkennen
  - Bei Virenfamilien die einzelnen Mutanten anhand des Codeaufbaues unterscheiden.

- Bei Virenfamilien die einzelnen Mutanten anhand der Codelänge klassifizieren.
5. VirScan verwendet sog. AVR-Module, um hochgradig verschlüsselte Viren und ganze Virenstämme sicher erkennen zu können. So findet das AVR-Modul für Mini/Tiny Viren alleine 360 verschiedene Mini-, Tiny- und Trivial-Viren. Theoretisch ist es nicht möglich, einen Mini-Virus zu schreiben, der NICHT mit dem AVR-Modul entdeckt werden kann!
  6. Die AVR-Module sind 'zukunftsicher', das heißt, sie erkennen schon heute Viren, die morgen erst entwickelt werden. Dank des Codeanalyser kann VirScan jedoch diese Viren schon heute sicher klassifizieren und den Virenfamilien zuordnen!
  7. VirScan ist der einzige Virens Scanner der regelbasiert nach Script Viren und Würmer suchen kann.

### 2.3.4 Technisches zum Programm VirScan Plus

VirScan überprüft normalerweise nur ausführbare Programme, die z.B. auf EXE, COM, BIN, OVL, OVR, SYS, APP oder OBJ enden, sowie Dateien, in denen sich Scriptviren einnisten können. Es können selbstverständlich über Parameter andere "Extensionen" (Endungen) gewählt werden.

Der Virensuchalgorithmus ist zwar hoch optimiert, aber alleine jede Datei einzeln nach allen Viren zu durchsuchen, braucht seine Zeit. Wir nehmen jedoch an, Sie werden überrascht sein, wie schnell VirScan Ihre Festplatte untersucht!

## 2.4 Das VirScan Plus Handbuch

Dieses Handbuch wurde mit WORD erstellt und einem vom Programmator entwickeltem Hilfsprogramm nach ASCII portiert (VirScan.DOC) bzw. nach dem PDF Format konvertiert (VirScan.PDF). Sie können deshalb dieses Handbuch auf JEDEM Drucker, der mindestens 64 Zeilen pro Blatt und einen Seitenvorschub unterstützt, ausdrucken (auch auf Laserdruckern).

**Befehl:**            **COPY VIRSCAN.DOC        LPT1**

Zum Betrachten der Datei VirScan.PDF benötigen Sie den Acrobat Reader Version 4.0 oder höher.

## 2.5 Urheberrecht

Der Programmautor - Ralph Roth - besitzt alle Rechte an diesem Computerprogramm UND seiner begleitenden Dokumentationen. Eine Vervielfältigung des Programms und/oder der Dokumentation ist ohne schriftliche Genehmigung des Autors untersagt und stellt eine Urheberrechtsverletzung dar!

Eine Ausnahme stellt die Sharewareversion des Programms dar:

- Anwender dürfen dieses Programm kopieren und weitergeben.
- Sharewarehändler dürfen nach schriftlicher Genehmigung das Programm als Shareware vertreiben.



**Das Verändern des Programms und/oder der Dokumentation ist strengstens verboten!**

## 2.6 Shareware

VirScan wird u. a. nach dem sog. Sharewareprinzip vertrieben, d. h. Sie bestellen sich bei einem Sharewarehändler die Sharewareversion von diesem Programm. In der Regel verlangt der Sharewarehändler hierfür eine Vermittlungsgebühr, die zwischen 1 und 10 Euro liegt. Mit dieser Gebühr haben Sie jedoch nicht das Programm gekauft, sondern nur dem Händler seine Auslagen für Werbung, Kopieren usw. bezahlt!

### 2.6.1 Das Sharewareprinzip

Das Programm versteht sich als Shareware, dass heißt, Sie dürfen es testen und ausprobieren. Wenn Sie aber damit länger als vier Wochen arbeiten, wird eine Registrations-

gebühr fällig. Shareware können Sie also risikolos austesten. Falls Ihnen das Programm zusagt, kaufen Sie sich eine Vollversion.

Falls dieses Programm als Shareware-Programm angeboten wird, darf das Programm unentgeltlich weitergegeben werden, wenn die zugehörigen Dateien nicht verändert und nicht weggelassen werden (gilt nicht für die Vollversion). Registrierte Anwender dürfen natürlich die Vollversion **nicht** weitergeben!

Die kommerzielle Nutzung der Sharewareversion (in Firmen, öffentlichen Anstalten, Schulen etc.) ist untersagt. Für die oben aufgeführte Registrationsgebühr erhalten Sie die Vollversion und den neuesten und aktuellsten Programmupdate (neueste Programmversion).

Unterstützen Sie das Sharewarekonzept durch Ihre Registrierung! In der Vollversion fallen die Aufforderungsbildschirme weg! Außerdem erhalten Sie mit Ihrer Bestellung die derzeit aktuellste Programmversion!

Zum Bestellen ihrer persönlichen Vollversion starten Sie bitte das Programm REGISTER.COM und ein Bestellschein wird ausgedruckt. Für weitergehende Hinweise über das Sharewareprinzip wird zusätzlich auf die Datei HINWEIS.COM hingewiesen!

## 2.7 Was sind eigentlich Computerviren?



Bei Computerviren handelt es sich um Programme, die Dateien bzw. Programme befallen. Sie "hängen" sich in den meisten Fällen an das Ende eines Programms und vergrößern es in der Regel zwischen 1000 und 4000 Bytes.

Nach dem Aufruf des infizierten Programms wird zuerst das Programm, dann der angehängte Virus in den Arbeitsspeicher geladen. Beim Starten des Programms durch das Betriebssystem wird jetzt zuerst der Virusteil angesprungen. So kann der Virus entweder das geladene Programm manipulieren oder ein neues angreifen. Anschließend springt der Virus zum eigentlichen Programm über. Durch diese Taktik merkt der Computerbenutzer normalerweise nicht, dass seine Programme von einem Virus infiziert sind. Falls Sie mehr zu Viren wissen möchten, dann lesen Sie bitte das Kapitel "ALLES WISSENSWERTE ÜBER VIREN".

Wie alle anderen Programme auch, befindet sich ein Computervirus als ein kleines Programm namenlos im Arbeitsspeicher. Diese wenige Kilobytes Programmcode enthalten aber für den Virus spezifische Maschinenbefehle, an denen er erkannt werden kann (die sog. Virensignaturen).

## 3 Starten von VirScan

Legen Sie die VirScan Diskette in Laufwerk A ein und geben Sie folgendes ein:

```
A: [ENTER]
VirScan [ENTER]
```

VirScan wird dann gestartet, gibt einen kurzen Hilfsbildschirm aus, und fragt Sie anschließend nach verschiedenen Parametern, die Sie eingeben müssen (siehe unten). Wenn Sie später mit VirScan vertraut sind, können Sie VirScan so aufrufen, dass er alle benötigten Parameter aus der Kommandozeile liest.



Wenn VirScan alle Dateien untersucht hat und ein Virus gefunden wurde, drücken Sie die ENTER Taste. Falls **KEIN** Virus gefunden wurde, bekommen Sie in etwa folgende Bildschirmanzeige:

```

H:\WINDOWS\System32\cmd.exe
VirScan Plus 12.942 ■ (c) 20.10.1990-2003 by ROSE SWE, Ralph Roth
VirScan Plus - Virensuchprogramm gegen bekannte & unbekannte Computerviren
Tip: Die Datei VIRUSDEF.DOC enthält eine Beschreibung über Virenarten
Seriennummer: USP-#55.491 ■ Okt. 2003 ■ [Einzelplatzlizenz]

--=[ Statistik ]--
■ Dateien untersucht ..... 37
■ Viren gefunden ..... 0 <0.0%>
■ Viren gereinigt ..... 0 <0.0%>
■ Benötigte Zeit ..... 00:07.85 <Min:Sek.Hund.>
■ Anzahl untersuchter Bytes ..... 825.449 <105.018 Bytes/Sek>

--=[ Ende der Statistik ]--

Dies ist eine Lizenzversion von VirScan Plus! Weitergabe untersagt!
E:\LAUFWE~1\rose_swe.dir\USP-Full>

```

(Abbildung: VirScan Plus nach dem Suchlauf)

### 3.1 Während des Suchlaufes

Während des Suchlaufes können Sie mit folgenden Tasten VirScan beeinflussen:

- <**Escape**> Bricht die Programmausführung ab. Die gerade untersuchte Datei wird jedoch noch zu Ende untersucht.
- <**Leertaste**> Hält die Programmausführung solange an, bis Sie eine andere Taste drücken. Dies ist besonders dann sinnvoll, wenn Ihr System weitgehendst verseucht ist und Sie sich die einzelnen Dateien genauer anschauen wollen.

## 3.2 Nach dem Suchlauf

Wenn VirScan alles untersucht hat, und einen Virus gefunden hat, müssen Sie anschließend noch die <**Enter**> Taste drücken.

Anschließend gibt VirScan aus, wie viele Programme untersucht worden sind, wie viele Viren gefunden und wie viele Viren entfernt wurden und wie lange VirScan hierzu gebraucht hat. Ferner errechnet VirScan die durchschnittliche Suchgeschwindigkeit, die für jeden Computer etwas anders ausfällt. Auf verschiedenen Testanlagen (Pentium + CACHE) wurden jedoch Suchgeschwindigkeiten von über 5 MB pro Sekunde erzielt!

Wenn VirScan anzeigt: "**420 MB Programmcode untersucht**", Sie jedoch eine 1.0 GB Festplatte besitzen, ist dies nicht ein Programmfehler, sondern die Summe aller AUSFÜHRBAREN Programme auf Ihrer Festplatte (bestimmte Texte oder Datendateien nach Viren abzusuchen ist sinnlos, **hier nimmt VirScan eine Optimierung vor!**).

## 4 Unterstützte Parameter

Wird VirScan ohne zusätzliche Parameter gestartet, so wird nach den einzelnen Optionen gefragt, z. B. welches Laufwerk untersucht werden soll. Es können jedoch zusätzliche Parameter beim Start übergeben werden.

### 4.1 Parametersyntax

**VirScan**      [LW:] [/ALL] [/ANALYSE] [/AUTO] [/BOOT] [/CDROM]  
 [/CONT] [(/F)xxxx.yyy] [(/D)xxxx] [/HILFE] [/MEHR]  
 [/LAPTOP] [/LOG[=xxx]] [/PRT] [/REG] [/VL]  
 [/TURBOAUS] [/DEL] [/MEM] [/MEMHI] [/NOMEM]  
 [/NOPART] [/NOSCRIPT] [/NOTROJ] [/KILL] [/JN]  
 [/LESEN] [/REP] [/SHOWLOG[=xxx]] [/SHOWKEY]  
 [/SICHER] [/SPEICHER] [/Q] [/?] [/UNB] [/ULTRA]  
 [/MEMHI] [/MUTANT] [Verzeichnis] [/VTC] [/WIN]  
 [/ZEIT]

Die eckigen Klammern bedeuten, dass die Parameter wahlfrei sind. Sie müssen jedoch mindestens einen Parameter angeben, damit VirScan weiß, was das Programm zu tun hat, andernfalls fragt Sie VirScan nach den einzelnen Parametern.

Anwender, welche die amerikanische Parametereingabe mit dem Minuszeichen gewohnt sind, können statt den Slashzeichen ('/') das Minuszeichen ('-') verwenden.

Beispielsweise ist -? äquivalent mit /?

Die Datei VIRSHELP.TXT (meist im Verzeichnis \DOKU) enthält ebenfalls eine Kurzbeschreibung der einzelnen Parameter.

Hinweis: Zwischen den einzelnen Parametern muss mindestens ein Leerzeichen vorhanden sein!

### 4.2 Die Umgebungsvariable ‚VirScan‘

Statt VirScan immer mit Parametern aufzurufen, kann VirScan mit einer so genannten Environmentvariable (Umgebungsvariable) gesteuert werden.

Geben Sie beispielsweise am DOS Prompt folgendes ein:

```
SET VIRSCAN=C: D: /UNB /MEMHI
```

Wenn Sie nun VirScan OHNE Parameter starten, ließt VirScan aus der Variable alle benötigten Parameter aus und untersucht in diesem Fall Laufwerk C: und D: mit den Optionen:

```
n /UNB - unbekannte Viren suchen  
n /MEMHI - Speicher bis 1 MB untersuchen
```

## 4.2.1 Zurücksetzen von voreingestellten Werten

Manchmal ist es wünschenswert, schon fest (also per SET VIRSCAN=...) eingestellte Optionen wieder rückgängig zu machen. Dies erfolgt einfach durch Angabe eines Minuszeichens nach der Option. Damit wird die Option ausgeschaltet!

Beispielsweise haben Sie folgendes eingeben:

```
SET VIRSCAN=C: /Q /TURBOAUS /MEM
```

Sie möchten jedoch den Speichertest ausschalten. dann starten Sie VirScan mit folgendem Parameter:

```
VirScan /MEM-
```

## 4.2.2 VirScan per AUTOEXEC.BAT Datei konfigurieren

Wenn Sie wollen können Sie den SET VIRSCAN=... Befehl in Ihre AUTOEXEC.BAT aufnehmen. Beachten Sie, dass Sie genügend Platz für Umgebungsvariablen reserviert haben, ansonsten erhalten Sie beim Booten folgende Meldung o.ä.:

**Umgebungsbereich erschöpft**

Lesen Sie in diesem Fall in Ihrem DOS-Handbuch, wie man mit dem /P Schalter von COMMAND.COM den Umgebungsbereich vergrößert!

## 4.2.3 Beispiele für das Setzen der Umgebungsvariable

Maximale Sicherheit

```
SET VirScan=/AUTO /MEMHI /UNB /LOG /IVT /MUTANT
```

oder

```
SET VirScan=/AUTO /MEMHI /UNB /LOG /IVT /TURBOAUS
```

Normale Bedingungen

```
SET VIRSCAN=/AUTO
```

### 4.3 Bsp.: Tägliche kurze Prüfung per AUTO-EXEC.BAT Datei

Fügen Sie beispielsweise folgende Zeilen in Ihre AUTO-EXEC.BAT Datei:

```
PATH=%path%;c:\VIRSCAN  
VIRSCAN C:\DOS /UNB /MEMHI C:\*.EXE C:\*.COM /IVT  
SET VIRSCAN=/AUTO /MEMHI
```

Es wird dann bei jedem Hochfahren des Systems Ihre Systemdateien auf Viren untersucht.

## 5 Die einzelnen Parameter

### 5.1 /? oder -? (Hilfestellung)

Gibt eine kurze Hilfestellung zu den einzelnen Parametern aus.

### 5.2 /ALL (Alle Dateien überprüfen)

Überprüft ALLE Dateien statt nur ausführbaren Programmen. Diese Option ist mit Vorsicht anzuwenden, weil sie Fehlalarme verursachen kann.

### 5.3 /ANALYSE

Wurde ein Virus gefunden, liefert diese Option noch genauere Angaben zum Virus.

### 5.4 /AUTO (Autopilot aktivieren)

Diese Option ist wohl die stärkste und komfortabelste Funktion am ganzen Programm! Sie ist besonders für Anwender gedacht, die sich nicht näher mit der Funktionsweise des Programms beschäftigen wollen.

Wenn Sie den Autopilot aktivieren, werden zunächst folgende Parameter gesetzt:

- Arbeitsspeicher bis 640 KB untersuchen.
- Ton ausschalten.
- Suchen im Turbo-Modus
- CD-ROM Laufwerke nicht untersuchen

Zusätzlich ermittelt der Autopilot welche Laufwerke am Computer/Netzwerk angeschlossen sind. Anschließend werden alle Laufwerke, die von DOS erreicht werden können untersucht. Es ist dabei egal, ob es sich um Festplatten, RAM Drives, Netzwerkplatten oder 'geSUBSTete' Laufwerke handelt. Die Diskettenlaufwerke A: und B: werden standardmäßig nicht untersucht und müssen bei Bedarf zusätzlich angegeben werden. Ab Version 9.41 wird standardmäßig das CD-ROM Laufwerk nicht mehr auf Viren untersucht, weil es meines Erachtens keinen Sinn macht, sich durch 600-700 MB Daten durch zu suchen, die eine Zugriffszeitverhalten wie

eine Diskette besitzen. Falls Sie ein CD-ROM Laufwerk explizit untersuchen lassen wollen, müssen Sie zusätzlich die Option /CDROM verwenden!

Sie haben die Möglichkeit weitere Optionen zum Autopilot hinzufügen bzw. zu deaktivieren! Falls Sie schon ein Laufwerk oder einen Pfad eingegeben haben, erkennt dies der Autopilot und ignoriert das entsprechende Laufwerk. Beispielsweise rufen Sie VirScan wie folgt auf:

**VirScan -auto d:\tools**

Der Autopilot untersucht nun ALLE Laufwerke, mit Ausnahme des Laufwerkes D:, dort wird nur das Verzeichnis D:\TOOLS untersucht!

## 5.4.1 Beispiele für den weiteren Einsatz des Autopiloten

Nachfolgend die Einstellungen für Parameterübergabe mittels

- 1.) der Kommandozeile
- 2.) der Umgebungsvariable *VIRSCAN*, unter der Voraussetzung, dass `SET VIRSCAN=/AUTO` schon gesetzt wurde.

### 5.4.1.1 Zusätzliches Untersuchen des Laufwerks A:

- 3.) `VirScan -auto a:`
- 4.) `VirScan a:`

### 5.4.1.2 Ton einschalten

- 5.) `VirScan /q- /Auto`
- 6.) `VirScan -q-`

### 5.4.1.3 Den hohen Arbeitsspeicher untersuchen

- 7.) `VirScan /memhi /Auto`
- 8.) `VirScan /memhi`

### 5.4.1.4 Nach neue unbekanntem Viren suchen

- 9.) `VirScan /unb /Auto /mutant`
- 10.) `VirScan /unb /mutant`

### 5.4.1.5 Ergebnis ausdrucken

- 11.) `VirScan /Auto -print`

12.) VirScan /prn

## 5.5 /BATCH (Batchmodus)

Wenn Sie diese Option angeben, müssen Sie, falls ein Virus gefunden wurde, nicht mehr mit einem Tastendruck VirScan verlassen, sondern VirScan kehrt automatisch zu DOS zurück. Sinnvoll, um VirScan aus Batchfiles heraus oder permanent im Hintergrund laufen zu lassen. VirScan gibt folgenden Exitcode an DOS zurück:

```
0      Kein Virus wurde gefunden
1      Viren wurden gefunden
>1    interner Fehler
```

## 5.6 /BOOT (Bootviren suchen)

Mit diesem Parameter werden Programme zusätzlich nach Bootviren (sog. Droppern) abgesucht (was aber i. a. unnötig ist, weil Bootviren sich nicht in Programmen aufhalten). Die Suchgeschwindigkeit wird durch diese Option verschlechtert, ferner besteht die Gefahr von Fehlalarmen. Normalerweise benötigen Sie diese Option nicht, außer Sie wollen zusätzliche Sicherheit z. B. bei der Option /MUTANT oder Sie haben eine größere Virenkollektion! Im normalen Modus werden Dateien nur nach Programmviren durchsucht (Erklärungen zu den einzelnen Virenarten siehe auch unten), wenn Sie also nach allen Viren suchen lassen wollen, schalten Sie die /BOOT Funktion ein.

## 5.7 /CDROM (CD-ROM scannen)

Standardmäßig wird ein CD-ROM Laufwerk **\*NICHT\*** von VirScan untersucht! Eine CD enthält normalerweise keine Viren und die Untersuchung eines CD-Laufwerkes benötigt oft mehrere Stunden. Falls Sie dennoch mal eine CD durchsuchen wollen so müssen Sie zusätzlich den Parameter /CDROM angeben.

Beispiele:

- Mit Autopilot: `VirScan -auto -cdrom`
- Mit Laufwerksangabe: `VirScan l: -cdrom`

## 5.8 /CONT (Fortlaufendes Scannen)

Mit dieser Option kann fortlaufend ein Laufwerk untersucht werden. Programmiert wurde diese Option für den Einsatz in Multitasking Umgebungen wie Windows, OS/2 oder Net-Clients um so im Hintergrund auf Viren scannen zu können. Das Programm läuft bis Sie es per ESC-Taste abbrechen. Aus diesem Grund sollten Sie zusätzlich den Suchlauf protokollieren lassen. Aufrufbeispiel:

```
VirScan c: /cont /log
```

## 5.9 /D (Directory) oder <Verzeichnis>

Hiermit kann ein Verzeichnis und seine Unterverzeichnisse nach ausführbaren Programmen untersucht werden. Der Parameter /D wird nur noch zur Kompatibilität zu früheren Versionen unterstützt. Wenn Sie ein Verzeichnis angeben, muss es sich um den absoluten Pfadnamen handeln, während mit dem Parameter /D 'Abkürzungen' wie... oder **c:** oder \ usw. erlaubt sind.

Beispiele:

```
VIRSCAN /DK:\NET /D..  
VIRSCAN C:\DOS A:\NEU /D.
```

```
SET VIRSCAN=/D\ C:\DOS
```

## 5.10 /DEL (Delete/Löschen von Dateien)

Es werden alle infizierten Dateien gelöscht! Ohne vorherige Abfrage! Zusätzlich wird, falls die Funktion /KILL eingeschaltet ist, zuerst versucht, den Virus zu entfernen. Falls dies technisch nicht möglich ist, wird die Datei physikalisch gelöscht, d. h. die Datei kann selbst mit UNDELETE nicht wiederhergestellt werden! Tipp: Zusätzliche Ausgabe auf den Drucker oder in eine Datei (/LOG bzw. /PRT)!

## 5.11 /EXTR (Signatur extrahieren)

Mit dieser Option können Sie geeignete Signaturen für VirScan 'extrahieren'. Diese Option ist dann sinnvoll, wenn ein brandneuer Virus zugeschlagen hat und Sie nicht genug Programmierkenntnisse besitzen eine eigene Signatur

zu definieren (Suchstring), die in VIRSCAN.EXT aufgenommen werden kann.

### **Einschränkungen:**

- Diese Option funktioniert nur unter Verwendung des Debuggers.
- Diese Option ist nur in der registrierten Vollversion vorhanden.  
Hintergrund: Es soll Hackern, Virenprogrammieren und sonstigen Freaks nicht ein Werkzeug in die Hand gegeben werden, um ihre Viren noch zu verbessern, bzw. die Funktion von VirScan zu analysieren.
- VirScan kann u. U. bei polymorphen Viren keinen eindeutigen Suchstring erzeugen (Beschreibung polymorphe Viren s. u.). Hierzu kann jedoch die undokumentierte Funktion /HEUR (Vollversion) verwendet werden.
- VirScan kann bei nicht infizierten Dateien oft keinen Einsprungspunkt finden (Meldung: Einsprungspunkt nicht vorhanden). In diesem Fall wird eine Generierung des Suchstrings aus Sicherheitsgründen (Fehlalarme) unterlassen!

Tipp: VirScan zusätzlich mit der Option /LOG oder /PRT laufen lassen, um anschließend die Suchstrings vergleichen zu können.

## **5.12 /FSuchMaske oder Suchmaske (einzelne Dateien untersuchen)**

Hiermit können einzelne Dateien und Dateigruppen untersucht werden. Laufwerk, Pfad und Wildcards werden unterstützt! Die Option /F wird aus Kompatibilitätsgründen weiterhin unterstützt! Bitte beachten: Es wird nicht rekursiv gesucht!

Beispiel:

```
VirScan /FG:\TOOLS\NEU\VI*.EX?
```

```
VirScan *.*
```

## **5.13 /H (/HILFE oder /HELP)**

Zeigt die Datei VIRSHELP.TXT an, die eine kurze Hilfestellung zum Programm enthält.

## 5.14 /IVT (Interrupt Virentest)

Mit dem Parameter /IVT kann der Arbeitsspeicher nach ca. 250 der bekanntesten Viren untersucht werden. Dies erfolgt mit so genannten "Am I there" Aufrufen, die in Sekundenbruchteilen durchgeführt sind (im Vergleich zum langsamen Untersuchen des Arbeitsspeichers). Der Arbeitsspeicher wird hierbei unter anderem auf folgende Viren untersucht:

- Jerusalem und verwandte Viren
- Frere Jaque
- Fu Manchu
- Tequila (Tarnkappen/Stealth-Virus, 14 Varianten)
- Yankee Doodle/Vacsina (45 Varianten)
- Cascade und Yap (14 Varianten)
- Flip/Omicrone (6 Varianten/Substealth-Virus)
- Parity Check (4 Varianten, Bootvirus)
- dBase
- Plastique (AntiCad, Invader, Tobacco, 4.21, 5.21 und Cobol)
- Tremor (Tarnkappenvirus)

[Dies ist nur ein Auszug der bekanntesten Viren]

Bei Erkennung des Virus wird der Benutzer darüber informiert.

Sie sollten diese Option nicht verwenden, wenn Sie Novell Netware installiert haben, weil es zu Überschneidungen der Interruptaufrufe kommt. Diese Funktion wurde ursprünglich automatisch durchgeführt, es hat sich jedoch herausgestellt, dass die so genannten "Am I there" Aufrufe nicht 100% kompatibel mit verschiedenen Betriebssystemen und Konfigurationen sind. Falls es also zu ungewöhnlichen Seiteneffekten kommt, so könnte es an dieser Option liegen.

Diese Option untersucht -falls vorhanden- auch den hohen Arbeitsspeicher (HMA) auf Viren.

## 5.15 /JN (Vor dem Löschen abfragen)

Wenn Ihr System/Disketten von Viren befallen ist, können Sie mit den Optionen /KILL und /DEL den Virus entfernen. Dies geschieht weitgehendst automatisch. Wenn Sie jedoch den Parameter /JN setzen, werden Sie vor dem Löschen ei-

ner befallenen Datei gefragt, ob diese Datei gelöscht werden soll oder nicht.

## 5.16 /KILL (Virenkiller aktivieren)



Aktivieren des Virenkillers. VirScan kann zurzeit die meisten in Deutschland auftretenden Viren (ca. 450 Viren) vernichten und die ursprüngliche Datei/Bootsektor wieder herstellen (soweit technisch möglich). Die Datei VIRSCAN.TXT enthält eine Liste der entfernbarer Viren, sowie eine Liste von weiteren speziellen Virenkillern, die Sie bei ROSE Softwareentwicklung erhalten können.



**ACHTUNG:** Die Anwendung des Virenkiller erfolgt auf eigenes Risiko, sie ist nur gedacht, Viren zu entfernen, falls keine Originalprogramme mehr vorhanden sind.

Viren werden laufend von Hackern verändert, mit dem Ergebnis, dass so genannte Familiensucherkennungen verwendet werden müssen, eine genaue Diagnose ist in diesem Fall nicht mehr möglich. Eine Entfernung könnte in diesem Fall zu einem unkorrekten Programm führen.



**ACHTUNG:** Die Entfernung eines Partitionsvirus kann bei einer Fehldiagnose u. U. zu einer nicht mehr ansprechbaren Festplatte führen. Fertigen Sie deshalb zuerst einen Backup an. Bei Unsicherheit analysieren wir den Virus gerne kostenlos.

### 5.16.1 Allgemeine Hinweise zum Virenkiller

**Hinweis:** Damit nicht nach dem Entfernen der Viren die Dateien re-infiziert werden, muss vor dem Entfernen, von einer garantiert virenfreien Diskette gebootet werden (Kaltstart). Anschließend gleich den Virenkiller starten!



Wird nicht von einer virenfreien Diskette ein Kaltstart durchgeführt, kann unter Umständen die Entfernung zu katastrophalen Fehlern führen!



**Achtung Speicherplatz:** Für das Entfernen werden zusätzliche 5 KB freier Arbeitsspeicher benötigt. Deshalb benötigt VirScan mindestens 520 KB freien Arbeitsspeicher!

## 5.16.2 Entfernen von Boot- und Partitionsviren

VirScan kann ca. 99.8 Prozent aller Bootviren von Disketten entfernen. Diese Funktion ist i. a. nicht kritisch.



Probleme kann es bei der Entfernung von Partitionsviren geben: VirScan kann immerhin ca. 95 Prozent aller Partitionsviren von der Festplatte entfernen, denken Sie jedoch daran, dass bei einer Fehldiagnose zu einer nicht mehr ansprechbaren Festplatte (falsche Partition) führen kann. In diesem Fall muss mit einem Programm wie dem **'Norton Disk Doktor'** die Festplatte repariert werden!

## 5.16.3 Hinweise bei Mehrfachinfektionen



Dateien können von mehreren verschiedenen Viren befallen werden. Hier muss VirScan u. U. seine Waffen strecken. Bsp: Eine Datei ist vom 1704/Cascade und anschließend vom Jerusalem Virus infiziert worden. VirScan entfernt jetzt den 1704 Virus, wobei VirScan jedoch Code vom Jerusalem Virus entfernt, weil sich dieser NACH dem 1704 befindet. Das Ergebnis ist eine zerstörte Datei! Tipp: Bei Mehrfachinfektionen verschiedener entfernbarer Viren, die Dateien löschen lassen (/DEL).

## 5.16.4 Virus kann nicht entfernt werden?



Versuchen Sie bei Dateiviren mit dem Programm RVK (ROSE SWE Viren Killer) oder bei Bootviren mit dem Programm MBR-Kill den Virus zu entfernen. Sollte dies nicht klappen, so senden Sie uns bitte eine Diskette mit möglichst vielen befallenen Dateien zu. Wir werden umgehend einen Virenkiller entwickeln!

## 5.17 /LAPTOP (Unterstützung für Laptops)

Mit dieser Option kann VirScan an Monochrom-, LCD- und Laptop-Bildschirme angepasst werden (andere Farbauswahl).

## 5.18 /LESEN (Anleitung lesen)

Lesen dieses Handbuches mittels eingebauten Listprogramms. Blättern mit den Pfeiltasten, Verlassen mit ESC.

## 5.19 /LOG und /LOG= (Reportdatei anlegen)

Es wird eine Reportdatei namens VIRSCAN.LOG im aktuellen Verzeichnis angelegt. In diese Datei werden alle Dateien eingetragen, die von Viren befallen sind. Weiterhin werden alle Informationen über das zu untersuchende Laufwerk mit eingetragen. Bei Disketten mit Schreibschutz muss natürlich der Schreibschutz entfernt werden, sonst kann keine Log-Datei erzeugt werden (typischer Anwenderfehler)!

Alternativ können Sie auch einen anderen Dateinamen bestimmen. Verwenden Sie hierzu den Parameter /LOG=Dateiname (oder /LOG:Datei), also z.B.: /LOG=C:\TMP\TÄGLICH.LOG.



**HINWEIS:** Eine ältere gleich lautende Datei (z. B. VIRSCAN.LOG) wird überschrieben!

## 5.20 /MEHR (Mehrere Disketten nacheinander untersuchen)

Wenn Sie nicht jedes Mal VirScan für jede Diskette neu starten wollen, so geben Sie die Option /MEHR mit an.

Sie werden dann gefragt:

**"Bitte Diskette entnehmen und eine neue Diskette einlegen.  
Disk bereit? [J/N]"**

Legen Sie eine neue Diskette ein und geben Sie danach "J" ein. Die Leertaste und Enter sind äquivalent zu "J", während die ESC für "N" verwendet werden kann! Diese Option funktioniert nur in Verwendung mit der Option [LW:]! Wenn Sie /MEHR bei Festplatten angeben, wird dieser Parameter für Festplattenlaufwerke ignoriert.

Beispiele:

```
VIRSCAN A: C: /MEHR  
VIRSCAN B: -mehr
```

```
SET VIRSCAN=-mehr
```



**Achtung:** VirScan verwendet ab Version 11.00 Overlaydateien, weshalb die Overlaydatei VIRSCAN.OVR sich nicht auf der zu Untersuchenden Diskette befinden darf!

## 5.21 /MEM (Memory)

Ihr System-Speicher wird auf alle konstanten Viren untersucht. Mit einer Anzeige, welches Segment gerade untersucht wird. Diese Funktion kann bei nicht 100%-tig kompatiblen IBM-Rechnern zu Schwierigkeiten führen!



Befindet sich ein Virus im Arbeitsspeicher, so muss dieser zuerst durch einen Kaltstart von einer sauberen Systemdiskette entfernt werden!

## 5.22 /MEMHI (Hoher Arbeitsspeicher)

Wie die Option /MEM, es wird jedoch auch der Arbeitsspeicher bis 1 MB auf Viren untersucht. Diese Funktion ist nur für PC-Rechner sinnvoll, die einen Treiber verwenden, der DOS in den hohen Arbeitsspeicher verschiebt (HMA). Bei PC-Rechnern, welche die so genannte A20 Leitung benutzen, wird dieser Speicherbereich ebenfalls untersucht (also bis 1088 KB Arbeitsspeicher).

Das Programm muss das ganze BIOS nach verdächtigen Sequenzen absuchen, weshalb VirScan bei langsameren Rechnern teilweise mehr als eine Minute benötigt!

## 5.23 /MUTANT (nach mutierten Viren suchen)



Mit dieser Option können Sie zusätzlich nach mutierten (also veränderten) Viren suchen, die sonst nicht erkannt werden. Dies wird dadurch erreicht, dass eine Erkennung nicht mehr zu 100 Prozent übereinstimmen muss, sondern bis zu sechs Stellen sich vom Suchstring unterscheiden dürfen. Im Gegensatz zur Option /UNB wird also mit einer bestehenden Signatur gesucht, wobei Treffer jedoch nicht mehr zu 100 Prozent übereinstimmen müssen!

Diese Option ist gedacht, um bei einem System das sich abnormal verhält, eventuelle "Virentreffer" zu landen. Mit verschiedenen mutierten Testviren wurde eine Treffer-rate von 100 Prozent erzielt! Einen "Treffer" meldet VirScan ungefähr so:

**Warnung: C:\COMMAND.COM evtl. mit xy-Virus infiziert!**

Weil diese Option mit Sicherheit Fehllalarme verursacht (z. B. wird ein Veronezh Virus im Programm VIRSTOP.EXE

gefunden) werden standardmäßig folgende Optionen zusätzlich eingeschaltet:

- Turbomodus EIN
- Ton aus
- Virenkiller aus

Die Option /MUTANT ist ebenfalls wie die Option /UNB nicht für den unerfahrenen Anwender gedacht. Ein kleiner Tipp hierzu: Ein Dateivirus macht sich immer dadurch bemerkbar, dass er versucht so viele Programme wie nur möglich zu infizieren. Deshalb sind drei oder vier "infizierte" Dateien (bei der Option /MUTANT und/oder /UNB) auf der Festplatte noch lange kein Indiz dafür, dass ein Virus zugeschlagen hat!



Bei Verdacht können Sie uns unverbindlich eine ver-seuchte Diskette zusenden!

Ab Version 9.22 wird bei der Option /MUTANT zusätzlich der Boot-/Partitionsssektor nach mutierten Viren abge-sucht!

## 5.24 /NOMEM (Arbeitsspeicher nicht untersuchen)

Mit dieser Option können Sie die Schnellüberprüfung des Arbeitsspeichers auf bekannte und unbekannte Viren un-terbinden. Diese Optionen sollten Sie nur bei langsamen Rechnern verwenden! Diese Funktion ist komplett in As-sembler entwickelt und deshalb extrem schnell!

## 5.25 /NOPART (Partitionstabelle nicht scannen)

Mit dieser Option können Sie das Überprüfen der Partiti-onstabellen und des Bootsektors auf Festplatten un-terbinden. Bei Disketten wird der Bootsektor jedoch \*IMMER\* untersucht! Vorteil: Schneller Suchvorgang.

## 5.26 /NOSCRIP (Nicht nach Scriptviren suchen)

Es wird nicht nach VBS, HTML, Corelscript, Java usw. so-wie nach IRC Würmer gesucht.

## 5.27 /NOTROJ (nicht nach Trojanischen Pferden suchen)

Mit dieser Option können Sie das Überprüfen nach trojanischen Pferden unterbinden.

## 5.28 /OFFSET (Offset anzeigen)

Diese Option gibt -falls ein Virus gefunden wurde- die Position des Virencodes bezüglich des Dateianfanges an. Ebenfalls wird, bei einer beschädigten Datei, angezeigt, wohin der Einsprungspunkt hinzeigt. Diese Option dürfte für Sie relativ uninteressant sein, weshalb sie standardmäßig auf AUS geschaltet ist. Diese Option ist voll kompatibel zu den Optionen /LOG, /PRN und /REP.

## 5.29 /PROZ - Informationen zum Prozessor

Diese Option zeigt Informationen (Prozessortyp, Coprozessortyp, Taktgeschwindigkeit, Revision etc.) über den eingesetzten CPU Prozessor an.

## 5.30 /PRT oder /PRN oder /PRINTER

Analog zu /LOG, der Bericht wird jedoch auf dem Drucker ausgegeben. Schalten Sie den Drucker ein, sonst wartet VirScan so lange, bis der Drucker "Online" ist. Anzeige über Fehlerfenster! Diese Option ist mischbar mit der Option /LOG!

## 5.31 /Q (Quiet)

Wenn VirScan einen Virus findet, wird dies mit einem Piepsen angezeigt. Wenn Sie Ihre Arbeitskollegen nicht stören wollen, so können Sie VirScan mit dieser Option stumm schalten!

## 5.32 /REG (Registration)

Wenn VirScan in der Sharewareversion mit der Option /REG gestartet wird, dann versucht VirScan die Datei REGISTER.COM auszuführen und einen Bestellschein zu drucken.

## 5.33 /REP (Report)

Falls Sie nicht schon die Option /LOG eingeschaltet haben, wird diese Option zusätzlich eingeschaltet. Beim anschließenden Suchlauf wird jede untersuchte Datei in die Datei VIRSCAN.LOG eingetragen (mit protokolliert), ob sie infiziert ist oder nicht.

Diese Option ist besonders dann sinnvoll, wenn Netzwerke untersucht werden sollen, oder Sie sich sicher sein müssen, dass die Datei untersucht wurde oder nicht!

Um den Namen für die Reportdatei abzuändern, benützen Sie bitte die Option /LOG=

## 5.34 /SHOWLOG= (Reportdatei betrachten)

Manchmal ist es wünschenswert die Datei VIRSCAN.LOG in einem Textbetrachter anschauen zu können, besonders dann, wenn Sie zum Beispiel von einer Bootdiskette gebootet haben und keinen Zugriff auf den Editor EDIT haben.

Verwenden Sie nur die Option /SHOWLOG, wird die Datei VIRSCAN.LOG angezeigt. Verwenden Sie die Option /SHOWLOG=Dateiname, wird die Datei "Dateiname" angezeigt. Somit steht Ihnen also ein kleines Listerprogramm zur Verfügung, mit dem Sie beliebige Textdateien lesen können, die maximale Größe der Textdatei beträgt 4 MB!

## 5.35 /SICHER (Sicherheitsmodus)

Diese Option ist das Gegenstück zur Option /ULTRA. Wenn Sie diese Option abgeben wird ein aufwendiges Suchverfahren verwendet; die Gefahr für Fehlalarme wird jedoch ebenfalls erhöht. Die Suchgeschwindigkeit wird hierdurch ebenfalls merklich herabgesetzt. Im Gegensatz zur Option /TURBOAUS sind der Debugger, Codeanalyser und die AVR-Module aktiv und können somit auch polymorphe Viren erkennen!

## 5.36 /SPEICHER (Speicherbelegung)

Zeigt den internen freien Speicher von VirScan an. Ist z. B. dann sinnvoll, wenn Sie Speicherplatzprobleme (-> Netzwerk) haben.

## 5.37 /TURBOAUS (nicht im Turbo-Modus suchen)

Turbo-Modus ausschalten. Um bei der Suche nach allen Viren die Ausführungsgeschwindigkeit noch zu beschleunigen, ist in VirScan einen "intelligenten" Debugger integriert. Dieses Programm ermittelt erst einmal, wo der Virus sitzen könnte und untersucht anschließend die Datei. Ein Virus "hängt" sich nämlich normalerweise an den Anfang oder das Ende eines Programms an. Standardmäßig ist der Turbo-Modus eingeschaltet.

Falls Sie die gesamte Datei untersuchen lassen wollen, starten Sie VirScan mit der Option /TURBOAUS!

### 5.37.1 WARNUNG



Es ist nicht sinnvoll VirScan immer mit ausgeschaltetem Turbo-Modus suchen zu lassen. Gründe:

- VirScan ist im Turbo-Modus bis zu 25x schneller!
- Die rechnerische Wahrscheinlichkeit ist sehr hoch, dass VirScan mit ausgeschaltetem Turbo-Modus einen FEHLALARM erzeugt.
- Der Debugger arbeitet nicht im ausgeschalteten Turbo-Modus und kann somit keine -oft- **wertvolle "Hinweise"** liefern!
- VirScan benötigen um polymorphe Viren und die so genannten AVR-Module zu erkennen den Debugger (somit auch den schnelleren Turbomodus)!

## 5.38 /ULTRA (Schnelleres Suchverfahren)

Das Gegenstück zur Option /TURBOAUS. Mit diesem Parameter verwendet VirScan einen anderen Suchalgorithmus, der ungefähr 20 - 30% schneller ist, als der normale Suchvorgang. Bedenken Sie, das VirScan EXE Dateien nicht so 'genau' untersucht (COM, SYS und andere Dateien wie gehabt), weshalb einige wenige Viren nicht mehr in EXE Dateien gefunden werden. Dieser Parameter ist ideal für die tägliche Festplattenprüfung.

## 5.39 /UNB (Unbekannte Viren suchen)



Ja, Sie lesen richtig! VirScan ist in der Lage, neue unbekannt Viren zu erkennen! VirScan sucht, wenn Sie den Parameter /UNB setzen nach typischen Befehlen, die ei-

gentlich nur Viren und ähnliche Programme verwenden. VirScan zeigt unbekannte Viren mit einer der folgenden Meldungen an:

Dateiviren:

- Unbekanntes (Relokator/VSS) Virus gefunden.
- Unbekanntes (Relokator) Virus gefunden.
- Unbekanntes (POP BX) Virus gefunden.
- Unbekanntes (POP BP) Virus gefunden.
- Unbekanntes (Trap) Virus gefunden.
- Unbekanntes (Dropper) Virus gefunden.
- Unbekanntes (Vienna) Virus gefunden.
- Unbekanntes (Cascade) Virus gefunden.
- Unbekanntes (Memory) Virus gefunden.
- Unbekanntes (POP SI) Virus gefunden.
- Unbekanntes (POP DI) Virus gefunden.
- Unbekanntes (FileOpen) Virus gefunden.
- Unbekanntes (EXE Locater) Virus gefunden.
- Unbekanntes (Boot-Dropper) Virus gefunden.
- Unbekanntes (Decoder) Virus gefunden.

Dass hier natürlich Fehllalarme verursacht werden können dürfte selbsterklärend sein!

VirScan überprüft ab Version 9.5 immer, ob sich ein unbekannter Bootvirus im Bootsektor bzw. in der Partitionstabelle befindet. Falls ein (neuer) unbekannter Bootvirus gefunden wird, meldet dies VirScan wie folgt:

Bootviren:

- Bootsektor C: Unbekanntes Boot-Virus gefunden.

Mit Verwendung des Parameters /UNB wird die Empfindlichkeit für dieses Verfahren erhöht, was natürlich auf die Möglichkeit der Fehllalarme erhöht. VirScan verwendet das gleiche Verfahren wie ChkPC, welches über zwei Jahre getestet wurde, bevor die Routinen in VirScan übernommen wurden!

## 5.40 /VL (Viren-Liste)

Es werden alle Viren, die VirScan erkennen kann ausgegeben. Die Ausgabe auf einen Drucker oder in eine Datei umzuleiten ist möglich! Programm kehrt anschließend zu DOS zurück. Um z. B. die Virenliste auszudrucken geben Sie folgendes ein:

(c) by ROSE SWE

[http://come.to/rose\\_swe](http://come.to/rose_swe)

**VirScan /vl /unb /prn**

## 5.41 /VTC

Setzt bestimmte Optionen, wie sie im VTC Virus Test benötigt werden. Gesetzt werden:

`/BATCH /BOOT /ALL /Q /ZEIT /MUTANT /NOMEM`

## 5.42 /WIN (Kompatibilität zu Windows)

VirScan erkennt selbst, ob das Programm unter Windows (3.1/95/98/ME/NT/2000) gestartet wurde und setzt dann diesen Parameter automatisch. Zur weiteren Unterstützung von Windows sind ein Icon und eine PIF-Datei beigefügt. Wenn Sie VirScan unter Windows im erweiterten Modus nutzen wollen, so verwenden Sie hierzu bitte die Datei VIRSCAN.PIF (VirScan sucht dann im Hintergrund nach Viren!).

## 5.43 /ZEIT (Nicht auf unübliche Zeit überprüfen)

Mit dieser Option kann die Überprüfung auf eine unübliche Zeit abgeschaltet werden. Normalerweise wird jede Datei gemeldet, die ein unübliches Datum besitzt (62 Sekunden, 63 Minuten oder Jahr>2080). Siehe auch '62 Seconds Virus'.

## 5.44 LW: (Laufwerke)

LW ist ein existierendes Laufwerk das mit den Buchstaben "A" bis "Z" angesprochen werden kann. Existiert das Laufwerk nicht, so wird dies mit folgender Fehlermeldung gemeldet:

**Kann Laufwerk X: nicht ansprechen (Netzwerk?)**

Der Partitionssektor bzw. Bootsektor wird immer mit untersucht! Sie können mehrere Laufwerke angeben.

Aufruf: `VIRSCAN C: F:`  
(Festplatten C und F werden untersucht)

Falls es sich um ein CD-ROM Laufwerk handelt, müssen Sie zusätzlich den Parameter /CDROM angeben, ansonsten wird das Laufwerk nicht untersucht und Sie erhalten dann folgende Meldung (siehe auch Parameter /CDROM):

CD-ROM Laufwerk X: wird nicht untersucht!

## 5.45 Beispiele für Aufrufe

Möglich wären auch folgende Aufrufe:

```
VirScan -? /lesen
```

```
VIRSCAN c: d: /MEM /q
```

```
VirScan a: /mehr /kill /PRN -TURBOAUS
```

Alte Parametersyntax:

```
VirScan a: b: /De:\dos /fg:\my\F*.OVL /F*.exe /mehr
```

Neue Parametersyntax:

```
VirScan a: b: e:\dos g:\my\F*.OVL *.EXE /mehr
```

```
VIRSCAN S: T: R: /MEM /DEL /TURBOAUS /REP
```

```
VirScan c: d: /mem /unb /q /Printer
```

```
VirScan -auto -memhi -prn
```

## 6 Sonstige Funktionen

### 6.1 VirScan unter Windows

Sie können VirScan ohne weiteres unter Windows verwenden; Im 386'er Modus von Windows 3.x/9x/ME/2000/NT kann VirScan sogar noch besser 'arbeiten', weil VirScan dann Windowsressourcen ausnützen kann! Speziell hierfür wurde ein Icon (VIRSCAN.ICO) und eine PIF-Datei (VIRSCAN.PIF) kreiert. Im Programm Manager wählen Sie Datei - Neu und geben unter 'Befehlszeile'

VIRSCAN.PIF

ein. Anschließend wählen Sie Datei - Eigenschaften und wählen 'Anderes Symbol'. Geben Sie hier

VIRSCAN.ICO

ein. Wenn Sie nun das VirScan Symbol anklicken wird das Programm gestartet. Falls Sie andere Parameter übergeben wollen, müssen Sie mit dem Windows PIF-Editor die Datei VIRSCAN.PIF verändern.

Analog gibt es weitere PIF-Dateien für VirScan:

VSP\_W310.PIF, VSP\_W311.PIF, VSP\_W95.PIF und VSP\_NT40.PIF

Diese Datei kann analog unter Windows eingebunden werden. Diese PIF-Datei fragt Sie vor dem Start nach den gewünschten Parametern, falls nicht mit SET VIRSCAN=... Parameter vordefiniert wurden.

### 6.2 VirScan unter Windows 9x und Windows NT/2000

VirScan wurde sorgfältig unter den Betriebssystem Windows 95/98 und NT/2000 getestet. VirScan kann unter Windows in der DOS-Box problemlos gestartet werden, es wurden hierbei keine Inkompatibilitäten festgestellt. Selbst mehrere parallele Aufrufe von VirScan brachten Windows nicht zum Absturz. VirScan enthält etliche Routinen zur Unterstützung von Windows und nutzt dabei Windows Ressourcen zum schnelleren Suchen!

## 6.3 VirScan unter OS/2

VirScan wurde sorgfältig unter den Betriebssystem OS/2 Version 2.00 getestet (DOS-Box und DOS Full Windows) sowie unter OS/2 Warp (3.0 und 4.0). Es wurden keine Inkompatibilitäten festgestellt. Selbst mehrere parallele Aufrufe von VirScan brachten OS/2 nicht zum Absturz. Unter OS/2 darf VirScan jedoch bestimmte Dateien nicht öffnen. Dies ist ganz normal, es handelt sich dabei um Dateien, die OS/2 ständig geöffnet hat (HARDERR.EXE u. a.)!

## 6.4 VirScan unter Netzwerke

VirScan ist Netzwerk fähig und hat spezielle Routinen zur Netzwerkunterstützung integriert! Weil es inzwischen verschiedene Netzwerke auf dem Markt sind, können wir Ihnen keine Garantie geben, dass VirScan Plus auch auf Ihrem Netzwerk läuft. VirScan wurde auf allen handelsüblichen Netzwerken getestet.

VirScan wurde u.a. getestet unter Novell Netware 3.1x bis 4.1x, IBM-Tokenring, Novell Lite (Personal Netware), Lantastic, MS-Lan Manager, Windows NT, Windows for Workgroups sowie NFS PC-Lan.

Sie können mit VirScan Plus jedes Diskettenlaufwerk, jede Festplatte und jedes Netzlaufwerk untersuchen, wenn dieser Datenträger von DOS aus erreichbar ist! Bitte beachten Sie, dass Sie zum Untersuchen aller Laufwerke entsprechende Zugriffsrechte benötigen.

## 6.5 Hinweise für Netzwerkadministratoren



Die Entseuchung eines Netzwerkes ist nicht einfach, dies sollten nur entsprechende Spezialisten durchführen!

Um VirScan effektiv auf einem Netzwerk einzusetzen beachten Sie bitte folgenden Hinweise (gilt auch für normale, nicht vernetzte Computer):

- Alle User müssen sich ausloggen und Ihren Rechner ausschalten.
- Fahren Sie das System auf Einzelusermodus herunter (shutdown 0, reboot o. ä.)
- Booten Sie von einem möglichst virenfreien Rechner, von Diskette!

- Loggen Sie sich als Superuser ein.
- Falls möglich als Superuser, der nur Lese- und Ausführungsrechte besitzt (hierdurch wird eine versehentliche Weiterverbreitung ausgeschlossen).
- Starten Sie VirScan für sämtliche Netzlaufwerke, zusätzlich mit den Optionen /MEM und /REP, eventuell auch mit /UNB, /BOOT oder /MUTANT!
- Werten Sie die Datei VIRSCAN.LOG aus.
  
- Starten Sie VirScan mit den Optionen /DEL und /KILL. Zum Entfernen eventueller Viren benötigen Sie jetzt natürlich Superuser Recht!
- Überprüfen Sie nochmals, wie oben beschrieben das Netzwerk auf Viren.
- Überspielen Sie die Originalsoftware auf das Netz. Anschließend wieder das Netz untersuchen lassen.
  
- Entfernen Sie von sämtlichen Rechnern die Viren, bevor die Rechner wieder ans Netz gehen.
- Wiederholen Sie die oben genannten Schritte bis das Netz und die angeschlossenen Rechner virenfrei sind!

## 6.6 Zusätzliche Fehlermeldungen

Folgende Fehlermeldungen werden zusätzlich ausgegeben:

- **Kann Laufwerk X: nicht ansprechen (Netzwerk?)**

Über DOS kann nicht auf das Laufwerk zugegriffen werden. Eventuell ist auch im Laufwerk keine Diskette eingelegt worden!

- **Kann Verzeichnis "XXX" nicht finden (Netzwerk?)**

Sie haben entweder das Verzeichnis falsch eingegeben (bitte am Schluss ohne Backslash "\"), es existiert nicht oder Sie dürfen nicht darauf zugreifen (in Netzwerken oder bei Verwendung von SHARE.EXE).

- **Aus-/Eingabefehler: XXXX.YYY Fehler: DOS(zzz)/IO(www)**

VirScan kann die Datei "XXXX.YYY" nicht öffnen. Sie haben keinen Zugriff auf diese Datei (Netzwerk oder Diskette ist Schreibgeschützt). Diese Fehlermeldung dürfe normalerweise nicht auftreten!

Sie können, falls Sie entsprechende Fachliteratur besitzen, die Fehlercodes selber auswerten (INT 21h).

Drücken Sie in diesem Fall die <ESCAPE> Taste um VirScan abzuberechnen!

## 6.7 Suchgeschwindigkeit

Wenn Ihnen VirScan etwas langsam vorkommt so ist anzufügen, dass die meisten anderen Viren Scanner nicht einmal mehr als 10000 Viren suchen können. (Sicherheit kostet Zeit!) Bedenken Sie, dass das Programm hoch optimiert ist (Assembler-Code)! VirScan Plus zählt zu den schnellsten Virenschanner der Welt!

## 6.8 Wie werden neue Virenerkennungen in VirScan aufgenommen?

Sie können selbst Virensignaturen in VirScan aufnehmen. Sie müssen jedoch folgende Hinweise beachten:

- Datei VIRSCAN.EXT mit einem ASCII-Texteditor einladen (z. B. EDIT.COM von MS-DOS). Nicht Wordstar oder Word verwenden!
- Jede Zeile, die keine Virenerkennungen besitzt, muss mit einem Semikolon (;) anfangen.
- Virensignatur muss als Hexcode eingegeben werden. Damit VirScan korrekt arbeitet, muss die Erkennung mindestens 16 Zeichen (8 Bytes) maximal 28 Zeichen (14 Bytes) lang sein.
- Schreiben Sie den Namen, Signatur und Bemerkung in die gleichen Spalten, wie in der Datei VIRSCAN.EXT. Bemerkungen, die über 80 Zeichen pro Zeile hinausgehen machen nichts, solange Sie nicht einen Zeilenumbruch durchführen.
- Die Datei darf nicht mehr als 200 Virensignaturen enthalten. Falls sie mehr als 200 Signaturen besitzt, können Sie diese ROSE SWE zusenden und Ihnen wird ein kostenloser Update zugesandt! (Bitte jedoch frankierten und adressierten Rückumschlag + Diskette beifügen!) Sie merken dies, wenn VirScan meldet:

Zu viele Erkennungen in der Datei VIRSCAN.EXT

- Bitte beachten Sie jedoch, dass in die Datei nur konstante Virensignaturen eingefügt werden dürfen (mehr hierzu s. u.)!
- Trojanische Pferde, logische Bomben und Viren in Hochsprache können Sie in die Datei VIRSCAN.TRJ aufnehmen. Verwenden Sie hierzu das Bonusprogramm (falls vorhanden) EXEHEAD.EXE mit der Option /t.

## 6.9 Wie erzeugen Sie eine Erkennung

Es gibt mehrere Möglichkeiten:

- Sie entnehmen die Erkennung aus einer Zeitschrift.
- Sie erhalten die Erkennung von ROSE SWE zugesandt (nach Analyse des Virus).
- Sie analysieren den Virus selbst (setzt sehr gute Assemblerkenntnisse voraus).
- Sie verwenden in der registrierten Vollversion die Option /EXTR, welche geeignete Erkennungen erzeugt.
- Sie haben das Programm EXEHEAD.EXE und wollen keinen Virus erfassen sondern ein Trojanisches Pferd: Dann starten Sie EXEHEAD wie folgt:

```
exehead trojan.exe /t >> virscan.trj
```

Eine Signatur vom Programm "trojan.exe" wird für die Datei VIRSCAN.TRJ erzeugt und an die Datei VIRSCAN.TRJ angehängt!

## 7 Fehllalarm? Ja/Nein?



Die rechnerische Wahrscheinlichkeit, dass VIRSCAN einen Fehllalarm bei einem 50 KB Programm anzeigt, liegt zwischen  $1:9.44 \cdot 10^{14}$  und  $1:1.1 \cdot 10^{29}$ ! Nehmen Sie bitte einen Virenbefall nicht auf die "leichte Schulter"! VirScan ist jedoch ein Virensuchprogramm das mehrere Tausend Viren sucht, dabei handelt es sich oft um hochgradig verschlüsselte Viren, weshalb es -rein technisch gesehen- zu Fehllalarmen führen kann!

### 7.1 Bekannte Fehllalarme (mit der Option /UNB)

Die Programme FileShield von McAfee und Viren Schutz Schild (bis Version 1.05) von ROSE SWE sind entwickelt worden, um Programme gegen Viren zu immunisieren. Bei solchen immunisierten Programmen findet VirScan u. U. einen unbekanntem Virus vom Typ "**Relokator/VSS**"! Alle anderen unbekanntem Viren, besonders die POP-Viren sind ernstzunehmende Hinweise auf eventuelle neue Viren, besonders dann, wenn Ihre Festplatte von einem Typ durchgehend "verseucht" ist!

**Unerfahrene DOS-Anwender sollten  
die Funktion /UNB nicht verwenden!**

#### 7.1.1 Programme die einen Fehllalarm erzeugen

Folgende Programme erzeugen nachweislich einen Fehllalarm, wenn sie mit der Option /UNB oder /MUTANT untersucht werden:

**Zurzeit sind keine Programme bekannt!**

#### 7.1.2 WARNUNG: Option /TURBOAUS UND /UNB

Die Option /UNB kann, insbesondere mit dem Parameter /TURBOAUS zu Fehllalarmen führen. Deshalb dürfen NICHT zusätzlich die Optionen /KILL und/oder /DEL verwendet werden!

## 7.2 Virenbefall von Bootsektoren



Wenn VirScan einen Bootvirus in einem Bootsektor findet, ist es fast 100%-tig sicher, dass es sich nicht um einen Fehllalarm handelt!

## 7.3 Virenbefall von Dateien

### 7.3.1 Ein Virus in nur einer Datei



Wenn VirScan einen Virus in nur einer einzigen Datei gefunden hat, ist es sehr wahrscheinlich, dass es sich hier um einen Fehllalarm handelt. Besonders dann, wenn Sie die Datei schon mehrmals ausgeführt haben und sie sich auf der Festplatte befindet.

### 7.3.2 Mehrere Viren in einer Datei/Bootsektor



Wenn VirScan einen Virus gefunden hat kann es sein, dass VirScan in einer Datei bzw. im gleichen Bootsektor zwei Viren findet.

Der Hintergrund:

VirScan erkennt mit ca. 150 Suchstrings und AVR-Modulen 98% aller Computerviren die sich in der "Wildnis" befinden! Mit den restlichen Suchstrings werden "seltene" Viren gesucht, bzw. der gefundene Virus genauer untersucht. So kann es z.B. sein, dass VirScan einen Jerusalem.PcVsDs.Guru.2200 Virus anzeigt. Das bedeutet konkret, dass es sich um eine 2200 Bytes lange Variante des PcVsDs Virus (Untervariante Guru) handelt, der eine modifizierte Version eines Jerusalem Virus ist.

## 7.4 Die am weitesten verbreiteten Viren

Liste der in Europa am weitesten verbreiteten Boot und Datei Viren. Aktuelle Version siehe "Wildlist" in der Datei VIRSCAN.TXT und RIMC Projekt auf unserer Homepage. Es handelt sich hierbei um Viren, die bei Kunden (ca. 1990-1998) auftraten.

- AntiCMOS.A
- AntiEXE.A
- Argyle (Evolution)
- Arusiek.817
- ASBV
- Barrotes.1310.A

(c) by ROSE SWE

[http://come.to/rose\\_swe](http://come.to/rose_swe)

- BatchComp Trojan
- Burglar.1150
- Butterfly.302
- Byway.A
- Cascade.1701.A
- Cascade.1701.W
- Cascade.1704.A
- Cascade.1704.AC
- Civil\_Defense.6672
- Cluster
- Delwin 1199 & 1759 (Goblino)
- Dir-II.A (Creeping Death, Cluster)
- Ear.1700
- Explosion.1000
- F-Soft (drei Varianten)
- Fido.300
- Flip.2153.A/E
- FORM.A
- Gnat
- Hallöchen.2011
- Honecker Trojan
- HWF.937
- Imperial\_Probe
- Jerusalem.1808
- Jerusalem.AntiCad
- Jumper.B
- Junkie.A
- Kazor.4444.A
- Kerstin.923
- Major.1644
- Manzon
- MediaMarkt
- Megachirops.516 (Cryptor 1.07/Cryptor M2)
- MMIR.Red\_Mercury (RedSector, EatThis)
- Monte\_Carlo.1541
- MusicBug
- Natas.47xx
- Neuroquila.A/B
- Nightfall (alle Varianten)
- No\_of\_the\_Beast
- One\_Half (beide Varianten)
- Ontario.512
- Parity\_Boot.A
- Parity\_Boot.B (ca. 60 %)
- Parity\_Boot.ENC (NewBoot1/Quandary)
- Pieck
- Pojer
- Predator.McFly
- PS\_MPC/G2 (Weizenbier u.a.)
- Quicky (V.1376/Quicksilver)
- Quit
- Quox
- Reverse.A (Red Spider)
- Ripper (Jack\_the\_Ripper)
- Satan.616
- Scitzo.1329
- Seventh\_Son.302
- SideWinder
- Sirius (Hello, VFAC, Eumels & Annihilator)
- Siybelle.853
- SPE:Alive
- SPE:Alive.001
- SPE:Alive.003
- SPE:Homunculus
- Stoned.Angelina
- Stoned.Michelangelo
- Stoned.Monkey.B
- Stoned.Noint.A
- Stoned.Standard.A
- Tai-Pan.438 (Whisper)
- Tai-Pan.666 (Doom 2)
- Tequila
- Three\_Tunes
- Tiny.CPP.239
- Tony\_Boot.A
- Tremor
- Trivial (diverse)
- Trojector.1561
- UPS.1155
- V-Sign (Cansu)
- Vaccina.TP.5.A/Unk (Vaccina 1339)
- VBasic.5120
- VCL (Vega, Dumb u.a.)
- Vienna.648.Reboot.A (der Klassiker...)
- Vienna.AntiVir.724
- Vienna.AntiVir.970
- Vienna.BloodSpill.666
- Vienna.Bua
- Vienna.FHAS-1 (Vienna.486)
- Vienna.Pose.1155 (Byte-Warr.1155)
- Vienna.Pose.1164 (Byte Warrior)
- Weizen.471 (Weizenbier)
- Wet.A
- Whiskey
- Windows "!" Trojan
- Wordz
- Yankee\_Doodle.Login
- Yankee\_Doodle.TP.44.A (ehm. DDR!)
- Yankee\_Doodle.XPEH

## 7.5 Die Programme GUARD.SYS, VDEFEND.SYS, DEFENDER.COM und TSAFE.COM u.a.

Wenn VirScan die oben genannten Dateien untersucht kann es sein, dass VirScan bis zu 30 verschiedene Viren in solch einer Datei findet. Zum Beispiel kann der **Flip-Virus** in den Dateien DEFENDER.COM und TSAFE.COM (TNT-Virus) gefunden werden!

Falls Sie einen der o.g. Speicherwächter geladen haben, kann es sein, dass VirScan bis zu 55 Viren im Arbeitsspeicher findet!

### **Erklärung:**

Bei diesen Programmen handelt es sich um einen Fehllalarm, der einfach erklärt werden kann: Die Programme sind ebenfalls Antivirenprogramme und besitzen folglich auch sog. Virenerkennungen. Die Erkennungen werden normalerweise verschlüsselt im Programm oder in einer entsprechenden Datei abgelegt, damit andere Programme nicht versehentlich eine Vireninfektion melden.

Die Programme der Firma Carmel (Turbo Virus, TSafe u. a.), die auch für PC-Tools (VDEFEND.SYS) Antivirenprogramme geschrieben haben, sind diesbezüglich sehr schlampig programmiert! So passiert es, dass nach dem Starten der o. g. Programme die Erkennungen nicht aus dem Arbeitsspeicher entfernt werden! Andere Antivirenprogramme melden dann eine Verseuchung des Arbeitsspeichers!

Ebenfalls ärgerlich ist, dass die Erkennungen unverschlüsselt im Programm abgelegt werden, was leider zu Fehllarmen führt, wenn die gleichen Erkennungen verwendet werden (Anscheinend auch bei dem Programm PA-VirusScan v1.1 oder niedriger)!

## 7.6 Mehrere Viren im Arbeitsspeicher



Wenn Sie vor dem Starten von VirScan ein anderes Virensuchprogramm verwendet haben bzw. ein Antivirenprogramm verwendet, welches im Hintergrund vor Viren schützen soll, dann handelt es sich um einen Fehllalarm (siehe auch "die Programme GUARD.SYS, TSAFE.COM, DEFENDER.COM...")!

## 7.7 Analyse bei Virenverdacht



Wenn Sie sich nicht sicher sind, ob Sie einen Virus "besitzen", können Sie uns diesen einfach zusenden! Verwenden Sie hierzu den Fragebogen VIRMELD.DOC im Unterverzeichnis DOKU.

## 7.8 Unbekannte oder mutierte Viren



Lesen Sie hierzu die Anmerkungen die den Parametern /UNB (unbekannte Viren) und /MUTANT (mutierte Viren) beigefügt wurden!

## 8 Neue Funktionen und wissenswertes über VirScan Plus

### 8.1 Veränderungen der einzelnen Programmversionen

Dies stellt eine Kurzübersicht dar, die Datei WHATSNEW.DOC bzw. das Programm WHATSNEW enthält eine detaillierte Beschreibung der Programmverbesserungen.

Ab Version 4.55 von VirScan wurde eine neue Funktion integriert, mit der jedes Mal beim Starten von VirScan die Datei VIRSCAN.EXT eingelesen wird. In diese Datei können Sie die Erkennungen (sog. Signaturen) von neuen Viren hinzufügen. Dann wird zusätzlich nach diesen neuen Viren gesucht.

Ab Version 5.0 kann der Systemspeicher (Arbeitsspeicher) auf Virenbefall untersucht werden.

Ab Version 6.0 ist ein Virenkiller integriert. Zusätzlich kann VirScan jetzt jederzeit mit der ESC-Taste abgebrochen werden.

Ab Version 7.0 wurde eine Warnfunktion integriert. VirScan meldet bei einer Übereinstimmung des "Suchstring" mit der zu untersuchenden Datei von ca. 98% einen Virusverdacht. Damit kann VirScan auch modifizierte, aber bekannte Viren erkennen! Zusätzlich wird jetzt bei einer Festplatte der Partitionssektor mit untersucht.

In Version 7.8 ist ein intelligenter Dateiendebuffer integriert worden, um die Verarbeitungsgeschwindigkeit nochmals zu steigern. Weil der Tequila Virus keine konstanten Erkennungen besitzt wurde in VirScan ein zusätzlicher Suchalgorithmus eingebaut. Mehr hierzu siehe unten!

Version 8.0 wurde netzwerktauglich gemacht.

Version 8.5 findet mit der Option /UNB auch neue unbekannte Viren!

Version 8.6 kann den Arbeitsspeicher bis 1 MB untersuchen.

Version 9.0 hat einen eingebauten 'Autopiloten', der für unerfahrene Anwender alle nötigen Einstellungen vornimmt!

Version 9.20 findet mit der Option /MUTANT neue modifizierte Viren (teilweise auch noch unbekanntes)!

Version 9.40 unterstützt CD-ROM Laufwerke. Version 9.45 hat mehrere mathematische Vergleichsverfahren implementiert um hochgradig polymorph (=vielgestaltig) verschlüsselte Viren zu erkennen.

Version 9.50 verwendet einen heuristischen (regelbasierenden) Ansatz um unbekanntes Bootviren erkennen zu können (gleiches Verfahren wie CHKPC.COM)!

Version 10.00 hat einen heuristischen Codeanalyser und Minidisassembler eingebaut, um komplexe verschlüsselte Viren erkennen und identifizieren zu können!

Version 11.00 erkennt über 3900 Viren anhand einer Vielzahl von sog. AVR-Modulen.

Version 11.49 erkennt über 8500 Viren und hat einen mathematischen "Decryptor" eingebaut um hochkomplexe polymorphe Viren analysieren zu können!

Version 12.00 erkennt Script Viren und IRC Würmer.

Version 12.30 verwendet eine neue zusätzliche Suchmaschine (Datei Virscan.IRC).

## 8.2 VirScan und ein unübliches Dateidatum

VirScan erkennt alle "62-Seconds" und "100-Years" Viren anhand eines unüblichen Dateidatums (das Dateidatum ist auf das Jahr 2090 oder 60 bzw. 62 Sekunden gesetzt). VirScan erkennt auch Viren, die das Dateidatum auf den 13. Monat, 63 Minuten, 30 Stunden usw. setzen!

### 8.2.1 62-Sekunden/100 Jahre Viren

Fast alle Stealthviren verwenden einen Trick um zu erkennen, ob eine Datei schon infiziert wurde oder nicht. So wird z. B. die Uhrzeit auf 62 Sekunden bzw. das Datum auf das Jahr 2095 gesetzt, weil dies der DIR Befehl nicht anzeigt!

VirScan zeigt also keinen Virus an, sondern äußert nur den Verdacht auf das Vorhandensein eines solchen Virus. Dank dieser Routine haben schon mehrere Anwender brand-

neue Viren (u. a. Tequila, Predator, Agrypt, Natas, Frodo, Tremor und über zehn Vienna Varianten) entdeckt, weil diese Viren ebenfalls ein 62-Sekundeneintrag bzw. 100-Jahreeintrag verwenden! Etwa 10% aller Dateiviren setzen das Datum auf einen ungültigen Wert, um so schnell infizierte Dateien erkennen zu können! Fast alle Tarnkappen-viren verwenden diese Methode, um schnell infizierte von uninfizierten Dateien unterscheiden zu können!

Wenn Sie nur eine verdächtige Datei auf Ihrem Datenträger finden, können Sie davon ausgehen, dass diese Datei ein ungültiges Dateidatum besitzt. Besitzen jedoch alle EXE oder alle COM-Dateien auf der Festplatte ein ungültiges Datum, dann haben Sie einen Virus!

## 8.3 VirScan und Stealth Viren

Die so genannten Stealthviren (Stealth = heimlich) kann VirScan nur dann erkennen, wenn Sie von einer unverseuchten Diskette einen Kaltstart durchgeführt haben.

HINTERGRUND: Hat ein Stealth-Virus sich eingenistet, so wird dem Anwenderprogramm, das ein verseuchtes Programm untersucht, immer das Originalprogramm "vorgetäuscht", anstatt dem Verseuchten!

### 8.3.1 Der Parity\_Boot, AntiExe, Ripper Virus (u. a.)

Solch ein Virus wird nur erkannt, wenn von einer unverseuchten Diskette ein Kaltstart durchgeführt wird, da sonst der Virus einem die Kopie des Originalbootsektors "unterjubelt"! Also immer von einer schreibgeschützten Originaldiskette booten (sog. Stealth Virus)!

VirScan verwendet ab der Version 9.33 ein neues Verfahren, um eventuelle AKTIVE!!! Stealthviren auf Disketten entdecken zu können. Wenn Sie laufend z. B. den Parity Check Virus auf Disketten finden, aber nicht auf der Festplatte, liegt es daran, dass Sie keinen Kaltstart von einer virenfreien Diskette durchgeführt haben!

## 8.4 Suchverfahren mittels Platzhalter

Von einem Kunden haben wir 1992 den Tequilavirus erhalten, bei dem überhaupt nichts mehr konstant ist. Das einzige Merkmal einer verseuchten Datei ist, dass sie ein Dateidatum von 62 Sekunden hat. Deshalb verwendet VirScan (u.a.) eine Suchroutine, die auch mit Platzhaltern suchen kann (neben den AVR-Modulen). Der zusätzliche Vorteil

dieses Algorithmus ist, dass mit einer Erkennung, bis zu 100 Varianten eines Virusstammes erkannt werden können. (z. B. Jerusalem Familie)

Theoretisch wäre es möglich Virenerkennungen mit Platzhaltern in die Datei VIRSCAN.EXT aufzunehmen. Leider mussten wir feststellen, dass die meisten Anwender nicht in der Lage sind, neue Erkennungen der Datei hinzuzufügen. Deshalb wird dieser Punkt nicht beschrieben. Falls Sie VirScan nach einer solchen Erkennung suchen lassen wollen, so senden Sie uns bitte den Virus und die Erkennung zu! VirScan wird dann aktualisiert.

Zwischenzeitlich gibt es Viren, die sind so hochgradig variabel verschlüsselt, dass selbst das Suchverfahren mit Platzhaltern nicht mehr eingesetzt werden kann. Es muss dann ein mathematisches Näherungsverfahren (AVR-Modul) speziell für diesen Virus integriert werden!

## 8.5 Der Dateiendbugger

Wenn Sie VirScan im Turbomodus = EIN suchen lassen, untersucht VirScan erst einmal, wo der Virus sich befinden könnte (den so genannten Einsprungspunkt). Falls ein Programm jedoch ein Einsprungspunkt außerhalb der Datei besitzt, zeigt VirScan dies mit folgender Meldung an:

"Warnung: Einsprungspunkt außerhalb der Datei"

Wenn Sie diese Meldung ein oder zweimal erhalten, können Sie ziemlich sicher sein, dass diese Programme nicht lauffähig sind.

Falls jedoch fast jede Datei eine solche Warnung erzeugt, haben Sie einen Stealth-Virus im Arbeitsspeicher, der versucht VirScan auszutricksen. Bitte von einer absolut virenfreien Diskette booten und nochmals suchen lassen (zusätzlich mit AntiLink).

So erzeugt beispielsweise der aktive Tequilavirus (Stealth-Virus) pro infizierte Datei eine Anzeige von "62 Sekunden" und einen Einsprungspunkt außerhalb der Datei!

Die Arbeit des Debuggers wird in der untersten Zeile im Programm angezeigt (nur wenn der Turbomodus eingeschaltet ist). Sie erkennen dies an der Anzeige:

Scanning: -Dateiname-            xxxx Bytes.            Typ: (Typ/Ext)

## 8.5.1 Bedeutung von "Typ"

"Typ" ist das Resultat des Debuggers. Dabei bedeutet im einzelnen:

Typ	Beschreibung
AUS	Turbomodus ist ausgeschalten!
COM	Programm ist eine echte COM-Datei.
EXE	Ist eine echte EXE-Datei
MINI	Die Datei ist zu klein, um den Debugger einsetzen zu können, deshalb wird die ganze Datei untersucht.
NORM	Datei ist keine EXE Datei, wahrscheinlich eine COM-Datei! (z. B. eine GEM-Applikation, oder COM-Datei ohne Sprungbefehl)
PJMP	Ein, durch eine Mutation Engine verschlüsselter Sprung wurde gefunden und ermittelt (Poly-Jump).
PUSH, PRET	Eine Trick (PUSH, RET) den einige Viren verwenden wurde gefunden und ermittelt.
SYS	Datei ist ein Gerätetreiber (Systemdatei).
UNB	Datei ist wahrscheinlich kein ausführbares Programm, der Einsprungspunkt ist unbekannt.

## 8.5.2 Bedeutung von "Ext"

"Ext" ist die Dateiendung des Programms (im Dateinamen enthalten)

Was können Sie aus den Angaben schließen (Beispiele):

(COM/EXE)

Datei ist eine echte COM-Datei, wurde aber in EXE umbenannt.

(NORM/EXE)

Datei ist keine EXE Datei! Der Aufruf dieses Programms dürfte einen Systemabsturz mit sich ziehen.

(EXE/OBJ) (EXE/APP) (EXE/OVR) (EXE/OVR)

Datei ist vom Typ EXE, kann aber wahrscheinlich nicht ausgeführt werden, weil sie eine spezielle Overlaydatei ist. Ein Virus wird jedoch meistens solche Dateien infizieren, weil für ihn die Dateien wie normale Programme aussehen.

(SYS/EXE)

Datei ist ein Gerätetreiber, der als SYS-Datei von CONFIG.SYS aktiviert werden kann oder direkt ausgeführt werden kann. Beispiel: EMM386.EXE

## 8.6 Der Integrierte Virenschutz

Das Programm enthält einen integrierten Checksummentester, um einen möglichen Virenbefall gleich anzeigen zu können. Die zum Programm gehörige Checksumme befindet sich in der Datei mit der Endung "XXX".

Diese in der Datei befindliche Checksumme sowie das Hauptprogramm dürfen auf keinen Fall verändert bzw. modifiziert werden! Das Hauptprogramm nimmt sonst an, es sei eventuell von einem Virus befallen worden (dem Programm noch unbekannter Virus)!

### 8.6.1 Der eingebaute Checksummentester

Folgende Merkmale der EXE-Datei werden überwacht und auf Veränderungen überprüft:

- n** Checksumme - Wird auch nur ein Bit des Programms vom Virus verändert, so stimmt die Checksumme nicht mehr (eigene sichere Routine, nach ANSI X3.66 - CRC-Poly ist: 0xDEBB20E3).
- n** Dateilänge - Wird ein Programm über Nacht um ein oder zwei KB länger, ist es infiziert!

 Wir raten ab, irgendwelche Änderungen an der EXE & XXX-Datei durchzuführen, da dann das Programm mit Sicherheit nicht mehr läuft! Die Datei mit der Endung "XXX" enthält auch die aktuelle Version, wie viel verschiedene Viren vom Checksummentester erkannt werden können. Das Testen der Checksumme nimmt ca. 0.1-2 Sekunden Zeit in Anspruch (je nach Rechnertyp und Laufwerk). Unserer Ansicht nach einem vertretbaren Aufwand! Ist die Checksumme in Ordnung, wird das Programm ausgeführt. Andernfalls wird eine ausführliche Fehlermeldung mit Hinweisen auf mögliche Fehlerquellen ausgegeben.

## 8.6.2 Hinweise für das Programm SCAN.EXE

Ab der Version 4v65 von SCAN.EXE von McAfee gibt es die Optionen:

```
n    /AV - add validate bzw. /AG
n    /CV - check validate bzw. /CG
n    /RV - remove validate bzw. /RG
```

Diese Funktionen sind aber inkompatibel mit dem Checksummentester von VirScan, weil die Funktionen /AD und /RV jeweils 10 Bytes zum EXE-Programm hinzuaddieren bzw. entfernen!

 Wir raten von diesen Funktionen ab, denn jedes Mal wenn Sie SCAN C: /AV eingeben, verbraucht SCAN (bei 1000 Dateien) zwischen 10 KB und ca. 1 MB Speicherplatz, der unwiderruflich verloren ist!

Falls Sie versehentlich SCAN /AV oder /RV eingegeben haben, so ist das Programm **Z E R S T Ö R T**, weil der Programmselbstschutz annimmt, ein Virus hat das Programm befallen. Es reichen schon ein paar Bytes Veränderung um einen Virus einzupflanzen!

## 8.6.3 Hinweise für die Programme TAV & FShield

Mit den Programmen Turbo Anti Virus der Firma Carmel, FileShield von McAfee, Viren Schutz Schild von ROSE u. a., ist es möglich, ausführbare Programme gegen Manipulation (Virenbefall) zu schützen. Dies wird erreicht, indem das Programm mit einer "Schutzhülle" versehen wird. Diese Schutzhülle ist ein kleines Maschinenspracheprogramm und hat eine Länge zwischen 400 und 2800 Bytes. Für den integrierten Checksummentester ist ein solcher Längenzuwachs natürlich sehr virenverdächtig - das Programm wird NICHT ausgeführt, wenn es nachträglich mit einem solchen Programm geimpft wurde!

## 8.7 VirScan und Arbeitsspeicher

VirScan verwendet Overlays, um den Speicherverbrauch zu minimieren. Falls EMS-Speicher vorhanden ist, wird dieser unterstützt! VirScan benötigt 500 KB freien Arbeitsspeicher, mit der Option Virenkiller je nach zu entfernendem Virus bis zu 580 KB! Trotzdem kann es vorkommen, dass für die Ausführung von VirScan nicht genügend Speicher vor-

handen ist. Dies wird von VirScan durch zwei Arten signalisiert:

1. Runtime Watchdog: Runtime Error 203 at xxxx:xxxx
2. Error: Not enough memory to start this program properly...

Bei der ersten Fehlermeldung hat VirScan noch nicht einmal genügend freien Speicher, um seine Ausgaberroutinen zu laden, während bei der zweiten Fehlermeldung VirScan angeben kann, wie viel Speicher noch zur Verfügung steht.

Falls Sie nicht genügend freien Speicher unter DOS zur Verfügung haben müssen Sie Ihre Speicherbelegung optimieren. Starten Sie bei MS-DOS Version 6.00 oder besser, einfach das Programm MEMMAKER! Sollten Sie kein MS-DOS besitzen, müssen Sie Ihre CONFIG.SYS und AUTOEXEC.BAT von Hand optimieren, verwenden Sie auf jeden Fall den Befehl LoadHigh. Entfernen Sie unnötige speicherresidente Programme, um mehr freien Arbeitsspeicher zu erhalten.

Alternativ können Sie mit MAKEBOOT (Vollversion) eine Bootdiskette erstellen, die nur die nötigsten Treiber enthält!

## 9 Alles Wissenswerte über Viren



Dieses Kapitel wurde komplett überarbeitet und erweitert. Weil dieses Kapitel allgemeingültig gehalten wurde und direkt nichts mit der Funktionsweise von VirScan zu tun hat, wurde dieses Kapitel in einer eigenen Datei untergebracht. Diese Datei heißt VIRUSDEF.DOC und enthält eine Klassifizierung aller Virenarten und Virengattungen, sowie ein historischer Rückblick über Computerviren.

### 9.1 Kurzbeschreibung aller Viren

Wenn Sie eine kurze Beschreibung zu einem bestimmten Virus suchen, so schauen Sie in der Datei VIRBIBEL.DOC nach! Diese Datei wird von uns immer wieder ergänzt. In der Datei VIRBIBEL.DOC finden Sie die Beschreibung zu verschiedenen Viren. Weitere Informationen über Viren können Sie sich auch in der Datei VIRSCAN.TXT ansehen.

Eine ausführliche Beschreibung zu einigen in Deutschland stark verbreiteten Viren finden Sie in der Datei BESCHREI.DOC!

Alternativ bietet ROSE SWE auch das Programm ViBa an. ViBa ist eine Datenbank nach SAA-Standard und enthält eine Beschreibung zu allen derzeit bekannten Viren (siehe auch REGISTER.COM).

## 10 Registration, Bestellungen und Sonstiges

Die Verwendung der Sharewareversion ist für vier Wochen zum Testen erlaubt. Nach dieser Periode MÜSSEN Sie sich eine Vollversion erwerben, andernfalls müssen Sie diese Software auf Ihrem System entfernen! Überlegen Sie sich auch, wie viel Arbeit hinter solch einem Programm steckt! Sie unterstützen nicht nur den Programmautor mit Ihrer Registration, sondern auch die Entwicklung anderer Programme und die Sharewareidee im allgemeinen!

### 10.1 Registrieren

Wenn Sie VirScan Plus oder auch an weiteren Produkten von ROSE SWE interessiert sind, so benutzen Sie bitte den Bestellschein der ausgedruckt wird, wenn Sie das Programm REGISTER.COM starten! Disketten sind nicht mehr im Format 5¼" Zoll (HD) lieferbar! Falls möglich erfolgt die Auslieferung auf CD-ROM.

Kleiner Tipp: Am einfachsten geht es, wenn Sie das Programm REGISTER.COM starten. Es wird dann ein kompletter Bestellschein ausgedruckt. Auf diesem Bestellschein können Sie auch noch verschiedene Optionen ankreuzen. Bei Fragen bezüglich des Bestellen's können Sie -falls vorhanden- das Programm BESTELLN.COM starten, welches weitere Tips enthält!

Als registrierter Anwender erhalten Sie weitere Programme zum halben Preis. Falls gewünscht, können Sie dann vom automatischen Update-Service Gebrauch machen. Zusätzliche Beratung bei Virenproblemen und nicht zuletzt Analyse von virenverdächtigen Code/Programmen.

### 10.2 Keydatei für VirScan Plus

VirScan Plus unterstützt so genannte Keydateien. Dies ist eine Datei, in der sich Ihre Adresse befindet. Wird diese Keydatei zu einer Sharewareversion hinzu kopiert fallen die Sharewarehinweise weg und stattdessen wird als Lizenznehmer Ihr Name ausgegeben. Sämtliche Funktionen der Vollversion werden durch die Keydatei frei geschalten.

**Welche Vorteile hat solch eine Keydatei?**

- Sie können sich aus dem Internet die aktuelle VirScan Plus Version herunterladen, haben somit immer eine aktuelle verfügbare Version. Bezugsquellen: Siehe ROSEBBS.TXT
- Sie ersparen sich und uns Schriftwechsel und das Bestellen von Updates.
- Persönliche Version mit Ihrem Namen als Lizenznehmer.
- Der Key ist 3 Jahre (36 Monate gültig). Zurzeit sind die Keydateien noch NICHT zeitlich beschränkt (Sonderaktion)! Also zugreifen!
- Sie können die Sharewareversion von VirScan Plus an Bekannte weitergeben, nur die Keydatei dürfen Sie nicht weitergeben!

### **Nachteile der Keydatei?**

- Sie müssen sich selbst die aktuelle Sharewareversion beschaffen. Wenn Sie wünschen können Sie sich per E-mail von uns über aktuelle Sharewareversionen informieren lassen. Mehr hierzu siehe Datei: ROSEBBS.TXT!
- In der Vollversion sind zusätzliche Bonusprogramme sowie weitere Texte beigefügt. Ein Teil der Bonusprogramme befinden sich in folgenden Archiven, die requestbar sind: DECOM.RAR, MBRKILL.RAR und MSCAN\*.RAR. Requestadressen siehe ROSEBBS.TXT
- Die Sharewareversion benötigt ca. 10 KB mehr Arbeitsspeicher für Sharewarehinweise.

**Hinweis:** Es ist nur möglich, pro bestellter VirScan Plus Vollversion eine Keydatei zu bestellen. Es gibt also zwei Möglichkeiten diese Keydatei zu beziehen:

1. Bestellung von VirScan Plus und der Keydatei.
2. Bestellung von VirScan Plus. Bestellung zum späteren Zeitpunkt der Keydatei. Sie erhalten dann die Keydatei mit einer aktuellen Sharewareversion zugesandt oder die Keydatei per Internet zugemailt. Für den Mailversand empfehlen wir PGP Verschlüsselung. Unabhängig hiervon wird eine Porto und Verpackungspauschale erhoben.

Kunden die bei einem Zwischenhändler eine Vollversion erworben haben können, wie unter 2.) aufgeführt, unter Angabe der Seriennummer eine Keydatei beziehen!

## 10.3 Anfragen

Anfragen, bezüglich der Sharewareversionen des entsprechenden Programms, werden nur dann beantwortet, wenn ein entsprechend frankierter Freiumschlag beigefügt ist! Triviale Anfragen, Anfragen die durch dieses Handbuchs geklärt werden können, werden unter Umständen NICHT beantwortet (viel zu teuer, viel zu umständlich!). Wenn Sie die Vollversion bei einem von ROSE SWE autorisierten Händler erworben haben, so wenden Sie sich zur Klärung Ihres Problems zuerst an ihn. Wir bitten Sie auch, von telefonischen Anfragen (oder evtl. "Anfragen zur Beseitigung eines Virus") abzusehen.

Sie können uns auch eine Email senden. Sie können zusätzlich virenverdächtigen Code als MIME "Attachement", als PGP-Datei oder als eine XX/UUdecoded Datei senden. Den PGP-Key finden Sie in der Datei ROSEBBS.TXT!

**Email, Fido und FAX: Siehe Datei ROSEBBS.TXT!**

### 10.3.1 Adresse

**ROSE Softwareentwicklung  
Dipl.-Ing. Ralph Roth  
Finkenweg 24**

**D 78658 Zimmern o. R.**

**FAX und Anrufbeantworter: +49.731-553310**

Bitte per Email aktuelle Adresse erfragen, falls Sie eine rasche Zustellung wünschen.

Anmerkung: Falls Sie ein Problem mit einem Virus haben, senden Sie uns lieber gleich eine infizierte Diskette oder Email zu.

### 10.3.2 Kommerzielle Anwender

Sie können zum Sonderpreis Mehrplatzlizenzen beim ROSE SWE erwerben. Setzen Sie sich, unter der Angabe des gewünschten Programms und der gewünschten Anzahl, schriftlich (am besten per FAX) mit uns in Verbindung.

## 10.4 Sonstiges

Falls Sie Anregungen, Verbesserungen oder auch Laufzeitfehler zu diesem Programm haben, so teilen Sie dies bitte auf einem Extrablatt mit. Denn nur so kann das Programm noch verbessert werden! Vielen Dank schon im voraus. Für Fehler im Programm, und für durch Fehler verursachte Schäden wird keine Haftung übernommen!



Verdächtige Programme bitte unter Verwendung der Datei VIRMELD.DOC an o. g. Adresse einsenden!

### 10.4.1 Ein Dankeschön an...

... Jürgen Werner für Tips zur Suchoptimierung, Thomas Krämer für Farbberatung und Signaturenbeschaffung, Tiffy, Peter Schöpf, Dietmar Braun und Eckart Beck für Test und Signaturenbeschaffung. Peter Hubinsky, Grischa Brockhaus, Andreas Marx, Thomas Geiger, den Autoren von HMVS (Jan & Lubos), Martin Rösler, Ralf Borgmann, Frederic Ahring und Stefan Kurtzhals. Daniela, Iris und Jutta für Korrektur. Gunther Zink für CD-ROM Tests. Jürgen Werner für die Überlassung von Programmroutinen. Olaf Kolling für dies und das (ya'know what i mean guy?). Kaot, Andreas Haak, Rand0m und Ghostbuster für die Programmierung von Killer-routinen.

... allen Sysops die VirScan verteilen (Ralph Biedermann, Pascal Äbi, Christian Emig, Virnet, SAC ftp, Camilla BBS, VHM, Joe Hartmann...).

... alle Anwender und Studenten der FHAS und Tübingen, die neue Viren zugesandt haben und sich mit Kritik und Verbesserungsvorschlägen nicht hinter dem Berg hielten.

### 10.4.2 Garantiausschlusserklärung



**Der Autor des Programms weist darauf hin, dass die Benutzung des Programms auf Ihre eigene Gefahr hin geschieht. Bei den Optionen "Viren entfernen" und "Dateien löschen" kann es bei unsachgemäßer Handhabung zu Datenverlusten kommen!**

Unter keinen Umständen ist der Programmautor haftbar für jegliche Folgeschäden, einschließlich aller entgangenen Gewinne und Vermögensverluste, oder anderer mittelbarer und unmittelbarer Schäden, die durch den Gebrauch oder die Nichtverwendbarkeit dieser Software und ihrer begle-

itenden Dokumentationen entsteht. Dies gilt auch dann, wenn der Autor über die Möglichkeit solcher Schäden unterrichtet war oder ist!

## 11 Ende des Handbuches

---

Vielen Dank, dass Sie diese Datei gelesen haben!