VirusZ_II_Deutsch

COLLABORATORS			
	TITLE : VirusZ_II_Deutsch		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		July 20, 2024	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VirusZ_II_Deutsch

1.1 Inhalt

VirusZ II 1.30
- Deutsche Anleitung -

SHAREWARE

1.2 Wichtiger Hinweis

Nachdem in letzter Zeit einige Fakes von VirusZ in Umlauf gekommen sind, enthalten ab jetzt alle Versionen ihre Original-Dateilänge im "About" Fenster. Wenn Sie sich nicht sicher sind, ob Sie eine saubere Version von

VirusZ erhalten haben, entpacken sie das Archiv zunächst auf eine bootbare Diskette, deaktivieren Sie alle Harddisks im BootMenu und fahren Sie das System von der vorbereiteten Diskette hoch (es werden die reqtools.library, die xfdmaster.library und die commodities.library im Verzeichnis Libs: benötigt). Vergleichen Sie nun die angegebene Länge im "About" Fenster mit der tatsächlichen Dateilänge ihrer Version. Stimmen die Werte überein, ist eine Infektion auszuschließen und Sie können das Programm getrost verwenden. Ansonsten ist das Löschen des veränderten Programmes angeraten.

Wenn Sie eine 100% saubere Version des aktuellsten VirusZ bekommen möchten, wenden Sie sich an die aufgeführten offiziellen Bezugsquellen.

Falls Sie irgendwelche Patches installiert haben, die VirusZ nicht erkennt und die harmlos sind, sollten Sie die entsprechende 'Check On Startup' Option ausschalten, um die Meldungen zu unterdrücken. Der Überwachungsmodus garantiert trotzdem die Erkennung erneuter Veränderungen an den Vektoren. Diese Methode arbeitet aber nur einwandfrei, wenn Sie VirusZ erst nach Installation aller Patches starten, da diese sonst vom Überwachungsmodus aufgegriffen werden.

1.3 Rechtliches

Das komplette VirusZ Softwarepaket mit Ausnahme der Reqtools.Library wurde geschrieben von Georg Hörmann und ist urheberrechtlich geschützt. Die Reqtools.Library wurde von Nico François geschrieben und darf frei kopiert werden. Die MagicWB Piktogramme wurden von Martin Huttenloher und Timm S. Müller entworfen.

Die Dateien dieses Paketes dürfen in keiner Weise verändert werden. Das Archivieren des gesamten Paketes ist erlaubt.

Der Autor ist weder verantwortlich für von Dritten vorgenommene Veränderungen an Teilen dieses Softwarepaketes noch für eventuelle Schäden oder Datenverluste, die durch die Benutzung dieses Programmes auftreten können.

1.4 Vertrieb

Durch den Vertrieb dieser Software dürfen keine größeren Gewinne erzielt werden. Eine geringfügige Gebühr für das Kopieren der Software und zur Deckung der Kosten für den Datenträger darf erhoben werden. Sie sollte eine Höhe von DM 5 nicht überschreiten. VirusZ darf ohne meine Genehmigung auf allen Public Domain CDs (wie Fred Fish etc.) vertrieben werden, solange es sich um keine kommerziellen Produkte handelt. Wenn Sie dieses Paket an Bekannte weitergeben wollen, so darf dies nur im kompletten Zustand geschehen. Falls Sie selbst bereits ein unvollständiges Paket erhalten haben, sollten Sie sich ihre Programme in Zukunft woanders besorgen. Zur Kontrolle folgt eine Auflistung aller Dateien, die zu diesem Paket gehören:

```
VirusZ (dir)
   ARexx (dir)
      CheckArc.vzrx
```

```
         CheckDir.vzrx
         CheckFile.vzrx
      Libs (dir)
         xfd (dir)
            .README.FIRST
            [...]
         xfdmaster.library
         reqtools.library
      ANSi.THeReaLM
      ANSi.ViRuSHeLP_DK
      Install Libs
      Install Libs.info
      Install.script
      VirusZ
      VirusZ.info
      VirusZ_Deutsch.Guide
      VirusZ_Deutsch.Guide.info
      VirusZ_English.Guide
      VirusZ_English.Guide.info
      VirusZ.History
      VirusZ.History.info
   VirusZ.info
```

1.5 Bezugsquellen

VirusZ erscheint unregelmäßig auf vielen BBSen und PD-Serien. Um wirklich die jeweils aktuellste Version zu erhalten, wenden Sie sich an folgende Bezugsquellen:

```
            Über Modem:                          TIME PD-Disketten:

             THE REALM                           A.P.S. -electronic-
         ++49-(0)515-43528                         Zu den Eichen 4
            UP TO 14.4k                            31634 Steimbke
         ONE NODE RINGDOWN                 Fon: 05026-1700  Fax: 05026-1615

            Nirvana BBS
      USR V34 FC Dual Standard
        ++49-(0)511-9524227
            V32 bis Node
         ++49-(0)511-522809

   Virus Help BBS - Team Denmark
        SysOp: Jan Andersen
          ++45-4659-6867
           USR 33.6 V.FC
```

Alle Anti-Viren-Programme können von der Virus Help BBS frei gezogen werden.

Zusatz-Info über THE REALM (vom Sysop persönlich):

Es gibt jetzt einen eigenen Account für VirusZ Benutzer. Jeder, der VirusZ haben will, der loggt sich als Handle: VirusZ, Password: VirusZ ein, und schon kann das neueste VirusZ gezogen werden.

Jeder, der sich auch gerne mal mit anderen Usern unterhalten will, aber eigentlich doch nur das neueste VirusZ haben möchte, der kann sich als richtiger User einloggen, braucht aber den Fragebogen NICHT auszufüllen, d.h. mir keine persönlichen Daten (z.B. Vorname, Tel.-Nr., ...) geben. Solche User bekommen dann einen eingeschränkten Zugriff auf die BBS.

Natürlich gibt es auch noch den ganz normalen Account, da kann sich jeder eintragen und bekommt dann vollen Zugriff auf die BBS.

Ein Userbeitrag oder Sauggebühr wird nicht erhoben, warum auch?

1.6 Shareware

VirusZ wird als Shareware vertrieben. Das bedeutet für Sie, daß Sie das Programm sowohl testen als auch weitergeben dürfen, aber bei regelmäßiger Benutzung eine Gebühr an den Autor zu entrichten haben. Dies nicht zu tun ist sowohl moralisch verwerflich als auch illegal. Wenn Sie die Gebühr bereits für eine ältere Programmversion entrichtet haben, bleibt es Ihnen überlassen, ob Sie dies wiederholen möchten. Ansonsten wird eine finanzielle Zuwendung in Höhe von DM 20 oder mehr empfohlen.

Die Entrichtung der Gebühr beinhaltet keinerlei Ansprüche auf Zusendung von Updates. Wenn Sie unbedingt auf einem derartigen Service bestehen, müssen Sie zusätzlich eine Diskette sowie genügend Rückporto (mindestens DM 3) beilegen.

1.7 Zusendungen

Falls Sie auf neue Viren, Patches oder Cruncher gestoßen sind, würde ich mich über deren Zusendung im Interesse aller Anwender freuen. Wenn Sie Ihre Diskette(n) zurückbekommen möchten, müssen Sie ausreichend Rückporto (DM 3) beilegen. Bei Unterlassung behalte ich mir vor, den/die Datenträger nicht zurückzusenden. Hier ist meine Adresse:

Georg Hörmann
Martinswinkelstraße 16c
82467 Garmisch-Partenkirchen
Germany

Ich habe keinen Internet-Zugang, und das aus folgenden Gründen:
1. Ich bin kein Student, der das Ganze umsonst an der Uni haben kann.
2. Ich habe (noch) keinen Goldesel für die Telefonrechnungen.
3. Ich habe momentan zu wenig Zeit, um mich überhaupt in die Materie einzuarbeiten und dann auch noch täglich Post zu bearbeiten.

1.8 Einführung

Dieses Kapitel soll nur einen groben Überblick darüber vermitteln, welche Möglichkeiten Ihnen VirusZ bietet.

Als erstes sollte erwähnt werden, daß VirusZ als Hintergrundprogramm benutzt werden kann, um jederzeit Disketten und Speicher zu überwachen. Sowohl für diese Tätigkeit als auch für jedes andere Aufgabengebiet stellt VirusZ umfangreiche Einstellungsmöglichkeiten zur Verfügung.

Außerdem bietet VirusZ verschiedene Prüfmechanismen für Dateien, Sektoren, Systemvektoren und Bootblöcke. Diese sollten immer dann verwendet werden, wenn Sie neue Software erhalten haben.

Schließlich kann VirusZ teilweise auch über ARexx gesteuert werden, was Sie in die Lage versetzt, Funktionen auch aus anderen Programmen aufzurufen.

VirusZ wurde als Commodity konzipiert und verzichtet komplett auf unsaubere Tricks, es folgt den Richtlinien des Style Guides und bietet Tastaturkürzel, Reqtools-Requester und viele andere nützliche Konzepte.

VirusZ ist weder lokalisierbar noch zeichensatzunabhängig! Daran wird sich auch in Zukunft nichts ändern, weil das ursprüngliche Konzept des Hintergrundprogramms immer erhalten bleiben wird. Die Unterstützung verschiedener Sprachen und Zeichensätze brächte aber unweigerlich eine enorme Volumenzunahme des Programms mit sich, die es für viele Anwender unmöglich machen würde, VirusZ ständig laufen zu lassen.

1.9 Voraussetzungen

Diese Version von VirusZ II benötigt folgende System-Resourcen:

- Kickstart 2.04 (oder neuer)
- MC68000 (oder besser)
- commodities.library v37+
- reqtools.library v38+
- xfdmaster.library v37+
- rexxsyslib.library v33+ (für ARexx Kommandos)

1.10 Installation

Kopieren Sie die Bibliotheken aus dem 'Libs'-Verzeichnis des VirusZ-Archivs bitte in das LIBS: Verzeichnis Ihrer System-Diskette oder Harddisk. Sie können zu diesen Zweck auch die 'Install Libs' Batchdatei aufrufen.

Nun können Sie entweder das VirusZ Piktogramm in Ihr WBStartup Verzeichnis ziehen oder folgende Zeile in Ihrer 'S:User-Startup' Datei einfügen:

VirusZ [Optionen]

Ein Verzeichnis aller verfügbaren Optionen ist im Kapitel Shell-Optionen enthalten.

1.11 Shell-Optionen

VirusZ unterstützt die folgende Schablone:

CX_PRIORITY/N/K,CX_POPKEY/K,CX_POPUP/K,PUBSCREEN/K,FC=FILECHECK/K,
DE=DECREXEC/S,DD=DECRDATA/S,ALL/S,AREXX/K,QUIT/S

Für eine detailliertere Beschreibung der Shell-Syntax, der Benutzung von Commodity-Programmen und der Definition von Hotkeys lesen Sie bitte das Ihrem Amiga beiliegende Handbuch.

Bitte beachten Sie, daß diejenigen Shell-Befehle, die eine Nachricht an den ARexx-Port von VirusZ versenden, zuerst testen, ob VirusZ schon aktiv ist. Falls dies nicht der Fall sein sollte, wird VirusZ zuerst installiert und anschließend das jeweilige Kommando an den Port versandt.

CX_PRIORITY:
Dieses Schlüsselwort definiert die Priorität des VirusZ-Brokers. Es werden Werte zwischen -128 und 127 unterstützt, der Standardwert ist 0.

CX_POPKEY:
Bei Angabe dieses Schlüsselwortes wird die darauffolgende Hotkey-Kombination als neue Grundeinstellung übernommen.

CX_POPUP:
Nach diesem Schlüsselwort muß entweder 'YES' (Ja) oder 'NO' (Nein) folgen. Je nach Angabe öffnet VirusZ dann beim Start sein Fenster.

PUBSCREEN:
Mit Angabe dieser Option gefolgt von einen gültigen Screen-Namen kann erreicht werden, daß VirusZ sein Fenster auf eben jenem Screen öffnet und nicht wie standardmäßig auf der Workbench.

FILECHECK:
Hierbei handelt es sich nicht um eine Option, sondern ein Kommando. Dabei wird das übergebene Argument nach etwaigen Jokern durchsucht und alle passenden Dateien mittels des ARexx-Kommandos CHECKFILE getestet. Es werden folgende Returncodes unterstützt:
RC = 0 : Test beendet, keine Viren gefunden.
RC = 5 : Eine oder mehrere Dateien sind verseucht!
RC = 10: Fehler beim Testen.
Beispiel: VirusZ FILECHECK "dh0:~(#?.info)" DECREXEC

DECREXEC:
Diese Option gilt nur in Verbindung mit FILECHECK und schaltet das Entpacken ausführbarer Dateien ein.

DECRDATA:
Diese Option gilt nur in Verbindung mit FILECHECK und schaltet das Entpacken nicht-ausführbarer Dateien ein.

ALL:
Diese Option gilt nur in Verbindung mit FILECHECK und veranlaßt VirusZ, auch alle existierenden Unterverzeichnisse des Suchpfades zu durchsuchen.

AREXX:
Dieses Kommando ermöglicht es, einen von VirusZ unterstützten ARexx-Befehl direkt an den Port von VirusZ zu senden. Das Argument wird einfach an den

ARexx-Port weitergereicht. Der Returncode der Shell entspricht dann dem des ausgeführten ARexx-Befehls.
Beispiel: VirusZ AREXX "CHECKDIR dh0: SKIPDIRS"

QUIT:
Diese Option sendet den ARexx-Befehl QUIT an den VirusZ-Prozess und beendet ihn damit. Dies ist sinnvoll in Script-Dateien, um VirusZ z.B. nach dem Prüfen einiger Dateien wieder beenden zu können.

1.12 Workbench Tooltypes

Für eine ausführliche Erklärung zur Benutzung von Workbench Tooltypes und Commodity-Programmen und der Definition von Hotkeys lesen Sie bitte das Ihrem Amiga beiliegende Handbuch.

VirusZ unterstützt folgende Tooltypes:

CX_PRIORITY:
Dieses Schlüsselwort definiert die Priorität des VirusZ-Brokers. Es werden Werte zwischen -128 und 127 unterstützt, der Standardwert ist 0.

CX_POPKEY:
Bei Angabe dieses Schlüsselwortes wird die darauffolgende Hotkey-Kombination als neue Grundeinstellung übernommen.

CX_POPUP:
Nach diesem Schlüsselwort muß entweder 'YES' (Ja) oder 'NO' (Nein) folgen. Je nach Angabe öffnet VirusZ dann beim Start sein Fenster.

PUBSCREEN:
Mit Angabe dieser Option gefolgt von einen gültigen Screen-Namen kann erreicht werden, daß VirusZ sein Fenster auf eben jenem Screen öffnet und nicht wie standardmäßig auf der Workbench.

1.13 Hintergrund

Um das sofortige Überprüfen neu eingelegter Disketten und auch des Speichers immer zu gewährleisten, sogar wenn z.B. gerade Dateien oder System-Vektoren geprüft werden, ist der Hintergrund-Checker als zweiter Task installiert. Dieser Task erledigt mehrere Dinge:

1. Er testet eine Vielzahl von Speicherstellen und Library/Device-Vektoren auf bekannte Viren und entfernt diese gegebenenfalls aus dem Speicher.
2. Er prüft den Bootblock jeder neu eingelegten Diskette auf Viren.
3. Er prüft den Disk-Validator jeder neu eingelegten Diskette auf Viren.
4. Er überwacht alle wichtigen Systemvektoren auf Veränderungen.

Lesen Sie dazu auch die Background Voreinstellungen.

1.14 Menüs

Wenn das Hauptfenster von VirusZ aktiv ist, können Sie aus den folgenden beiden Menüs Funktionen auswählen:

Project	Prefs
File Check	File Check
Sector Check	Sector Check
Vector Check	Vector Check
Bootblock Lab	Bootblock Lab
Show Brains...	Background
About...	Miscellaneous
Hide	Save Prefs
Quit	

1.15 ARexx Port

VirusZ hat nun auch endlich einen ARexx Port. Der Name dieses Ports ist 'VIRUSZ_II.REXX' und er bietet folgende Kommandos:

HIDE	QUIT
CHECKFILE	CHECKDIR

Bitte werfen Sie auch einen Blick auf die Scripts im ARexx Verzeichnis. Sie werden als Beispiele zur Verwendung der Kommandos mitgeliefert und zeigen eindrucksvoll die Möglichkeiten, die sich durch ARexx bieten.

1.16 ARexx: HIDE

Syntax: HIDE

Dieses Kommando veranlaßt VirusZ, sein Hauptfenster zu schließen und im Hintergrund weiterzuarbeiten. Um das Fenster wieder zu öffnen benutzen Sie bitte den definierten Hotkey oder das Exchange Commodity.

1.17 ARexx: QUIT

Syntax: QUIT

Dieses Kommando beendet VirusZ.

1.18 ARexx: CHECKFILE

```
Syntax: CHECKFILE Datei [DECREXEC] [DECRDATA]

Datei  ist der Name (incl.  Pfadangabe) der Datei, die zu prüfen ist.  Bitte
beachten  Sie, daß im ARexx-Modus nur geprüft, jedoch nicht repariert werden
kann.   Die  Optionen  DECREXEC und DECRDATA veranlassen VirusZ, ausführbare
bzw. nicht ausführbare Dateien vor der Überprüfung zu entpacken.

Sie erhalten eines der folgenden Ergebnisse:
RC =  0 : Alles lief glatt und die Datei ist sauber.
RC =  5 : Datei ist infiziert!
RC = 10 : Fehler beim Prüfen. Das kann an einem falschen Dateinamen, einer
          falsch geschriebenen Option oder einem internen Fehler liegen.
```

1.19 ARexx: CHECKDIR

```
Syntax: CHECKDIR Verz [SKIPDIRS] [DECREXEC] [DECRDATA]

Verz  ist das Verzeichnis, welches geprüft werden soll.  Bitte beachten Sie,
daß  alle  Dateien in diesem Verzeichnis nur überprüft, nicht aber repariert
werden.   Normalerweise  durchsucht VirusZ auch alle Unterverzeichnisse, die
im  angegebenen  Verzeichnis existieren.  Mit SKIPDIRS kann dies unterbunden
werden.    Die   Optionen  DECREXEC  und  DECRDATA  schalten  das  Entpacken
ausführbarer bzw.  nicht-ausführbarer Dateien ein.

Sie erhalten eines der folgenden Ergebnisse:
RC =  0 : Test abgeschlossen, keine Viren gefunden.
RC =  5 : Eine oder mehrere Dateien sind verseucht!
RC = 10 : Fehler beim Prüfen. Das kann an einem falschen Verzeichnisnamen,
          einer falsch geschriebenen Option oder einem internen Fehler
          wie z.B. Speichermangel liegen.
```

1.20 Danksagungen

Folgenden Personen möchte ich meinen besonderen Dank aussprechen:

* Flake/TRSI für Viren, Patches, Fehlerberichte und die aktuellen Neuigkeiten aus dem Netz
* Jan Bo Andersen, Lars Kristensen und alle anderen Mitglieder von Virus Help - Team Denmark für Viren, Übersetzungen und einen großartigen Support
* Holger Hesselbarth für Patches, Ideen und mehr
* Ralf Thanner für alles (ein Name sagt mehr als 1000 Worte:-))
* Axel Folley für moralische und finanzielle Unterstützung
* Holger Wessling für seinen unglaublichen Ideenreichtum
* Dave Jones für Patches, Viren, Bugreports und vieles mehr
* Martin Huttenloher für MagicWB
* Martin Odaischi für Dutzende von Viren und großzügige Finanzspritzen
* Heinz Lindner für residente Programme und neue Kickstartversionen
* Markus Stiebeling für Fehlerberichte und Tips
* Rüdiger Prang für Patches und TEX-Docs
* Steve/Silicon Designs 3003 für Viren und Cruncher

* Jim Maciorowski für seine Unterstützung, Briefe und Spenden
* allen restlichen Personen, die mich im Laufe der Zeit unterstützt haben
* und selbstverständlich allen registrierten Benutzern von VirusZ

1.21 Über SHI

Es ist verboten, VirusZ II ohne meine Genehmigung auf irgendwelchen SHI Disketten zu verbreiten. Ich bin KEIN Mitglied von SHI und habe deshalb auch keinerlei Interesse, mit dieser Organisation oder ihrem Leiter Erik Løvendahl Sørensen in irgendeiner Art und Weise in Verbindung gebracht zu werden.

1.22 Über MagicWB

Die Piktogramme des VirusZ-Paketes sind für die Verwendung mit einer MagicWB Workbench konzipiert. MagicWB ist ein kompletter Ersatz für die relativ unschönen Piktogramme der Workbench. Falls Ihnen die Piktogramme gefallen, lassen Sie sich bitte beim Autor registrieren und Sie erhalten das komplette MagicWB-Paket.

MagicWB wurde von Martin Huttenloher erschaffen, das VirusZ-Piktogramm wurde von Timm S. Müller entworfen.

1.23 File Check

Einleitung

In den frühen Tagen der Amiga-Viren dachte wohl niemand an File- oder gar Linkviren. Ein guter Virenkiller mußte den Bootblock anzeigen und einige Vektoren überprüfen können. Aber heutzutage geht die größte Gefahr nicht mehr vom Bootblock, sondern von infizierten Dateien aus.
Deshalb wurde dieser einzigartige Datei-Prüfer entwickelt. Er bietet Ihnen einige Möglichkeiten, die Sie woanders vergebens suchen werden. Als erstes wäre zu erwähnen, daß es möglich ist, nahezu alle gepackten Dateien vor der Überprüfung zu entpacken. Zweitens können bei Mehrfachinfektionen von Dateien alle Viren in einem Durchgang entfernt werden.
Alles dies wurde erst möglich durch die Verwendung meiner Xfdmaster.library in Verbindung mit einer speziellen Pufferverwaltung. Wenn Sie sich für einen Datei-Prüfer entscheiden müssen, bleibt Ihnen also nur eine Wahl.

Eine absolute Weltneuheit in Sachen Linkviren-Kontrolle wurde zuletzt exklusiv für VirusZ verwirklicht: Es ist jetzt möglich, Linkviren auch dann zu erkennen, wenn sie nicht im ersten Hunk einer Datei enthalten sind, sondern in einem völlig beliebigen. Dadurch ist es möglich, auch solche Linkviren aufzuspüren, die von einigen vorwitzigen Zeitgenossen mittels angehängter Hunks o.ä. unkenntlich gemacht wurden.

VirusZ erkennt auch sogenannte 4EB9-Linker. Diese werden oft dazu verwandt, trojanische Pferde vor Intros oder Hilfsprogramme zu hängen. VirusZ ist in der Lage, derartige Dateien zu "zerlegen" und die Einzeldateien nach

Dateiviren und Trojanischen Pferden zu durchsuchen. Sollte dabei ein Virus entdeckt werden, kann jedoch nur die komplette Datei gelöscht werden.

ACHTUNG: Bitte verwenden Sie nach Möglichkeit immer die Entpack-Option, um auch wirklich alle Viren aufzuspüren. VirusZ erkennt alle Dateiviren NUR im ungepackten Zustand.

Datei Requester

Nachdem Sie den Menüpunkt 'File Check' aus dem 'Project' Menü gewählt haben, erscheint als erstes ein Datei-Requester. Hier können sie unter optionaler Verwendung von Mehrfachauswahl die Dateien und/oder Verzeichnisse markieren, die Sie überprüfen möchten.
Wenn Sie mehrere Einträge selektieren möchten, müssen Sie während der Auswahl mit der Maus eine der beiden <SHIFT> Tasten gedrückt halten. Mit dem 'All' Gadget können Sie alle Einträge auf einmal anwählen.
Drücken Sie nun auf das 'OK' Gadget, um die Überprüfung zu starten oder 'Cancel', um den Vorgang abzubrechen.

Ausgabefenster / Kontroll-Leiste

Jetzt öffnet sich ein zweigeteiltes Fenster. Den größeren Teil nimmt der Ausgabebereich ein, in dem Informationen zum Prüf-Vorgang ausgegeben werden. Der kleinere Teil ist der Kontrollbereich. Durch betätigen von 'Stop' wird der Ablauf unterbrochen und ein Requester dargestellt, mit dem man entweder mittels 'Continue' mit der Überprüfung fortfahren oder durch Auswahl von 'Abort' den Vorgang ganz abbrechen kann. Nach Beendigung eines Durchgangs kann man mit 'Exit' die gesamte Prüfschleife verlassen oder mit 'Check Again' wieder ganz am Anfang beginnen.

Wichtige Hinweise

Die Programmroutine zur Entfernung von Linkviren ist absolut zuverlässig, solange die infizierten Dateien nicht bereits vom Virus teilweise zerstört wurden. Wenn die Programmstruktur verändert ist oder ein anderes Problem auftritt, wird dies gemeldet und der Vorgang abgebrochen.
Die Schutzbits von zu überprüfenden Dateien werden wenn nötig automatisch auf den jeweiligen Vorgang angepaßt, d.h. zum Lesen wird das Lesebit gesetzt, zum Reparieren das Schreibbit etc. Falls das Betriebssystem einen Requester mit dem Hinweis darstellt, die gerade geprüfte Diskette sei schreibgeschützt, so deutet dies darauf hin, daß VirusZ soeben versucht hat, die Schutzbits zu verändern. Da dieser Vorgang völlig ungefährlich ist, ist es empfehlenswert, beim Überprüfen von Disketten den Schreibschutz von vornherein zu entfernen.

Noch ein Tip

Es kann manchmal vorkommen, daß eine Datei zuerst infiziert und darunter auch noch gepackt ist. Wenn Sie eine derartige Datei zwar desinfizieren, aber nicht entpacken möchten, sollten Sie sie mit ausgeschalteter Entpack-Option nochmals überprüfen.

1.24 File Check Preferences

Skip Subdirectories

Sie können diese Option einschalten, wenn Sie zwar selektierte Verzeichnisse prüfen möchten, nicht jedoch weitere darin enthaltene Schubladen.

Auto-Handle Viruses

Falls während des Prüfvorgangs eine verseuchte Datei entdeckt werden sollte, erscheint normalerweise ein Requester, der Ihnen die Möglichkeit bietet, den Virus zu entfernen oder aber nichts zu tun. Mit dieser Option können Sie diesen Requester umgehen und Viren automatisch entfernen lassen.

Check Without Repair

Diese Option verhindert, daß verseuchte Dateien repariert werden. Statt dessen wird einfach nur der Name des Virus ausgegeben und der Prüfvorgang fortgesetzt. Diese Möglichkeit eignet sich gut für einen ersten Überblick über eine neu erworbene Diskette.

Generate Report

Dieser Schalter bietet Ihnen die Möglichkeit, den Text, der während des Prüfvorgangs erzeugt wird, als Textdatei zu speichern. Dazu erscheint nach Beenden der Überprüfung ein Datei-Requester, in dem Sie den Pfad und Namen des zu speichernden Textes wählen können.

Auto-Save Report

Ist diese Option angewählt, erscheint kein Datei-Requester, um einen Pfad/Namen für einen zu speichernden Report auszuwählen. Es wird einfach der voreingestellte Pfad (Default Report Path) und ein von VirusZ erzeugter Name verwendet.

Emulate ExAll()

Normalerweise benutzt VirusZ die Kickstart-Routine ExAll(), um den Inhalt eines Verzeichnisses auszulesen. Dies funktioniert allerdings bei einigen Kickstarts nicht richtig. Sollte der Dateiprüfer also keine Dateien finden, schalten Sie diese Option ein und versuchen Sie es noch einmal. Sollten sich bei Ihrem Kickstart keinerlei Probleme ergeben, so lassen Sie diese Option aber bitte auf "aus", weil die Originalroutine schneller arbeitet als die Emulation.

Decrunch Executables

Wenn Sie diese Option einschalten, versucht VirusZ, gepackte ausführbare Dateien vor dem Überprüfen zu entpacken.
ACHTUNG: Diese Option sollte nur in Notfällen abgeschaltet werden. VirusZ erkennt alle eingebauten Viren nur im entpackten Zustand.

Decrunch Data Files

Wenn Sie diese Option einschalten, lädt VirusZ auch Datenfiles und versucht diese wenn nötig vor dem Überprüfen zu entpacken. Dies ist besonders nützlich für Datenfiles, die eigentlich ausführbare Dateien enthalten, wie z.B. XPK Dateien.

Skip Crypted Files

Diese Option ermöglicht, kodierte Dateien einfach zu überspringen. Das kann sinnvoll sein, wenn Sie die Dateien selbst kodiert haben und genau wissen, daß sie keinerlei Viren enthalten. Sie sparen sich dann das nervtötende Beantworten vieler Password-Requester.

Use External Slaves

Diese Option schaltet die Benutzung externer Slaves der xfdmaster.library ein. Dies ist zur Zeit wenig sinnvoll, da keine externen Slaves existieren, die ausführbare Programme entpacken können. Es ist vielmehr angeraten, diese Option auszuschalten, um Systemabstürze zu vermeiden, die von schlecht programmierten Slaves ausgelöst werden können.

Default Report Path

Hier können Sie den standardmäßigen Pfad für das Abspeichern von Reports eingeben. Dieser wird dann benutzt, wenn Sie das automatische Speichern von Reports gewählt haben.

Amount Of Lines Displayed

Dieses Gadget enthält die maximale Anzahl von Zeilen, die im Ausgabefenster dargestellt werden sollen. Es ist ratsam, diesen Wert bei hochauflösenden Bildschirmmodi nicht zu groß zu wählen, da sich die Darstellung sonst extrem verlangsamen kann.

1.25 Sector Check

Laufwerk wählen

Nachdem man den Menüpunkt 'Sector Check' aus dem 'Project' Menü gewählt hat, erscheint als erstes ein Laufwerks-Requester, mit dessen Hilfe man das zu überprüfende Laufwerk auswählt. Es werden nur Diskettenlaufwerke unterstützt, die über das Trackdisk.Device angesprochen werden können. Mit 'OK' wird der Prüfvorgang gestartet.

Ausgabefenster / Kontroll-Leiste

Jetzt öffnet sich ein zweigeteiltes Fenster. Den größeren Teil nimmt der Ausgabebereich ein, in dem Informationen zum Prüf-Vorgang ausgegeben werden. Der kleinere Teil ist der Kontrollbereich. Durch betätigen von 'Stop' wird der Ablauf unterbrochen und ein Requester dargestellt, mit dem man entweder mittels 'Continue' mit der Überprüfung fortfahren oder durch Auswahl von 'Abort' den Vorgang ganz abbrechen kann. Nach Beendigung eines Durchgangs kann man mit 'Exit' die gesamte Prüfschleife verlassen oder mit 'Check Again' wieder ganz am Anfang beginnen.

1.26 Sector Check Preferences

Auto-Repair Sectors

Wann immer ein infizierter Sektor entdeckt wird, erscheint ein Requester, der Ihnen die Möglichkeit bietet, den Sektor entweder zu reparieren oder nichts dergleichen zu tun. Wenn Sie diese Option einschalten, wird dieser Requester unterdrückt und der Sektor automatisch repariert.

Check Without Repair

Diese Option sollten Sie einschalten, wenn Sie sich nur einen Überblick über den Zustand einer Diskette verschaffen wollen, ohne irgendwelche Reparaturen vornehmen zu wollen.

Amount Of Lines Displayed

Dieses Gadget enthält die maximale Anzahl von Zeilen, die im Ausgabefenster dargestellt werden sollen. Es ist ratsam, diesen Wert bei hochauflösenden Bildschirmmodi nicht zu groß zu wählen, da sich die Darstellung sonst extrem verlangsamen kann.

1.27 Vector Check

Einleitung

Die meisten Viren arbeiten nach ein und demselben Prinzip. Entweder sind sie resident oder sie verbiegen Vektoren von Libraries oder Devices. Deshalb wurde der Vektoren-Prüfer entwickelt, der Ihnen helfen soll, neue Viren, die VirusZ noch nicht automatisch erkennt, zu finden.

Der Großteil der Informationen, die Ihnen im Ausgabefenster bereitgestellt werden, sind nur für Programmierer oder erfahrene Anwender aussagekräftig, deshalb werde ich versuchen, die Erklärungen auf das Nötigste zu beschränken, um den Durchschnittsanwender nicht unnötig zu verwirren.

VirusZ ist in der Lage, Ihnen anstatt der relativ nichtssagenden Offsetwerte auch den Funktionsnamen von Bibliothekseinsprüngen anzuzeigen. Dazu werden aber sogenannte FD Dateien benötigt. Diese finden Sie z.B. auf den Extras Disketten der Workbench 1.2/1.3 oder als Teil der meisten Assembler- und Compilerpakete. Ich darf Sie aus rechtlichen Gründen nicht mitliefern.

Ausgabefenster / Kontroll-Leiste

Nachdem man den Menüpunkt 'Vector Check' aus dem 'Project' Menü gewählt hat, erscheint ein zweigeteiltes Fenster. Der obere Teil beinhaltet den Ausgabebereich, in dem Informationen zu den einzelnen Vektoren ausgegeben werden. Mit dem Scrollbalken kann man sich im dargestellten Text frei bewegen. Der kleinere Teil ist der Kontrollbereich. Durch Drücken des 'Refresh' Gadgets werden die Vektoren erneut ausgelesen und der Text auf den neuesten Stand gebracht. Dies ist nützlich, nachdem z.B. einige Vektoren gelöscht wurden. Mittels 'Exit' verläßt man das Fenster. Will man während des Betrachtens der Vektoren einige Einstellungen verändern, kann man dies direkt mittels 'Prefs' tun. Die Anzeige wird automatisch erneuert, wenn man das Voreinstellungsfenster mittels 'Use' verläßt.

Haben die angezeigten Zeichenkolonnen auch eine tiefere Bedeutung?

Hinter jedem dargestellten Vektor erscheint ein Kommentar. Solange Sie dort 'Ok' lesen können, ist der Vektor in Ordnung. Es können auch verschiedene Namen von Programmen erscheinen, die bestimmte Vektoren verbiegen und von VirusZ erkannt werden, so z.B. 'SetPatch'.
Falls aber die Meldung '*** NON-STANDARD VECTOR ***' erscheint, sollten Sie sich zumindest einmal Gedanken darüber machen, ob Sie eventuell Programme im Hintergrund gestartet haben, die diese Änderungen hervorrufen könnten. Falls dies nicht der Fall ist, könnte es sich um einen neuen Virus handeln.

Menüs

Das Vektor-Fenster besitzt ein Menü namens 'Clear'. Es ermöglicht Ihnen, einzelne Reset-Vektoren zu löschen oder auch alle auf einmal.
Das 'Misc' Menü bietet derzeit nur eine Funktion: 'Save Report...'. Damit ist es möglich, den angezeigten Text als Ascii-Datei abzuspeichern.

1.28 Vector Check Preferences

Show ResModules

Es werden residente Module angezeigt, die nicht im ROM liegen.

Show Exec Interrupts

Die Interrupt-Tabelle von Exec wird dargestellt und kommentiert.

Show CPU Interrupts

Die Interrupt-Tabelle der CPU wird dargestellt und kommentiert.

Show Devices

Die Liste aller geladenen Devices wird auf Einsprünge überprüft, die nicht ins ROM zeigen.

Show Libraries

Die Liste aller geladenen Libraries wird auf Einsprünge überprüft, die nicht ins ROM zeigen.

Hide Known Patches

Normalerweise werden bekannte Veränderungen mit dem Namen des Verursachers angezeigt. Mit dieser Option kann diese Ausgabe unterdrückt werden. Dies kann nützlich sein, um sich überflüssige Informationen zu ersparen.

Hide 'OK' Vectors

Mit dieser Option können sie die Ausgabe aller Vektoren unterdrücken, die mit 'Ok' kommentiert würden. Dadurch kann man die Anzahl der auszugebenden Zeilen drastisch reduzieren und so eine übersichtlichere Anzeige erhalten.

Use FD For Offsets

```
------------------
```
Dieser Schalter bewirkt, daß VirusZ die Namen der Bibliotheksfunktionen aus sogenannten FD Dateien ausliest und damit die Standardmeldung 'Offset -xyz' ersetzt. Wenn eine Funktion nicht definiert ist (alte FD Datei oder reservierter Eintrag), wird die normale Offsetmeldung gezeigt.
Sie finden die FD Dateien auf der WorkBench 1.2/1.3 Extras Diskette oder in fast allen Assembler- und Compiler-Paketen. Ich darf sie aus rechtlichen Gründen nicht mitliefern.

```
FD Path
-------
```
Dieses Gadget enthält das Verzeichnis, in dem sich die FD Dateien befinden. Die Dateien dürfen auch gepackt sein, solange der benutzte Packer von der xfdmaster.library unterstützt wird (also praktisch alle:-).

```
Amount Of Lines Displayed
-------------------------
```
Dieses Gadget enthält die maximale Anzahl von Zeilen, die im Ausgabefenster dargestellt werden sollen.

1.29 Bootblock Lab

```
Achtung
-------
```
Seien Sie vorsichtig mit dem Beschreiben oder Installieren Ihrer Harddisk. Ich hafte in keinster Weise für Ihre Fehler.

```
Laufwerk / Anzeige
------------------
```
Es existieren zwei Cycle-Gadgets im Bootblock Lab, eines auf jeder Seite der Statuszeile. Mit dem linken wählen Sie das Laufwerk, mit dem Sie arbeiten möchten, mit dem rechten die Art der Darstellung des Bootblockinhaltes. Sie können die beiden Gadgets mittels <D> oder <SHIFT-D> (Laufwerke) und <B> oder <SHIFT-B> (Darstellung) auch über die Tastatur bedienen.

```
Name
----
```
Immer wenn ein Fehler auftritt, wird eine entsprechende Meldung in der Statuszeile ausgegeben. Dabei wird aber der Name des aktuellen Bootblocks überschrieben, der normalerweise als Status angezeigt wird. Dieses Gadget ermöglicht die wiederholte Ausgabe des Bootblocknamens.

```
Exit
----
```
Beendet diesen Programmteil.

```
Read
----
```
Liest den Bootblock der Diskette im aktuellen Laufwerk in den Puffer. Es kann nur von DOS-Disketten gelesen werden.

```
Write
-----
```
Schreibt den Pufferinhalt in den Bootblock der Disktte im aktuellen Laufwerk. Die Dateisystem-Kennung und die Checksumme des Bootblocks werden

automatisch angepaßt.

Load

Öffnet einen Datei-Requester, mit dem man eine Bootblock-Datei laden kann. Es werden nur DOS-Bootblöcke unterstützt.

Save

Speichert den Pufferinhalt in die per Requester gewählte Datei. Somit ist es möglich, von wichtigen Bootblöcken (z.B. von Spielen) Sicherheitskopien zu erstellen.

Learn

Zur Zeit nicht verfügbar.

Prefs

Es erscheint das Fenster mit den Voreinstellungen. Dies ist nützlich, um Änderungen vorzunehmen, ohne daß das Bootblock Lab verlassen werden muß.

Install

Installiert einen Original-OS 2.04-Bootblock auf die Diskette im aktuellen Laufwerk. Die Dateisystem-Kennung wird automatisch angepaßt.

Funktionen über Menü

Zur Zeit nicht verfügbar.

1.30 Bootblock Lab Preferences

Ask Before Write Access

Es erscheint bei jedem Aufruf von 'Write' oder 'Install' eine Sicherheits-abfrage.

Read Inserted Disks

Diese Option ermöglicht es, den Bootblock einer neu eingelegten Diskette automatisch einzulesen. Dies ist nützlich, wenn Sie viele Disketten überprüfen möchten, da Sie diese dann nur nacheinander in ein Laufwerk einlegen müssen.

Install Uninstalled Boot

Wenn Sie diese Option anwählen, wird beim Installieren einer Diskette kein Standard-OS 2.04-Bootblock geschrieben, sondern die Diskette nicht-bootbar gemacht.

1.31 Show Brains...

Alle derzeit von VirusZ erkannten Bootblock-, File- und Linkviren werden in einer Liste aufgeführt. Die zweite Liste enthält alle Patches, die beim Vektorenprüfen erkannt werden.

1.32 Background Preferences

Check On Startup / Keep Under Surveillance

Die Schalter unter dieser Überschrift haben folgendes gemeinsam: der erste Knopf schaltet den jeweiligen Test beim Neustart ein/aus, der zweite Knopf (de)aktiviert den Überwachungsmodus. Die Bedeutung der Schalter ist weiter unten erläutert.

Die Speicherüberwachung erkennt die gleichen Patches wie der eigentliche Vektor-Prüfer und informiert Sie deshalb nicht über Änderungen, die von solchen ausgelöst wurden. Falls der Info-Requester erscheint und mitteilt, daß sich Vektoren verändert haben, dann benutzen Sie bitte den Vector-Check, um sich die Veränderungen genauer anzusehen.

Falls die Diskettenüberwachung einen unbekannten Bootblock meldet, so können Sie diesen mittels Bootblock Lab genauer begutachten.

ColdCapture

Prüft auf Veränderungen des ColdCapture-Vektors.

CoolCapture

Prüft auf Veränderungen des CoolCapture-Vektors.

KickTagPtr

Berechnet eine Prüfsumme über alle KickTags und vergleicht diese nach jedem Prüflauf auf Abweichungen.

CPU Interrupts

Überwacht alle Zeiger der Hardware-Interrupts.

Exec Interrupts

Prüft alle Interrupteinträge in der ExecBase.

Libraries/Devices

Sucht nach unbekannten Patches.

Bootblocks

Untersucht den Bootblock jeder eingelegten Diskette.

Disk-Validators

Untersucht den Disk-Validator jeder eingelegten Diskette.

Known Viruses

Durchsucht den Speicher nach bekannten Viren.

Surveillance Frequency

Dieses Gadget enthält die Anzahl Sekunden, die zwischen zwei Speicher-Tests verstreichen sollen. Diese Frequenz wird sowohl für die System-Überwachung als auch für den Virentest verwendet.

1.33 About...

Zeigt Informationen über VirusZ an. In den untersten Zeilen finden Sie die Filelänge, die das Programm haben sollte und den Speicherverbrauch des laufenden Programms.

1.34 Miscellaneous Preferences

Check Hunks On Startup

Dieser Schalter aktiviert die Überprüfung der Programm-Struktur von VirusZ bei einem Neustart. Ein Alert wird dargestellt, falls irgendetwas nicht in Ordnung sein sollte (deutet auf einen Linkvirus hin). Sie sollten auf diese Option verzichten, wenn Sie vorhaben, VirusZ mit einem Datei-Packer zu packen, weil diese meist die Struktur eines Programmes verändern.

Requesters Follow Mouse

Option an:
Alle Requester erscheinen mit dem negativen Gadget unter dem Mauszeiger.
Option aus:
Die Requester werden in der linken oberen Ecke dargestellt.

Quit Immediately

Option an:
VirusZ kann ohne zusätzliche Bestätigungen verlassen werden.

Install SnoopDos Task

Option an:
Ein Task namens 'SnoopDos', der keinerlei Prozessorzeit in Anspruch nimmt, wird erzeugt. Dieser verhindert, daß sich bestimmte trojanische Pferde ins System einbinden.

Pop Up On Startup

Option an:
VirusZ verhält sich beim Neustart ganz normal und öffnet sein Fenster.
Option aus:
VirusZ arbeitet im Hintergrund und kann nur über den definierten Hotkey und

das Programm Exchange kontrolliert werden.

Load Brain On Startup

Zur Zeit nicht verfügbar.

Close Main Window = Exit

Option an:
Bei Betätigung des Schließsymbols wird VirusZ beendet.
Option aus:
Das Schließsymbol bewirkt das gleiche wie der Menüpunkt Hide.

Center Main Window

Option an:
Das Fenster von VirusZ erscheint mittenzentriert am oberen Rand des Screens.
Option aus:
Das Fenster wird mit den zuletzt gespeicherten Koordinaten geöffnet. Man kann diese abspeichern, indem man das Fenster an die gewünschte Position zieht und dann den Menüpunkt 'Save Prefs' anwählt.

Activate On Startup

Mit dieser Option veranlassen Sie, daß das VirusZ-Hauptfenster beim Neustart sofort aktiviert wird. Sie sparen sich dadurch das Anklicken des Fensters, wenn Sie sowieso gleich ein Menüfunktion starten möchten.

Hotkey

Der voreingestellte Hotkey für das Öffnen des Hauptfensters.

Brain

Zur Zeit nicht verfügbar.

Devices

Hier können Sie alle Devices eintragen, die von VirusZ bei der Laufwerksüberprüfung herangezogen werden sollen. Sie werden im BootLab in der selben Reihenfolge erscheinen wie sie im Gadget eingegeben wurden. Sie können auch Devices eintragen, die Sie nicht ständig gemountet haben. Diese werden dann nur berücksichtigt, wenn sie auch wirklich vorhanden sind. Alle Namen müssen durch ein "|"-Zeichen getrennt sein.

1.35 Hide

Veranlaßt VirusZ, sein Fenster zu schließen und nur noch im Hintergrund weiterzuarbeiten. Sie können das Fenster wieder öffnen, indem sie den definierten Hotkey drücken oder mittels des Programmes Exchange den Befehl dazu geben.

1.36 Save Prefs

Speichert alle Voreinstellungen in die Datei 'ENVARC:VirusZ_II.prefs'. Diese Datei wird bei jedem Neustart zuerst gesucht und die darin enthaltenen Informationen gegebenenfalls übernommen.

1.37 Quit

Beendet VirusZ. Es werden alle belegten System-Resourcen zurückgegeben.