VirusWorkshop

Markus Schmall

COLLABORATORS			
	TITLE : VirusWorkshop		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Markus Schmall	March 2, 2022	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

VirusWorkshop

1.1 VirusWorkshop 6.7 - 29.09.1997 (C) by Flake/TRSi`97

```
                                        VirusWorkshop 6.7

                    A Tristar & Red Sector inc. production
                                 in 1997 !
                           coded by Markus Schmall



            ~~~~~Deutsche~Beschreibung~der~Funktionen~~~~~~

            ~~~~~English~description~of~the~functions~~~~~~
                  This programm was made possible based on the work of many  ↩
                     people,
      who send me bugreports, infected files, money, talked to me and
      gave me new motivation to continue the work on this. I want to
      thank you ALL. I cannot mention all your names here, but I think
      on you.

      This viruskiller is dedicated to Mr.Ingo Schmidt, without whose help
      VirusWorkshop would be today not one of the leading viruskillers on
      AMIGA. He always helped me to code tricky stuff and tested VW on the
      "hard" way.

      Special thanks to all the TRSilers, which helped me a lot and spread
      VirusWorkshop so fantastic.
```

1.2 Deutsche Anleitung

```
            ~~~~~~Wichtig~!~Lesen~Sie~diesen~Absatz~!~~~~~~

            ~~~~~~~~~~~~~~~~~~Einfuehrung~~~~~~~~~~~~~~~~~

            ~~~~~~~~~~~~~~~~~~Kopierrecht~~~~~~~~~~~~~~~~~
```

Die folgenden Texte sind leider derzeit nur in englischer Sprache verfügbar:

1.3 English-Documentation

It's not allowed to include VirusWorkshop/Dhunk/ ↩
documentations of
VirusWorkshop on any release by Safe Hex International. I am NOT a member of SHI (any more) and therefore I am not interested in any direct or indirect contact to Mr.Erik Loevendahl Soerensen, the leader of this organisation.

The VirusWorkshop is not allowed to be spreaded from the SHI main center in denmark.

1.4 PGP-Deutsche Anleitung

```
  PGP Unterstützung ab VirusWorkshop 4.4:
  ---------------------------------------

  Ich war die nervenden Anfragen und VOR ALLEN DINGEN die teilweise
  unqualifizierten Kommentare im Z-Netz/Rechner/Amiga/Viren leid und
  so habe ich mich dann doch noch dazu entschlossen, eine PGP
  Unterstützung für VirusWorkshop etc. anzubieten. Speichern Sie bitte
  mit einem Texteditor nur den PGP PUBLIC KEY BLOCK unter einem
  gesonderten Filenamen auf einen Datenträger und tippen sie
  folgenden String aus einer SHELL/CLI ein:

  PGP <Dateiname> und folgen Sie den Anweisungen von PGP !

  Um die Echtheit zu untersuchen, müssen Sie jetzt nur noch folgenden
  Text eingeben:

  als Beispiel für das VirusWorkshop Hauptprogramm:

  PGP VirusWorkshop.sig VirusWorkshop



-----BEGIN PGP PUBLIC KEY BLOCK----- Version: 2.6

mQCNAi6+nugAAAEEAOCPqXrZ0sDnn1nLfz/Q5y5fOhVqA69oEJF8W+crSdb/Ktce
+XBC7sQevqWLG0JKk4H8i03JjI5IQluUK/N2SQG+YQA0jzeenvhEtJvuz/LKxyXk
/JuKsPaYOfZen2HdtREl9qI7GnLI0mZSJcAn7QKmVmBPX9lSUyD1uhB1y2lFAAUR
tCVNYXJrdXMgU2NobWFsbCA8TS5TY2htYWxsQExEQi5oYW4uZGU+iQCVAgUQLtU/
u2IQqxPzqeIlAQEGlwP/QYNULLr6ONlqrqmwHAYa2cyhMph2bq5aT041Zh69/GOI
v+LCZft5pFCVCzVZxZd2GKuwmMi/0NSy19YUaE+Kcr3Ep3Xx/6Spgu4KVa8JVzTu
ymOlm6cGJs76Nzef9Sc3Np/5CjFs9QtlpPWu0jH/3bOaTu+l8hQ2t9zo2HZAqT0= =lqUF
-----END PGP PUBLIC KEY BLOCK-----

  Verwendete PGP Version: PGP 2.6ui zu finden im AMinet unter
  "Util/Crypt/PGPAmi26ui.lha".

  Ich verwende einen 1024 Bit Key, welcher wirklich genug
  Sicherheit bieten sollte. Daher kann es zu einigen
  Rechenpausen auf langsamen Rechnern kommen.
```

```
  Mein Unterschriftsname ist M.Schmall <M.Schmall@LDB.han.de> !
```

1.5 PGP-English documentation

```
  PGP support starting with VirusWorkshop 4.4:
  --------------------------------------------

  I was fucked up with all the nerving/stressing comments etc. and
  especially with several unqualificated comments in the german
  Z-Netz/Rechner/Amiga/Viren. So I decided to support PGP just to
  make me a more happier life without all the stressing stuff.

  Please save this textblock with an editor to a seperate file and
  type from SHELL/CLI:

  PGP <filename> and follow the instructions !

  To proove the programms, you have to enter the following texts:

  as example for the VirusWorkshop mainprogramm:

  PGP VirusWorkshop.sig VirusWorkshop


-----BEGIN PGP PUBLIC KEY BLOCK----- Version: 2.6

mQCNAi6+nugAAAEEAOCPqXrZ0sDnn1nLfz/Q5y5fOhVqA69oEJF8W+crSdb/Ktce
+XBC7sQevqWLG0JKk4H8i03JjI5IQluUK/N2SQG+YQA0jzeenvhEtJvuz/LKxyXk
/JuKsPaYOfZen2HdtREl9qI7GnLI0mZSJcAn7QKmVmBPX9lSUyD1uhB1y2lFAAUR
tCVNYXJrdXMgU2NobWFsbCA8TS5TY2htYWxsQExEQi5oYW4uZGU+iQCVAgUQLtU/
u2IQqxPzqeIlAQEGlwP/QYNULLr6ONlqrqmwHAYa2cyhMph2bq5aT041Zh69/GOI
v+LCZft5pFCVCzVZxZd2GKuwmMi/0NSy19YUaE+Kcr3Ep3Xx/6Spgu4KVa8JVzTu
ymOlm6cGJs76Nzef9Sc3Np/5CjFs9QtlpPWu0jH/3bOaTu+l8hQ2t9zo2HZAqT0=
=lqUF
-----END PGP PUBLIC KEY BLOCK-----



  Used PGP Version: PGP 2.6ui , which can be found in the AMinet:
  "Util/Crypt/PGPAmi26ui.lha".

  To ensure maximum security, I use a 1024 bit key for the PGP
  routines. This should be enough ! The problem is the high
  calculating process, which can last on slow systems a bit.
  Sorry for this, but I wanted to be sure !

  My signature name is Markus Schmall <M.Schmall@LDB.han.de>.
```

1.6 SHI_Prohibition

```
                    Es ist strengstens verboten, Teile des VirusWorkshop  Paketes   ↩
                       in  Safe
```

Hex Publikationen zu verwenden. Ich bin kein Mitglied von S.H.I. und möchte in keiner Weise in Kontakt mit Herrn Erik Loevendahl Soerensen, dem dänischen SHI Leiter, gebracht werden. Es hat Vorfälle gegeben, die mich zu diesem Verhalten gezwungen haben.

Es ist strengstens verboten, daß VirusWorkshop auf Disketten des SHI Hauptcenters vertrieben wird.

Es gibt leider immer noch Firmen, die VirusWorkshop im Set mit anderen Viruskillern fuer 29 DM verkaufen. Dies ist einfach Wucher ! Diese Firmen halten sich trotz des Verbotes (siehe VirusWorkshop.News) nicht an die preislichen Vorgaben.

-> Hiermit gilt ein strengestes Verbot für Mallander Computersoftware, VirusWorkshop zu vertreiben. Im August 1994 fand ich auf einer Viruskillerpackdiskette von dieser Firma VirusWorkshop in der Version 2.2 <-

WEITERHIN IST ES STRENGSTENS VERBOTEN, DASS DAS COMPUTER CENTER BOCHOLT UND UNIVERSUM SOFTWARE VIRUSWORKSHOP VERKAUFEN ! DIESE FIRMEN SIND MEINER MEINUNG NACH WEITERE NAMEN FUER MALLANDER SOFTWARE UND FORDERN AEHNLICHE PREISE !

Ein~Beispiel~für~das~Viruskillerpack~perfect~von~Mallander~ ↩
Software

1.7 Einige lernen es nie...

Hannover, August 1994

Markus Schmall
von Graevemeyerweg 25
30539 Hannover
Tel.:0511/514944

! Bitte nur 01772829402 anrufen !

Wieder einmal ein trauriger Anlass:

Das Viruskiller Pack perfekt von Mallander Computer Software in Bocholt. Dieses Pack wird in diversen Anzeigen für 29 DM angeboten und verspricht, die aktuellsten Viruskiller und diverse zusätzliche Informationen zu enthalten.

Am 01.08.1994. bestellten wir zu Testzwecken ein solches Pack. Am 08.08.1994. erhielten wir eine Nachnahmesendung für 42 DM von Mallander Software. Wir waren erschreckt, wie alt die Programme waren, die auf den beiden gelieferten Disketten zu finden waren.

Der Preis ist eine glatte Unverschämtheit ! Im VirusWorkshop Guidefile ist zu lesen, daß der Verkaufspreis für VirusWorkshop einschließlich

Porto/Verpackung und der Diskette nicht höher sein darf als 7 US Dollar. Mallander Computersoftware verstößt damit eindeutig gegen ein Verbot.

Es wird aber noch schöner: In dem File "VT-Liesmich", welches "vergessen" wurde auf die Diskette zu legen, ist zu lesen, dass VT nur komplett weitergegeben werden darf. Es fehlen aber sowohl die eigentliche Haupt-anleitung als auch diverse andere Texte, die dem kompletten VT-Archiv beiliegen. Wieder ein Verstoss gegen ein Verbot. Auch Herr Schneegold, der Programmierer, von VT hat eine preisliche Vorgabe, die in dreister Weise von Mallander Computersoftware übergangen wird.

Im BootX 4.50 Guidefile ist zu lesen, dass nicht mehr als eine kleine (nominal fee) Kopiergebühr für eine Kopie von BootX verlangt werden darf. Wir sehen, dass Mallander Computer Software sich nicht sehr an Richtlinien und Vorgaben/Verbote zu halten scheint.

Von Aktualität scheint der Laden in Bezug auf diese Viruskillerdisketten auch nicht viel zu halten. VT 2.54 wurde am 20.06.1993 veröffentlicht. VirusWorkshop 2.2 wurde am 10.7.1993. veröffentlicht. Die Programme sind über 1 Jahr alt und stellen keinen sicheren Schutz mehr dar.

Nur zur Erinnerung: Anfang August 1994 sind folgende Programmversionen aktuell:

-VT 2.66
-Virus Checker 6.42 mit Brain 1.04
-BootX 5.23a mit Recog 2.18
-VirusWorkshop 3.9

In einem Intro auf den Disketten ist folgenden Text zu lesen (nur wichtige Passagen):

```
'LIEBE COMPUTERFREUNDE, SIE ERLEBEN JETZT'
' EINE NEUE DISKETTE MIT SPITZEN PD-SOFTW'
'ARE ZUSAMMENGESTELLT IM HAUSE MALLANDER '
'COMPUTERSOFTWARE.       WIE UNTERSUCHUNG'
'EN ERGEBEN HABEN, FINDET MAN DIE SOFTWAR'
'E, DIE DIE FIRMA MALLANDER COMPUTERSOFTW'
'ARE ANBIETET, TEILWEISE ERST EIN HALBES '
'JAHR SPAETER IN IRGENDWELCHEN PD-SERIEN '
'WIEDER.      WIE KOMMT DAS ???          '
'    NUN, DIE FIRMA MALLANDER COMPUTERSOF'
'TWARE BEKOMMT DIE SOFTWARE IMMER BRANDNE'
'U DIREKT VON DEN PROGRAMMIERERN ODER VON'
' INTERNATIONALEN COPY-PARTYS. WIR ERHALT'
'EN STAENDIG WELTWEIT VON UEBER 200 PERSO'
'NEN DIE NEUESTEN SOFTWAREPRODUKTIONEN.  '
'  WIR ORIENTIEREN UNS NICHT AM NORMALEN '
'PD-MARKT ODER AN PD-SERIEN.          BEI'
'UNS WERDEN SIE DIE BESTEN UND NEUESTEN  '
' SPIELE, ANWENDERPROGRAMME, DEMOS,GRAFIK'
', MUSIK, TOOLS UND AUCH EROTIKSOFTWARE '
'FINDEN !!!                              '
```

Die Aussagen sind in weiten Teilen einfach lächerlich. Wenn von der doch so großartigen Aktualität gesprochen wird, warum haben dann diverse PD Serien (z.B. TIME) weitaus aktuellere Versionen von Viruskiller als dieser tolle Laden ? Komisch, oder nicht ?

Mallander Computer Software übertreibt also ein einigen Punkten, verstößt einige Male gegen strikte Verbote und verlangt für diese 2 Disketten einen absolut überzogenen Preis.

Ich würde mich freuen, wenn dieser Text auch an die großen AMIGA Magazine in Deutschland gelangen würde. Im Z-NETZ/RECHNER/AMIGA/VIREN liest auf jeden Fall S.Paolini von der AMIGA PLUS mit und diverse andere Redakteure von AMIGA und AMIGA Special dürften auch Netzzugriff haben.

Mit freundlichen Grüßen

Markus Schmall
(Programmierer von VirusWorkshop)

Inhalt von Diskette 1:

-Jeweils eine Kurzanleitung (2-5 KB) zu VT 2.54, VirusChecker 6.26, BootX 4.50 und dem Schwarzkopfkiller.
-VT 2.54 samt der Utilities (aber ohne die eigentliche Anleitung und ohne die begleitenden Texte)
-Virus Checker (Hauptprogramm)
-Schwarzkopfkiller (Hauptprogramm)
-BootX mit einigen Zusatzdateien und dem Recogfile 1.63

Inhalt von Diskette 2:

-VirusWorkshop 2.2 mit Zusatzdateien und Kurzanleitung

-eine Datei mit dem Namen VirusInfo. Diese Datei stellt sich als uralte VT-Kennt Datei heraus, wo am Anfang Texte geändert worden sind.

Dies sollen wohl die 200 Seiten umfangreiche Virusinformationen sein, die groß in der Werbung angepriesen werden...

Kommentar 11.10.1994: Ich habe wieder eine Anzeige dieser Firma gesehen,

wo VirusWorkshop jetzt mit 500 erkannten Viren genannt wird. Dies kann nur eine Version der letzten Monate sein und diese Versionen sind mit einem ausdruecklichen Verkaufsverbot für Mallander Software belegt.

1.8 Shareware Aufforderung

VirusWorkshop ab jetzt (24.02.1994) ShareWare:

Der vorgeschlagene Betrag ist 15 DM oder 10 USDollar. Wenn Sie VirusWorkshop regelmäßig benutzen und das Programm mögen, dann würde ich mich über diese kleine Anerkennung sehr freuen.

VirusWorkshop ist voll funktionsfähig. Sie werden bei der Virenjagd nicht durch Nervrequester, Keyfiles oder ähnliche Verfahren beeinträchtigt, da ich dies bei einem Viruskiller für nicht angemessen halte.

VirusWorkshop ist ein Produkt, welches in einem Zeitraum von über 2 Jahren entwickelt wurde und in welches sicher mehr als 500 Stunden Arbeit investiert bisher wurde. Die Entwicklung des Programmes ist ja auch noch nicht abgeschlossen....Die Weiterentwicklung eines Viruskillers kann ja nicht abgeschlossen sein.....

Ich bin Student und programmiere VirusWorkshop als mein Hobby. Mir macht diese Arbeit Spass, aber indirekt verursacht dieses Projekt immense Kosten:

- jeden Monat muß VirusWorkshop verteilt werden (sowohl über DFÜ als auch per Post)
- neue Viren/Libraries/Patches etc. müssen von Mailboxen gezogen werden
- Erfahrungsaustausch mit Freunden innerhalb von Deutschland per Telefon verschlingt auch eine nicht zu vernachlässigende Summe.

Wenn Sie mir den Betrag senden, erhalten Sie von mir die nächste Version von VirusWorkshop am Veröffentlichungstag direkt per Post.

Wenn Sie schon für eine ältere Version von VirusWorkshop eine ShareWare Gebühr bezahlt, müssen Sie natürlich nicht immer wieder diese Gebühr bezahlen.

Wenn Sie die aktuellste Version von VirusWorkshop direkt von mir haben wollen, dann senden Sie einen frankierten Rückumschlag und eine Diskette an mich. Wenn das Rückporto nicht ausreichend ist, behalte ich es mir vor, diese Anfrage nicht zu beantworten bzw. die Sendung einfach mit zuwenig Porto der Post zu geben, denn ich sehe es nicht ein, daß ich die Portogebühren für Sie bezahle.

Denken Sie darüber nach !

Meine Adresse: Skandinavische Registrationsadresse

Markus Schmall
von Graevemeyerweg 25
30539 Hannover

Lars P. Kristensen
Safirvej 25
3650 Olestykke
Denmark

Phone: +4542175233

1.9 Shareware wanted !

VirusWorkshop is from now (24.02.1994) on ShareWare:

The suggested donation is 15 DM or 10$. If you like VirusWorkshop and use it regulary I would be very happy, if you send the suggested donation to me.

I don't like ShareWare programms, which need a keyfile to run correct. Atleast for a viruskiller this is not the real way to go. You get here a full working version without any limitations.

VirusWorkshop is a product, which was produced in many hours. I do not know how many hours, but I invested for sure more than 500 hours to produce it. And the development progress is still running...

I am a student and to code VirusWorkshop is my hobby. The work on VirusWorkshop makes me happy, but the costs to produce this viruskiller are very high:

- the viruskiller has to be spreaded every month.
- new viruses etc. have to be downloaded from mailboxes (mainly in nonlocal boxes).
- technical knowledge exchange by phone with friends in other sides of Germany is very high.

If you send me the donation, you will get the next version from VirusWorkshop direct from me at the releaseday by mail.

If you have already paid the Share for an older version of VW, then you need not to pay this share for a new version(but i will not stop you to do this).

If you want to get the latest version of VirusWorkshop, then please send me an envelope with stamps and a disc. If you cannot get in touch with german stamps, then send me 3 DM=2US$! I am not able to pay all the porto for you. If a letter with too low stamps arrives at my home, I will not answer or I will send it to you and you have to pay the porto !

So, please think about it !

My adress:

```
Markus Schmall
von Graevemeyerweg 25
30539 Hannover



ATTENTION !


If you leave in a scandinavian country, then you can use this
adress, too:

Lars P. Kristensen (Member of Virus Help Denmark)
Safirvej 25
Dk-3650 Oelstykke
+45 42175233
Denmark

The registration money is in dansk currency 60 krones.
```

1.10 Preferences

```
                                VirusWorkshop Preferences Menu
                        ------------------------------



        ~~~~~~~AutoRamKill~~~~~~~~

        ~AutoSpeicherKill!~

        ~~~The~Explode~Function~~~

        ~~Imploder~Funkt.~~

        ~~~The~FileID~Function~~~~

        ~~~~~~~~~New~Preferencesfilestructure~~~~~~~~~

        ~~~~~~~~~~~~~Back~to~the~mainmenu~~~~~~~~~~~~~
```

1.11 NewPref

```
                Structure of the new preferencesfile:
-------------------------------------

1.Longword: for the screenresolution.
2.Longword
          1.Byte: If "1" then the AUTOKILL function is
                  activated.
          2.Byte: If "1" then the FILEID funtion is activated.
          3.Byte: If "1" then the decrunch function is
```

```
                activated.
          4.Byte: If "1" then you will be asked at the exit, if
                  you really want to do this.

3.Longword: Just for selfidentification.
4.Longword: Width of the screen.
5.Longword: Height of the screen.
6.Longword: Just for selfidentification.

All this functions will be first activated AFTER the  RAMcheck.



Struktur des neuen Einstellungsfiles:
-------------------------------------

1.Langwort: verantwortlich fuer die Auflösung.
2.Langwort
          1.Byte: Wenn dieses Byte auf "1" steht, wird die
                  AUTOKILL Funktion aktiviert.
          2.Byte: Wenn dieses Byte auf "1" steht, wird die

        FILEID
         Funktion aktiviert.
          3.Byte: Wenn dieses Byte auf "1" steht, wird die
                  Decrunch Funktion aktiviert.
          4.Byte: Wenn dieses Byte auf "1" steht, werden Sie
                  bei verlassen von VirusWorkshop gefragt, ob
                  sie dies wirklich tun wollen.

3.Langwort: Nur zur Selbsterkennung
4.Langwort: Breite des Screens
5.Langwort: Höhe des Screens
6.Langwort: Nur zur Selbsterkennung



Diese Funktionen werden erst nach dem ersten RAMcheck aktiviert.
```

1.12 FILEID2

```
Wenn Sie diese Funktion aktivieren wird VirusWorkshop  die  FileID
Library verwenden,um den Filetyp zu erkennen.Diese Library erkennt
über 520 verschiedene Filetypen. Achtung:Der Speicherbedarf  nimmt
zu und die Geschwindigkeit beim Testen nimmt ab.

      Die FileID Library wurde von  Bloodrock/SDC programmiert.
             Das VirusWorkshop Archiv enthält V6.1 dieser
                              Library.
```

1.13 FILEID

If you start this option,VirusWorkshop will use the FileID.Lib to recognizes over 520 different fileformats. The recognition results can be sometimes wrong but recognition rate is very high. Please note that this function slows down the testprocess a little bit and the memoryusage is higher.

The FileID Library was written by Bloodrock/SDC.
(Version 6.1 is included in this archive.)

1.14 INTRO

Introduction to VirusWorkshop:

Welcome to another new viruskiller on the AMIGA(C). This virus-killer was programmed to help you to get rid of all the viruses hanging around. VirusWorkshop handles a big number of trojan horses, which try change the AmiExpress(C) mailbox programm and it is ideal for users, who just want to check their software in a very secure way for viruses and diskerrors.

VirusWorkshop is another try to make a viruskiller for a special usergroup.I think it is good to support Kickstart 1.x but the new features should be supported.VirusWorkshop needs at least 1 MB of memory to work properly.

Some of the functions (especially DECRUNCHING) take a lot of time, but the time goes on and higher processors than the MC68000 can be found at every corner. The decrunch process needs a lot of memory. VirusWorkshop uses for decrunching the mighty XFDmaster Library by Georg Hoermann(*).

Support OS2.XX higher version and let the AMIGA get the rank in the computerbusiness, which it deserves because of it‘s powerfull chips and the really good operating system.

The author allows the spreading of VirusWorkshop in any form. But don‘t take more than 4 US$ or 6 DM for a viruskillerdisk, which contains VirusWorkshop. VirusWorkshop is thought for the masses and not for a special group with a high money-capacities.

This especially counts for a big german shop, which sells a packet containing several viruskillers for more than 18 $. This is not allowed.

It‘s not allowed to spread VirusWorkshop on S.H.I. discs.

(*) Some words about the Xfdmaster Library: This library is very well coded but contains some"bugs"concerning powerpacked files. In other words: It can come to problems with powerpacked files.I

cannot test, if this is based on bugs in PP or in the library,
but the programms itself work on my AMIGA.

1.15 Einführung

Vorwort zu VirusWorkshop

Herzlich willkommen zu einem neuen Viruskiller auf dem AMIGA.Dieser Viruskiller wurde programmiert,um Ihnen zu helfen,die Virenprobleme entgültig zu vergessen. VirusWorkshop erkennt eine große Anzahl an trojanischen Pferden,die speziell auf das AmiExpress Mailboxsystem ausgerichtet sind. VirusWorkshop is ideal für User,die auf einfache Weise Ihr System auf eine sehr sichere Methode untersuchen wollen.

VirusWorkshop ist ein weiterer Versuch,einen Viruskiller für eine spezielle Usergruppe zu erstellen. Die Idee,Kickstart 1.x zu unterstützen ist generell nicht schlecht, aber OS 2.xx ist eindeutig der Stand der Dinge. VirusWorkshop braucht mindestens 1 Megabyte Speicher um zu arbeiten.

Einige der Funktionen (insbesondere das Entpacken) benötigen sehr viel Zeit und Speicher,aber die Zeit schreitet voran und schnellere Prozessoren als der MC68000 können an jeder Ecke zu angemessenen Preisen erworben werden.

Unterstützen Sie OS2.xx und neuere Version und gewährleisten Sie damit, daß der AMIGA den Rang bekommt, der ihm aufgrund seiner leistungsfähigen Chips zusteht.

Die Verbreitung von VirusWorkshop wird ausdrücklich befürwortet.

Ausnahmen:

1. KEINE Verbreitung auf S.H.I. Disketten...

   Ich habe keinerlei Interesse in Verbindung mit Erik Loevendahl Soerensen oder S.H.I. gebracht zu werden.

2. VirusWorkshop darf nicht auf Disketten verkauft werden, die mehr als 6 DM kosten (4us$). VirusWorkshop soll kein elitäres Project darstellen, was nur von Leuten mit großem Computerbudget bezahlt werden kann.

Dies gilt natürlich auch für Kaufhausketten und andere Anbieter. Es gibt ein erschreckendes Beispiel in Deutschland, wo ein Packet mit Viruskillern für 29 DM verkauft wird. Es ist schon dreist einen solchen Preis zu verlangen! Mall..... heißt dieser nette Laden, der solche Wucherpreise nimmt.

1.16 COPYRIGHT

Copyright:

This programm was developed to help people to get rid of problems with viruses. The author takes no responsibility if damage is caused by the use of this programm.

All parts of the programm are copyrighted by Markus Schmall.

Except:
- "XfDmaster.library", which is copyrighted by Georg Hoermann (VirusZ).
- "reqtools.library", which is copyrighted by Nico François (PowerPacker).
- "FileID.library", which is copyrighted by Bloodrock/TRSi.

Comment 13.03.1994: VirusWorkshop now uses intern the decrunch-routines from the great CrunchMania packer. CrunchMania is share-ware and was written by Thomas Schwarz.

All coders gave permission to include their libraries in every non commercial and free distributable production. If you want to sell this programm the final price for the customer should not be higher than $6 US dollars (this includes the costs for media and postage!).

VirusWorkshop has to be spreaded with ALL the files and without modification. If you get a vw archiv, which does not contain ALL files, then change your software supplier. I REALLY HATE IT, IF someone changes my docs (as happended on a AMIGA VIRUS BUSTERS disk. I don't know, who changed the docs, but I don't like that !).

It's not allowed to spread VirusWorkshop on S.H.I. diskettes.

There are no exceptions: Jan Bo Andersen and Lars Kristensen left SHI and so the prohibition is global and stay valid ! Good luck in the future, Jan !

1.17 Kopierrecht

Dieses Programm wurde entwickelt um Usern zu helfen, die lästigen Viren zu vernichten. Der Autor übernimmt keine Verantwortung für Schäden, die durch die Benutzung dieses Programmes entstehen.

Auf alle Programmteile hat Markus Schmall das Copyright.

Außer auf:

- "XfDmaster.library", für welche Georg Hoermann das Copyright besitzt.
- "reqtools.library", für welche Nico Francois das Copyright besitzt.
- "FileID.library", für welche Bloodrock/SDC das Copyright besitzt.

Alle Programmierer haben die Erlaubniss gegeben, ihre Libraries in jeder nicht kommerziellen und frei kopierbaren Produktion zu verwenden. Wenn Sie VirusWorkshop verkaufen wollen, dann stelle ich folgende Bedingung:

Der Endpreis,welcher Porto,Verpackung etc.enthält, darf nicht höher als 6 US Dollar sein.

Bitte beachten Sie, daß VirusWorkshop NICHT auf SHI Disketten verteilt werden darf. Es gibt ab VirusWorkshop 4.4 keinerlei Ausnahmen mehr, da Jan Andersen und Lars Kristensen SHI verlassen haben und ich jetzt keinerlei Ausnahmen für die Beiden (natürlich auch für Jan Nielsen) machen muß.

Das Verbot gilt global und zeitlich unbegrenzt !

Weiterhin ist es nicht erlaubt, daß Virus-
Workshop in dem internen SHI E-Mail Netz verteilt wird.

VirusWorkshop darf nur als komplettes Archiv weitergegeben werden. Wenn Sie VirusWorkshop nur zerstückelt auf einer Diskette finden, sollten Sie Ihren Softwarehandler etc. schnellstens wechseln !

Es ist hiermit strengstens der Firma Mallander untersagt, VW zu verkaufen. Ich behalte mir rechtliche Schritte bei Nichteinhaltung vor. Dieses Verbot gilt auch für das Computer Center Bocholt und Universum Software.

Zusatz 13.03.1994: Intern werden jetzt die Entpackroutinen des CrunchMania Packers verwendet. CrunchMania is Shareware und wurde von Thomas Schwarz geschrieben.

1.18 RELEASENOTE

Release notes:

This programm should work on:

1.All AMIGA computers with the following KICKSTART versions:

(VirusWorkshop expects unpatched versions, which are not patched by Decigel etc.)

```
-Kickstart V2.04  (V37.175 on A3000/A2000/A500(+))
-Kickstart V2.05  (V37.300)
-Kickstart V2.06  (V37.350)
-Kickstart V3.00  (V39.106)
-Kickstart V3.00a (V39.106b in the A1200)
-Kickstart V3.02  (V39.116BETA for the A4000) *
-Kickstart V3.03  (V40.9BETA for the A4000)   *
-Kickstart V3.04  (V40.38BETA for the A4000)  *
-Kickstart V3.1ß  (V40.55 for the A4000) *
-Kickstart V3.1ß  (V40.55 for the A3000) *
-Kickstart V3.1ß  (V40.62 for the A4000)
-Kickstart V3.1ß  (V40.62 for the A3000)
-Kickstart V3.1ß  (V40.68 for the A4000)
-Kickstart V3.1ß  (V40.68 for the A3000)
-Kickstart V3.1   (V40.70 for the A4000(t))
-Kickstart V3.1   (V40.70 for the A3000)
-Kickstart V3.1   (V40.63 for the A2000/A500(+))
-Kickstart V3.1   (V40.68 for the A1200)
-Kickstart V3.1   (V40.63 for the A600)
```

At the moment Kickstart 40.65 will be not supported. This is based on the problem, that I can't make this version work on my A4000. Hope to fix it as soon as possible (as soon as I see the first SX1 ...).

2. Amigas with MMUs, FPUs.
3. Amigas with 680xx prozessors (even on the MC68040).
4. All chipsets including the new AGA system.
5. Amigas with about 8 KB stack for larger directories

The support from VirusWorkshop for new Kickstart versions was only possible, because of the great help of some developers. I have several times asked a special person from Commodore Germany for suppport (or just to work 5 minutes on an A4000t), but he always said no.

Caution: The Kickstart 40.70 for the A4000 is not the same as in the A4000t !

We tested the programm with nearly all Workbench versions (including the new version 40.42) and SetPatch commands and all worked just fine.

The programm should work now on A600HDs and A600s, too. If there are any problems, then please let me know it. I have only written the OS routines and had no testmachines.

All caches etc. will be supported and the new COPYBACK mode from MC68040 is working, too.

This programm does crash, if utilities like ReKick are active. It is caused by the fact that the programm only checks the ROMs!In my opinion this is no bad fact because only some developers and hackers use such tools.

The programm was developed with the use of Kickstart 3.0x . It

works with older Kickstart version in the same way. Consider buying a new Kickstart version because only the new versions (OS2.++) make the AMIGA real worth using.

The Intuition Interface was designed using GadToolsBox 37.300 by JABA Developments.

VirusWorkshop is no background viruskiller. Every writecommand from an other programm can change the directory structure and the disc information cannot (sometimes) be completely checked.

Another point is that the usage of memory is too big.

This programm needs:
1. xfdmaster.library
2. reqtools.library
3. DMS packer (only if you use DMS check!)
4. OWS packer (" OWS)
5. gadtools.library
6. FileID.library
7. AmigaGuide (*) library

How many memory needs this viruskiller?

About 270 KB mainprogramm and the memory for the libraries and for the files. This means that it needs approx. 650 KB, when you try to check files. Result:

THIS PROGRAMM REQUIRES AT LEAST 1 MEGABYTE TO WORK.

I think this is not a real big disadvantage,because every real user should have at least 1MB memory.

This viruskiller was spreaded as a LHA archive with the name "TRSIVW67.lha". It contains the following files:

```
VirusWorkshop
VirusWorkshop.info
Virusworkshop-News
VirusWorkshop-News.Info
FILE_ID.DIZ
Install
Install.Info
Install.script
Pref-Edit
Pref-Edit.info
Vw.Displayme
VW.prefs
VW.prefs.README
MagiCWb.readme
   MAGICWB/...
```

```
   LIBS/explode.library
   LIBS/reqtools.library
   LIBS/xfdmaster.library
   LIBS/fileID.library
   DOCUMENTS/Virusworkshop.Guide
   DOCUMENTS/Virusworkshop.Guide.INFO
   DOCUMENTS/VWMemmon.Guide
   DOCUMENTS/VWMemmon.Guide.INFO
   DOCUMENTS/Starterproblems.Guide
   DOCUMENTS/Starterproblems.Guide.INFO
   DOCUMENTS/Pref-Edit.Guide
   DOCUMENTS/Pref-Edit.Guide.INFO
   DOCUMENTS/NewVirus.Guide
   DOCUMENTS/NewVirus.Guide.INFO
   DOCUMENTS/DHunk.Guide
   DOCUMENTS/Dhunk.Guide.INFO
   DOCUMENTS/VW-Save!.Guide
   DOCUMENTS/VW-Save.Guide.INFO
   DOCUMENTS/VW-Viruses.Guide
   DOCUMENTS/VW-Viruses.Guide.INFO
   DOCUMENTS/ELrm.Guide
   DOCUMENTS/ELrm.Guide.INFO
   TOOLS/Dhunk
   TOOLS/Dhunk.INFO
   TOOLS/ELrm
   TOOLS/ELrm.INFO
   TOOLS/VW-Save!
   TOOLS/VW-Save!.INFO
```

```
* = This Kickstartrelease  will  be  correctly  recognized,but  the
the Memorykill function is not fully avaible because this is a
BETA release and newer (official) versions are on the market.

(*) AmigaGuide  Library  is  (C) by  Commodore. Therefore I am  not
allowed to spread this library in the VirusWorkshop package.
```

1.19 Veröffentlichung

```
                    Notizen für die Veröffentlichung
                    --------------------------------


VirusWorkshop sollte auf folgenden Rechnern arbeiten:



1.Allen AMIGA Rechner mit folgenden Betriebssystemversionen:
(diese Versionen müssen aber an den original ROM Adressen
liegen. Also keine Kickstartversion bei $2000000!!!!)

-Kickstart V2.04  (V37.175 im A3000 und A2000/A500(+))
-Kickstart V2.05  (V37.300)
-Kickstart V2.06  (V37.350)
-Kickstart V3.00  (V39.106)
```

-Kickstart V3.00a (V39.106b für den A1200)
-Kickstart V3.02 (V39.116BETA für den A4000) *
-Kickstart V3.03 (V40.9BETA für den A4000)   *
-Kickstart V3.04 (V40.38BETA für den A4000) *
-Kickstart V3.1ß (V40.55 für den A4000) *
-Kickstart V3.1ß (V40.55 für den A3000) *
-Kickstart V3.1ß (V40.62 für den A4000)
-Kickstart V3.1ß (V40.62 für den A3000)
-Kickstart V3.1ß (V40.68 für den A4000)
-Kickstart V3.1ß (V40.68 für den A3000)
-Kickstart V3.1   (V40.70 für den A4000(t))
-Kickstart V3.1   (V40.70 für den A3000)
-Kickstart V3.1   (V40.63 für den A2000/A500(+))
-Kickstart V3.1   (V40.68 für den A1200)
-Kickstart V3.1   (V40.63 für den A600)

Kickstart 40.65 (CD32 Version) wird nicht unterstützt, da ich dieses Biest auf meinem A4000 nicht zum Laufen bekomme. Sobald ich die Möglichkeit habe, an einem CD32 mit SX1 etc. zu coden, werde ich diese Lücke schliessen.

2. Amigas mit MMU, FPU.
3. Amigas mit 680xx Prozessoren (einschließlich MC68040)
4. Amigas mit normalen,enhanced (ECS) oder AGA Chipset.
5. Amigas with atleast 8 KB of stack, if you work with large directories.

Achtung: Die Kickstart 40.70 Versionen in A4000 und A4000t unterscheiden sich. Beide Versionen werden natürlich anerkannt.

Der Support der verschiedenen Kickstartversionen war mir nur möglich durch den großartigen Support einiger Entwickler, die mich an Ihren Rechner arbeiten ließen. Auf Nachfrage bei Commodore Deutschland hörte ich immer nur, daß ich mich als Entwickler registrieren lassen sollte....Mir ging es auf einer Messe nur um Kickstart 40.70 für den A4000t. Ich wollte nur ein 10 KB File aus dem ROM lesen, um eine Anpassung schreiben zu können. Natürlich wurde ich abgewiesen mit diesem Wunsch...

Das Programm wurde mit sämtlichen (für uns verfügbaren) Workbench-versionen getestet (einschließlich der Workbench 40.42) und alle Funktionen arbeiteten gut.

Das Programm sollte auf A600HD und A600 arbeiten. Wenn Probleme auf-tauchen, dann lassen Sie es mich bitte wissen. Ich habe nur die Routinen für diese Rechner geschrieben. Leider standen mir keinerlei Testrechner zur Verfügung.

VirusWorkshop hat keine Probleme mit den Caches der Prozessoren MC68030 und MC68040.

Das Programm läuft nicht (bzw. der Vectorkiller),wenn Programme wie Rekick oder ZKick aktiv sind.VirusWorkshop testet direkt die ROMs.

VirusWorkshop wurde entwickelt unter Kickstart 3.1. Es arbeitet mit allen Betriebssystemversion größer=gleich V2.04.

Das Intuition Interface wurde entwickelt mit der Hilfe der GadTools Box 37.300,welche von JABA Developments geschrieben wurde.

VirusWorkshop ist kein Hintergrundviruskiller. Wenn Sie einen solchen Viruskiller benötigen, rate ich Ihnen zu VirusZ. Jedes Schreibkommando kann die Direktorystruktur verändern und es kann zu Fehlern beim Checken einer Diskette führen. Außerdem ist der Speicherverbrauch zu hoch.

VirusWorkshop benötigt: 1. xfdmaster.library
2. reqtools.library
3. DMS packer (nur beim DMS CHECK
4. OWS packer (" OWS)
5. gadtools.library
6. FileID.library
7. AmigaGuide Library (*)

Wiviel Speicher braucht VirusWorkshop ?

Ca.270 KB Speicher werden für das Hauptprogramm benötigt. Dazu kommen 250 KB für den Filecheck Buffer und zusätzlich noch Speicher für die Libraries und für Intuition.

Dieser Viruskiller wird in einem LHA Archiv mit dem Namen:

"TRSIVW67.lha" weitergegeben.Es enthält folgenden Files:

VirusWorkshop
VirusWorkshop.info
Virusworkshop-News
VirusWorkshop-News.Info
FILE_ID.DIZ
Install
Install.Info
Install.script
Pref-Edit
Pref-Edit.info
Vw.Displayme
VW.prefs
VW.prefs.README
MagiCWb.readme
   MAGICWB/...
   LIBS/explode.library
   LIBS/reqtools.library
   LIBS/xfdmaster.library
   LIBS/fileID.library
   DOCUMENTS/Virusworkshop.Guide
   DOCUMENTS/Virusworkshop.Guide.INFO
   DOCUMENTS/VWMemmon.Guide
   DOCUMENTS/VWMemmon.Guide.INFO
   DOCUMENTS/Starterproblems.Guide
   DOCUMENTS/Starterproblems.Guide.INFO
   DOCUMENTS/Pref-Edit.Guide

```
   DOCUMENTS/Pref-Edit.Guide.INFO
   DOCUMENTS/NewVirus.Guide
   DOCUMENTS/NewVirus.Guide.INFO
   DOCUMENTS/DHunk.Guide
   DOCUMENTS/Dhunk.Guide.INFO
   DOCUMENTS/ELrm.Guide
   DOCUMENTS/ELrm.Guide.INFO
   DOCUMENTS/VW-Save!.Guide
   DOCUMENTS/VW-Save.Guide.INFO
   DOCUMENTS/VW-Viruses.Guide
   DOCUMENTS/VW-Viruses.Guide.INFO
   TOOLS/Dhunk
   TOOLS/Dhunk.INFO
   TOOLS/ELrm
   TOOLS/ELrm.INFO
   TOOLS/VW-Save!
   TOOLS/VW-Save!.INFO
```

```
* =Diese Kickstartversion wird zwar korrekt erkannt, aber die
VectorkillerFunktion ist nicht aktiv, da neuere Betaversionen
existieren.
(*)= Auf die AmigaGuide Library hat Commodore das Copyright und
daher  ist es mir untersagt, diese Library mit in das VW Packet
einzubinden.
```

1.20 MENUINSTRUCTION

```
                    Description of the menus:
                    -------------------------


On the top there are two big boxes with some important information:

1a. Which Kickstart is used?
2a. Where is the VBR pointing to?
3a. Is the FILEID function activated(DEFAULT=NO)?
4a. Is the AUTOKILL function activated(DEFAULT=NO)?
5a. Is the DECRUNCH function activated(DEFAULT=NO)?
1b. Which CPU do you use?
2b. Which FPU do you use?
3b. Which MMU do you use?


At  the  moment  I  only use the AttnFlags in Execbase (296(a6)) to
test this stuff. If my new assembler arrives I am going to write an
optimized check  routine which executes  some MMU and FPU commands.
The assembler I am using at moment, does not support their
instructions...
```

1.21 Menuerklärung

Beschreibung der Oberfläche

Sie können 2 große Boxen im oberen Viertel erkennen,welche wichtige Informationen beeinhalten:

1a. Welche Kickstartversion wird verwendet ?
2a. Wohin zeigt das VBR ?
3a. Ist die FileID Funktion aktiviert ? (Grundeinstellung=Nein)
4a. Ist die Autokill Funktion aktiviert ? (Grundeinstellung=NEIN)
5a. Ist die Decrunch Funktion aktiviert ? (Grundeinstellung=NEIN).

Ich benutze z.Z. nur die AttnFlags aus der Execbase (296) um diese Werte zu erhalten.Mein derzeitiger Assembler hat Probleme mit der MMU und der FPU. Sobald eine neue Version, die richtig arbeitet, auf dem Markt ist, wird dieses Manko behoben.

1.22 SEKTORCHECK

Sektor Check:

Schritt 1:

Zuerst wird der Diskvalidator geladen und auf Virus untersucht. Dieser Vorgang wird bei allen Kickstartversionen durchgeführt.

Folgende Dos bzw. Disktypen werden unterstützt:

1. DOS0 = altes langsames Filesystem
2. DOS1 = altes schnelles Filesystem
3. DOS2 = langsames Filesystem mit internationalem Modus (Kick 2.+)
4. DOS3 = schnelles Filesystem mit "

(Kick 3.+)

5. DOS4 = langsames Filesystem mit internationalem Modus und DirectoryCaching.
6. DOS5 = schnelles Filesystem mit internationalem Modus und Directorycaching.

Zur Zeit sind mehr als 11 Viren bekannt,die den Diskvalidator infizieren können.

Schäden:

Alle Diskvalidatorviren können die Informationen der einzelnen Sektoren verändern. Der Revenge of the Lamer Exterminator und der Diskval1234 Virus zerstören Sektoren so, daß sie nicht wieder repariert werden können. Ich suche dringend nach dem RISC Virus.

Schritt 2:

Jeder Sektor wird einzeln geladen und auf Viren und Fehlern bei den Sektorchecksummen untersucht.Schäden der Saddam Viren, des neuen Pestilence 1.15 Bootblockviruses und des XCopy 6.5 Viruses (auch The course of Little Sven genannt) können repariert werden. Fehlerhafte Checksummen werden auf Wunsch on VirusWorkshop auch entfernt. Sektoren, deren Dateninhalt verändert wurde (z.B. vollständiges Überschreibung durch das Wort "LAMER" etc), können leider NICHT restauriert werden, da die Originaldaten nicht mehr verfügbar sind.

Schäden der folgenden Viren können NICHT restauriert werden:

-SHIT
-FAST EDDIE
-OVERKILL
-CRIME 92
-Lamer EXTERMINATOR
-BURN 1+2

Alle Sektorroutinen können NIEMALS 100% sicher bei FFS Disketten sein, da der Sektorinhalt den Daten eines Virus vergleichbar sein kann.

Saddam und die Clones suchen in dem ersten geladenen File nach der Sektormarke $8. Dann wird eine spezielle Sektorkennung (z.B.IRAK) an das erste Langwort des Sektors geschrieben.Die Marke $8 besagt, daß es sich bei dem Sektor um einen Datablock handelt. Nur der 1. Datablock eines Files wird von Saddam Viren codiert. VirusWorkshop testet aber jeden Block auf eine mögliche Veränderung.

VirusWorkshop verfügt über eine spezielle Sectorroutine,die nicht auf spezielle Langworte an erster Stelle des Sektors testet. Somit brauchen Sie keine Angst vor neuen Saddam Clones zu haben.

Der Little Sven Virus ersetzt die $8 nur durch $ABCD0008. Dieser Schaden kann von VirusWorkshop behoben werden.

VirusWorkshop verfügt über eine Routine, die die komplette Diskette auf falsche Checksummen testet. Es kann passieren,daß ein Requester mit folgender Meldung erscheint :

"SectorChecksum is not correct! Repair?"

Sie können diesen Schaden beheben,aber bei FFS Disketten besteht keine 100% Sicherheit. Ich würde in solchen Fällen immer zu Disk-Salv von Dave Haynie (11.27 oder höher !!!).

Als letzter Teilschritt wird er Rootblock der Diskette geladen und

auf Veränderungen des Saddam Viruses untersucht.

Schritt 3:

Der Bootblock wird geladen und untersucht. VirusWorkshop verwendet keine externen Bootblockbibliotheken!!!!

(Errare humanum est!)

Folgende Programme werden erkannt:

- 300+ Bootblock Viren
- 460+ Bootblöcke mit kleinen Hilfsprogrammen.

Der Sektorchecker wurde getested mit:

-GVP Serie II Controller im A4000+A2000 (MC68030+MC68000)
-Oktagon Controller im A4000/A2000
-MultiEvolution 2.2 im A500(+)
-Evolution 3.0 on A2000+A3000
-GVPs Combo 2
-normaler AT controller in dem A4000/A1200

Folgende Festplatten wurden verwendet:

-Quantum ELS+LPS
-Maxtor
-HP
-Fujitsu AT
-Syquest 105 SCSI

1.23 SECTORCHECK

Sector Check:

Path 1:

First of all the Disk-Validator will be loaded and checked for viruses. This will be done under all Kickstarts and FileSystems. The following DOSTYPES will be supported:

1. DOS0 = old Slow File System
2. DOS1 = old Fast File System
3. DOS2 = SFS with international mode (Kick 2.00+)
4. DOS3 = FFS with international mode
5. DOS4 = SFS with international mode and Dircache (Kick 3.00+)
6. DOS5 = FFS with international mode and Dircache

Slow File System = SFS
Fast File System = FFS

At the moment there are more than 11 viruses known, which can infect the Disk-Validator:

1. Saddam Hussein 1+2+3+4+5+6 (No. 2 contains a new crypt-routine and No. 3-5 are only simple editor patches!)
2. Return of the Lamer Exterminator (father of the Saddam virus?)
3. Diskval1234 (a Saddam clone)
4. Risc Diskvalidator (also Saddam clone)
5. Saddam V1.29 & Laurien (changed Saddam][/ editor patches)

Known Damages:

All of this viruses can change the information of the tracks. The R.O.T.L.E. and the Diskval1234 Virus can completely destroy the information in the sectors. I do not own the Diskval1234 and RISC viruses, so if you have them please send them to me.

The Return of the Lamer Exterminator uses the OK Flag (Offset $138 Rootblock) to be activated. VirusWorkshop deletes the virus and writes a normal validator on the disk. The changed flag will not be fixed because there can be other error on the disk, too. Simply reset your machine and load your workbench. Then insert the previous infected disk. Follow the instructions and your disk will be correct again.

Path 2:

All sectors will be loaded and checked for viruses. Damages caused by the SADDAM (+ clones) and by the LITTLE SVEN virus will be fixed. All other failures cannot be fixed. If a sector is a part of a very important file, you have bad luck. There is NO(!) way to rescue the file.

The damage caused by SHIT, Fast Eddie, Overkill, rime92 and the Lamer Exterminator viruses cannot be fixed. All sectorbased routines cannot be 100 % secure on FFS because the sectordata can be equal to the data written by a virus! (This is not my fault!It is because of the new structures of this system!)

Saddam and it clones check the sector for the startmark "$8". Then they write their special longwords (e.g. "IRAK) at this position and code (eor) the sectors with the sectornumber. The startmark"$8" declares the sector in the SFS systems as a DATABLOCK. Please note that not all DATABLOCKs are changed! Only the first DATABLOCK of a file will be coded by SADDAM.

I have added a special routine which does not need the Disk-Validator to check a coded string. This routine does not care about the first longword in the sector. Hopy it all works fine

now. All clones (e.g. Saddam][1.29) can be easily found and the damage can be repaired. I made this routine only work with DOS0 (OFS) disks because the Saddam Virus only works with this disks. This routine slows down the testprocess but it is really secure.

The Little Sven virus only exchanges the $8 with a $ABCD0008 longword. This damages can and will be fixed!

A routine is included, which checks the whole disk for invalid checksums and similar stuff. It can happen that a requester appears which says:

"SectorChecksum is not correct! Repair?"

You can now fix the block but remeber that there can appear problems, if you use FFS disks (DOS1/3/5). FFS sectors can contain the same data as the recognition mark from OFS and the viruskiller does not recognize it (a general problem several time discussed in various networks !).

If your working drive is a harddisc, VirusWorkshop checks the disc only for invalid checksums. This routine was only written to use it with floppydiscs. I can happen that you have a bugfree HD and VW claims to have found an unnormal sector. Better use DiskSalv by Dave Haynie to fix it.

At the last point of the second path there will be loaded the ROOT-block from your drive (DFX:) and it will be scanned for a changed pointer to the BITMAPBLOCK.

The SADDAM Viruses use this method to become installed !!!

Path 3:

The bootblock will be loaded and checked for viruses and tools/intros etc. Then please press the left mousebutton to come back to the main directory. Many guys (especially some foreign members of SAFE HEX INTERNATIONAL) asked me to write a public bootblocklibrary or to include a LEARN function in this viruskiller. I do not code such things because of the danger of MISUSE. Please understand me. I have too often seen some changed extern files from other wellknown tools.

I will never include any extern files for this viruskiller (except the decrunch and reqtools Library). Even protections can be hacked and so I canceled this idea. The whole VirusWorkshop code is much harder to crack than a 50 KB nonpacked bootblocklibrary.

(Errare humanum est!)

Following programms will be recognized:

- 300+ bootblock viruses
- 460+ Utility bootblocks

1.24 DateiCHECK

Die LinkViren Suchfunktion:

Beim Start dieser Funktion wird zuerst ein englischer Text auf dem Bildschirm eingeblendet, der mitteilt, daß die Zeichen // beim Filecheck nur bedeuten, dass ein Unterdirectory NICHT voll ausgedruckt wurde, da der Name unter Umstaenden zu gross fuer den Bildschirm geworden waere. Natuerlich werden diese Unterdirectories sauber durchsucht !

Zuerst wird das angwählte Laufwerk getestet:

1. Ist die Diskette bzw.die Harddisk validiert ?
2. Schreibschutz ?
3. Ist der BitmapZeiger korrekt? (Saddam virus...)

Es kann passieren,daß folgende Mitteilung erscheint:

"Use TrackCheck and DriveInfo first. Dir is not correct!"

Diese Mitteilung erscheint nur,wenn der BitmapZeiger und/oder das Validierungsflag des Rootblockes nicht korrekt ist.Ein falscher Bitmapblockzeiger kann repariert werden.

Danach wird jedes File geladen und auf Viren getestet.Wenn ein Virus gefunden wurde,erscheint eine Mitteilung,die Ihnen die Wahl läßt den Virus zu entfernen oder fortzufahren.Es werden mehr als 200 Linkvirus/trojanische Pferde etc. erkannt.

Wenn Sie den Filetest abbrechen wollen, dann drücken Sie bitte die linke Maustaste. Die letzten Files laufen dann sehr schnell durch (ohne Test etc.) und VirusWorkshop stoppt.

Nach dem Druck auf die linke Maustaste sehen Sie weiterhin ein Gadget mit dem Namen "Automatic". Dieses Requester ist für User gedacht, die den Vorgang der Fileuntersuchung automatisieren wollen. Alle gefundenen Viren werden automatisch entfernt. Diese Option muss bei jedem Filecheck neu aktiviert werden, damit Sie nicht zu leichtgläubig werden und sich mit der Materie immer wieder auseinandersetzen.

Wenn ein Virus gefunden wurde, dann müssen Sie möglicherweise die Startup-Sequence ändern, da ein Virus unter Umständen in dem File eingetragen war und jetzt, da er nicht mehr vorhanden ist, zu einem Abbruch führen kann.

DMS Check

Diese Funktion ermöglicht es dem User ein DMS Archiv auf das aktuelle Laufwerk zu entpacken und die Diskette danach gründlich zu testen.

Nichts Außergewöhnliches ? Sie müssen nur einmal am Anfang den DMS Pfad einstellen und dananch nur noch das geünschte Archiv auswählen.Gedacht für Sysops oder Trader,die Ihren neuen Programme nur schnell testen wollen.

Achtung ! Für diesen Vorgang benötigen Sie den DMS Packer. Damit ist nicht die DMSWIn Oberfläche gemeint , sondern nur der eigentliche Packer. VirusWorkshop stellt dem Packer ein eigenes Fenster zur Verfügung.Sollte der Speicher knapp werden, wird das normale Ausgabefenster benutzt.

VirusWorkshop arbeitet auch mit gesplitteten Archieven. Diese dürfen nur in 2 Teile geteilt sein (Wer teilt seine Archive in größere Teile ?)

Das File wird von VirusWorkshop immer als komplette Diskette gesichert.Bentuzen Sie danach einen DMS Splitter...

Comment 16.11.1993: VirusWorkshop arbeitet sauber mit den neuen DMS Updates von BLACKHAWK/PDX !!!

Leider arbeitet VirusWorkSHOP nicht mit den DMS Versionen oberhalb V2.0, da eine Eingabe im Fenster erwartet wird, die ich nicht liefern kann.

Filereq

Wenn Sie eine einzelne Datei testen wollen,dann ist dies die richtige Funktion für Sie.

1.Convert : Bootjob 1.3 Dateien werden in normale Bootblöcke zurück konvertiert.

2.SingleDir: Mit dieser Funktion können Sie ein einziges Directory untersuchen (z.B. C:). Allerdings muessen Sie eine Datei in dem zu untersuchenden Directory anklicken, was aber nicht zu schwer sein sollte.

3.SingleF : Wenn Sie eine Datei selektieren,wird diese untersucht. Wenn Sie nur ein Verzeichniss auswählen,wird dieses Verzeichniss untersucht.Es wird nur dieses Verzeichniss untersucht und keine Unterverzeichnisse.

* Mit Bootjob können Sie normale Bootblöcke in normale Files umwandeln.

1.25 FILECHECK

The File/Link/Trojan Check:

At the start of the filecheck, there appears a message saying, that -> // <- means a not printed (but checked) subdirectory. Nowadays the filenames (including pathnames) become very long and I had to cut it a little bit to have enough space on the screen.

First of all the choosen device will be checked:

1. Is it validated?
2. Is it write enabled?
3. Is the BitmapPtr correct? (Saddam virus...)

It can happen that the following message appears:

"Use TrackCheck and DriveInfo first. Dir is not correct!"

This message only appears if the BitmapPtr and/or the VALIDflag ($138) is not correct. A wrong Bitmap pointer caused by Saddam can be fixed , of course.

Every file will be loaded and scanned for viruses. If a virus was found a little message appears on your screen. You can destroy/fix all known link viruses and trojan horses. Over 200(!) species will be recognised. What do you want more?

If you want to stop the filetest, then simply press the left mousebutton. The last files of your directory become printed very fast on the screen and then the programm stops.

If you pressed you will recognize a gadget called Automatic. This gadget will automize the filechecking. If you have activated this, all viruses will be removed from the device and you don't have to wait and sit next to your machine all the night. This function has to be enabled every time you start a filecheck !!!!

If a virus was found, please check the startup-sequence because it can be possible that you have to fix it: A line has to be deleted...

This function includes a multicheck. Wait, I will explain it to

you:

The virus "Revenge of the Lamer Exterminator" (a species, which is not a real link virus like IRQ -> it does not add a hunk etc. to the infected file!) is infected 5 times by the IRQ-II virus. VirusWorkshop will ask you 5 times to kill the "IRQ" virus and as a last step it'll ask you to kill the "Revenge of the Lamer Exterminator" virus. It should work all correct by now. If you have problems, call me!

The Repairroutine for viruses, which add a hunk to the file, is a standart routine. Some viruses (CCCP,QRDL etc.) have wrong infect routines. That means that many files, which are infected with the above listed viruses, does not work. VirusWorkshop is not able to make this programms work again.

DMS Check

This option enables you to depack a DMS archive to a disk and to check the disk for viruses.Nothing special you may say.BUT you have only to specify the file you want to check and the dest. drive.At the start you have (only at the first start) to specify where the original DMSpacker can be found !Very usefull for SYSOPs and other person, who just want to check their new files and does not want to leave the VirusWorkshop.

ATTENTION: The DMS packer (and not DMSwin) is needed. This packer is not included in the VirusWorkshop archieve. VirusWorkshop has been tested with DMS1.11, DMS1.11+, DMS 1.53, DMS 2.02 & DMS 2.04. The output window for the DMS information is a special CON window, if you have enough free memory. If your free memory is too low, then the original WB output window will be used(or the CLI window, if you start the VirusWorkshop from your CLI).

VirusWorkshop recognizes both,splitted and complete archieves.If it detects a splitted archive it will ask for a second time for a name from an archive.I think this is enough. Who splits a normal DMS archieve in more than 2 parts ? Nobody I think.

The corrected and repacked archive will contain the whole disk and not only the splitted disc.Use a splitting archive after working with VirusWorkshop.

Comment 23.07.1993.:I have added an OWS checker,too.OWS is a diskwarper like DMS.This routine does not support singlediscs or such comfortable stuff.If you have once selected the DMS archiever it is too late.The DMS archiever will be used always.OWS is not often used on BBSs (at least I did not see one packed OWS file) but some users asked me to include this.

The actual version of OWS is 1.2c (08.08.1993.)

Comment 08.08.1993: I heard about problems with decrunching DMS files.I am using the DMS V1.11 Turbo Generic and it is working perfect.

Comment 16.11.1993: VirusWorkshop works perfect with the new DMS updates by BLACKHAWK/PDX. I am very sorry, but the new DMS 2.0x versions can't be used at the moment, because DMS wants to have an answer in the window, which I cannot produce.

Filereq

If you just want to test a single file, this is your right funtion. You can select, what to do.

1.Convert : Bootjob 1.3 files will be reconverted to normal boot-blocks and you can save the bootblock as a normal 1024 byte long file.

2.SingleDir: Now you can check a singledirectory without subdirs etc. in a very easy way: Just click into the directory you want to check and click on one file. Then this directory will be checked.

3.SingleF : You select a filename and this file will be scanned for viruses. If a virus was found, you can repair/delete the file,if you want to do this.

3a (VW2.4 and higher!): SingleF: You select only a directory and all files in the directory will be checked.

* Bootjob is a tool which can write bootblocks to disks as files, sectors and as a normal executable file.A virus can be saved as a normal file and can be given to other person and no viruskiller will find it.USE IT WITH CAUTION !!!!

1.26 MemoryCHECK

Die Speicher-Kontroll Funktion:

Folgende Pointer werde untersucht:

- fast alle Offsets der Exec & Dosbase
- die komplette Zeropage & Vectorpage
- Interrupts und Server

Sie können weiterhin Devices,Ports,Libraries,Tasks, Resourcen und Semaphoren testen. Diese Funktionen sind sind NICHT in der eigentlichen Speicher-Kontroll Funktion eingebaut,sondern müssen extra gestartet werden.

Weiße Schrift bedeutet IMMER,daß in Ihrem System einige Vektoren NICHT in ihrem normalen Zystand sind.Zögern Sie nicht,verbogene Vektoren zu löschen.Es werden zwar auch alle Patches entfernt, aber Sie können auch fast sicher sein,daß sich kein Virus im SPeicher befindet.

! VirusWorkshop erkennt nicht alle Viren mit Namen im Speicher !
Sämtliche neuen Viren ab 1.1.1994. sollten aber sauber im Speicher MIT Namen erkannt werden. Ältere Virenanpassungen werden in Stücken nachfolgen...

~Erkannte~Patches~(englisch)~

1.27 RAMCHECK

The Memory Check Function:

The following things will be checked:

- everything in ExecBase (library)
- everything in DosBase (library)
- Interrupts and Servers

You can also check devices, ports, libraries, tasks, resources and semaphores. This functions are not included in the RamCheck, however, in the same menu. The RamCheck function is the most important thing. All vectors in white letters are important. If you use SetPatch or similar stuff do not wonder about the high amount of changed vectors in Exec and Intuition. This functions are not printed in white letters!

IF WHITE LETTERS APPEAR, YOU SHOULD USE VECTORKILL!!!

If only one white text appears which says "Caused by explode.libs", then don't worry. It is the caused by the explode.library, a decrunching library for the great Turbo Imploder. Make sure that you only use version 6 and higher. Many bugs have been fixed and the accelerator card problems does not exist anymore.

All interrupts will be shown (zeropage and vectorpage). Several viruskillers only test the zeropage. There are some clever viruses, which do not touch the zeropage but modify the vectorpage. VirusWorkshop will show you both types!

VirusWorkshop does not know all viruses by name in RAM. If you see some white letters, just kill it. It does not destroy your system.

Attention:

Comment 24.01.1993: I have included a little "REKICK" test. All kickfiles should be detected by now. Note that I cannot give you in this way the 100% security because nearly all vectors point in the memory.

THIS FUNCTION CAUSES ENFORCERHITS BECAUSE IT READS THE ZEROPAGE & THE VECTORPAGE. THERE IS NO WAY TO SOLVE THIS PROBLEM. LIVE WITH IT OR LET THE VIRUSES STAY ALIVE. ALL OTHER VIRUSKILLERS CAUSE SUCH ENFORCER HITS, TOO.

If the ENFORCER is running, you $64 vector in the vectorbase is not correct. You can kill it but then is ENFORCER dead,too.

Comment 31.03.93: I have heard some rumors that a new Enforcer (37.36) is on the market right now. This version does not touch the $64 vec.!!

Comment 18.04.93: I have finally recieved Enforcer V37.36 and my Enforcer does touch the $64 vector. Two versions in circulation ?

~Recognized~patches~

1.28 Patches

The following patches will be recognized from VW:

- CPUClr 3.1 by P.Simon: It is patch for a GFX BLIT function, which makes the processor (only usefull for 68030&68040) make the work,

because it is a lot faster than the good old BLITTER.

- Switch NTSC by M.Kamper: This is a patch for the Int.OPENSCREEN function under Kickstart 2.xx.

- PatchAsm 1.0 by Flake/D-TECT: It is patch which changes a special byterow, which will be written from the ASM-One 1.15 release (TFA).

- Enforcer V37.28/36/39/49/52 by M.Sinz :Nothing more to say about this great debugger tools. The recognition code takes the $64 vector in the vectorpage, which will be changed by ENFORCER.

- Explode Library by J.A.Brower : This library patches the LOADSEG and in newer releases the NEWLOADSEG vectors in the Doslibrary. All with IMPLODER crunched files will be automatically decrunched.

- Segtracker by M.Sinz : This is a special tool for the ENFORCER friends of you. Changed offsets are (NEW)loadseg and Unloadseg. Segtracker 37.55 will be detected now, too (37.55).

- Selfdefender 0.900 by ?? : This programm is mainly used by BBS owners.It patches some vectors which can (will) be used at a system failure (GURU). The GURU does not appear because the SELFDEFENDER resets your machiene.All programms,which use the normal system requester routines crash.VW does not crash because of the use of the reqtools.library.

- Action Replay IV Software Update by Blackhawk/Paradox.This is a software update from the AR-III eprom software.Now it works with the A1200/A4000.
NOTE: This programm is not a real update by Datel. When will come your update ?

- DosTrace 1.0 & 2.0 by Peter Stuer: This is a programm like SnoopDos.It requires at least 512 KB memory and Kickstart 2.04. Over 10 vectors will be patched as default from DosTrace .VW re-writes the complete librarievectors and not only the 10 patched vectors.

- DosTouch 1.x : This is a SnoopDosclone like DosTrace.This patch will be removed correctly and only the patched vectors will be re-stored.

- NewAlert by Brian Gontowski: This patch installs a new ALERT-routine,which shows the user more informations than the real ALERT routine.Many Errors etc. will be shown.This tool is Kick2.++ only . The following vectors will be changed by this tool:
Kicktagpointer,Kickmempointer & Kickchckpointer...

- Degrader 1.60 by Chris Hames: This tool enables the user to run many systemfriendly programms,which does not want to work with AGA Amiga computers.You can emulate the PAL mode and other very interesting things.
The changed Coldcapture Vector will be rewritten...

- Virus Interceptor 1.14 by J.Eliasson: An antivirustool,which patches the LOADSEG & NEWLOADSEG vectors.Works with Kickstart 3.0.

Comment 16.11.1993: Fixed for version 1.15 !

- PPLoadseg 1.4 by Nico Francois: This tool patches the LOADSEG-vector and enables the user to use transparent PP data files.VW can rewrite the original LoadSeg vector.

- PowerData 38.200 by Mr.Berg: This tool makes the PP data files completely transparent.The datafiles can be loaded and decrunched. On the other hand the normal datafiles can be crunched while

saving them.The following Dos vectors will be changed:
DOS Open,DOS Close,DOS Examine,DOS Write ...
VW can only rewrite ALL vectors...

- Dircache 1.02 by L.Wolf:This tool is a diskcaching programm. It patches the BeginIO Vector of the specified device.Sometimes VW can recover the original value.In all other cases,VW tries to recover all vectors.

- RT Patch 1.1 & RT Patch 1.2:You should only use the newer&better version 1.2 of this programm.It patches several library,so that the REQTOOLS Library will be used.

- Syndicate Coder Patcher 37.18: This is a little tool, which installs a little patch in DosRead& DosWrite to (de)code the file, which is going to be accessed. Very positiv that this tool can remove itself by the "r" option.

- ReqChange 3.2 by ??? : This is a very usefull patch, which changes all types of requesters to the reqtools requesters. VW will rewrite the patch for OldOpenLibrary, because some viruses use this vector, too.

- Messkill Repair 0.9 by ?? : This is a little repairprogramm for damages caused by the ELENI! virus. This patch is not systemclear and not so well coded. Please delete it !

1.29 Supported_Screen_Resolutions

Supported Screen Resolutions

IMPORTANT: If you have an AMIGA 4000 with a 1084 monitor or a similar monitor, which does not work with higher AGA modes then please clear all monitordrives (except PAL and NTSC) in your directory sys:devs/monitors.
You cannot use other resolutions ! Think about buying a better monitor ! This "bug" appears with other programms, too.
(This text was copied from the great VT docfile !)

You can select all modes starting with 640*256. The heigth MUST be higher equal 256 pixels and the width MUST be higher equal 640 pixels/row.

The selection will be done via the preferences editor !

Name from the Preferencesfile: env:VW.Prefs

~New~Preferencesfilestructure~

1.30 ScreenModi

Unterstützte Screenauflösungen:

Wichtig: Wenn Sie einen A4000 mit einem 1084 Monitor (oder einem ähnlichen Gerät) benutzen, dann löschen Sie bitte alle Monitor-treiber aus dem devs/monitors Ordner bis auf PAL und NTSC. Andere Modi können Sie mit einem solchen Monitor so oder so nicht benutzen !
(Diese Textpassage wurde von dem großartigen VT Dokument kopiert!)

Alle Aufloesungen ab 640*256 werden unterstützt. Die Auswahl der Aufloesungen erfolgt im Preferences Editor !

Name der Preferencesdatei: env:VW.Prefs

~New~Preferencesfilestructure~

1.31 Boot->File

Die Bootblock zu File Funktion

Achtung ! Das aktuelle Laufwerk MUß DFx sein !

Der Bootblock wird geladen und danach als File auf Diskette gesichert.Diese Funktion arbeitet unabhängig von der DOS Version und kann sowohl 1024 als auch 2048 Byte lange Bootblöcke bearbeiten.

Normalerweise sind Bootblöcke 1024 Byte lang.Wenn Sie eine Disk haben,die direkt aus dem Bootblock startet (z.B. Pinball Fantasies oder fast alle Spiele von Psygnosis oder das Demo "Voyage" von Razor), kann es ganz sinnvoll sein, 2048 Bytes zu sichern. Viren, wie z.B. der OVERKILL Bootblockvirus überschreiben nämlich auch die Sektoren 2-3 und der Lader versagt und es kommt in den meisten Fällen zu einem Systemabsturz.

1.32 BOOT_TO_FILE

The Bootblock to File Function:

Note: The working drive must be DF0:, DF1:, DF2: or DF3:!

The bootblock (BB) will be loaded and then saved to disk. This function supports all FileSystems and works with 1024 / 2048 byte

long bootblocks.

The normal situation is that you only have to save 1024 bytes. If you have a disk, which loads directly from the bootblock (e.g. all Psygnosis games or trackloader demos e.g. Voyage/Razor 1911) it could be useful if you save 2048 bytes. If a virus like 'OVERKILL' copies the first 1024 bytes into sector 2-3, the data in this sectors are destroyed and the loader can crash.

1.33 FILE_TO_BOOT

The File to Bootblock function:

Note: The working drive must be DF0:, DF1:, DF2: or DF3:!

A chosen file will be loaded and checked for DOSx. If everything is correct, the bootblock will be written to disk.

1.34 File->Boot

Die File zu Bootblock Funktion

Achtung ! Das aktuelle Laufwerk MUß DFx sein !

Das selektierte File wird geladen und auf "DOS " gecheckt.Wenn es korrekt ist,wird es als Bootblock auf die Diskette geschrieben.

1.35 BB_Installation

Die Bootblock Installierungsfunktion:

Bitte beachten Sie,daß das aktuelle Laufwerk DFX sein MUß!

Sie haben die Möglichkeit einen normalen Bootblock und einen sog. MYSTIC Bootblock zu installieren. Danach werden Sie nach dem gewünschten Filesystem gefragt.

ACHTUNG! Wenn Ihre Diskette im FFS formatiert ist, müssen Sie natürlich auch FastFileSystem (FFS) wählen, da sonst das Betriebs-system nach dem nächsten Reset von einer falschen Filesystem-version ausgeht und es zu folgenschweren Fehlern kommen kann.

Wenn Sie ein Kickstart 3.xx System verwenden, dann werden Sie noch gefragt,ob Sie den internationalen Modus (mit Dircaching) benutzen möchten.

Beispiel: Sie wollen auf einer DOS1 Diskette (FFS) einen neuen Bootblock installieren ! Sie müssen dann bei der Installation unbedingt darauf achten, dass Sie

1.FastFileSystem angeben
2.Kein internationales Filesystem benutzen
3.Kein Dircache benutzen !

Im anderen Falle kommt es zu Fehlern auf ihrer Diskette, da die Daten nicht verarbeitet werden können.

1.36 INSTALL

The Install function:

Note: The working drive must be DF0:, DF1:, DF2: or DF3:!

You have the choice to install a normal Bootblock and "MYSTIC" bootblock. Then you will be asked for the filesystem. If you have a disk, which is formatted in FFS, you should use the FastFileSystem (FFS).

If you have the new Kickstart 3.xx system then you will be asked if want to use the international mode. This mode is an improved filingsystem(better errorcorrections/blockstructure).

The "D-TECT" bootblock enables you to kill all viruses in memory. This bootblock was especially written for the use with the older Kickstart 1.x versions. Under Kickstart 2.x and higher you should only use the normal bootblock because the "D-TECT" bootblock uses a direct ROMjump ($fc0000),which crashes under Kickstart 2.x.

Comment 25.07.1993.: The "D-TECT"bootblock was replaced by a MYSTIC bootblock with the same functions.It‘s new that the BB clearly performs a RESET on OS2.x & OS3.x AMIGAs. Due to the fact that I don‘t have a hardware register listing of the AGA chips, the BB will have a non complete Copperlist and shows you only garbage.If it happens, at least one of your vectors is changed.

Comment 26.07.1993.: The new "MYSTIC" bootblock contains no direct hardware access. It uses only INTUITION Library functions and it perfectly works on all MC680X0 and on ECS, AGA and on the normal chipset.

1.37 BB_Erstellung

Die Bootblock Erstellungsfunktion

Bitte beachten Sie,daß das aktuelle Laufwerk DFX sein MUß!

Stellen Sie sich folgende Situation vor:

Sie haben eine kleine Datei (max.954 Bytes lang),die zudem auch noch komplett PC relativ programmiert ist und Sie wollen nun dieses Programm aus dem Bootblock heraus starten.

Was tun, wenn man kein Wissen über den Bootblockaufbau hat ?

Benutzen Sie einfach diese Funktion !!! Ein Dateirequester erscheint und Sie können das zu ladende File aussuchen.Danach wird der Datei der nötige Bootblockcode hinzugefügt und auf Diskette gespeichert.Fertig.

Diese Funktion ist sinnvoll für Personen, die kleinen Utilities im Bootblock unterbringen wollen (als Beispiel).

1.38 MAKEBB

The Make BB function:

Note: The working drive must be DF0:, DF1:, DF2: or DF3:!

Just imagine the following situation:
You have a little file (max. 954 Bytes long), which is completly PC relativ and you want to start this programm in the bootblock.

What to do?

Simple use the "MAKE BB" function. A file requester appears and you can choose the file to load. You need not to write any routines, which execute the bootcode. This function makes all for you. Simply follow the given instructions.
This routine only supports the 1024 byte long bootblocks because it is to dangerous to write 2048 bytes, if you not know, what is on the blocks 2-3.

1.39 SHOW_Startup-Sequence

The Show S.Seq. function:

You can show the Startup-Sequence. It can be very important in some cases. Example: Viruses like the Disaster Master 2 Virus write "cls *" in the first place of the Startup-Sequence. This virus can easily detected by this function. I have missed this function in most other viruskillers.

1.40 Zeige_Startup-Sequence

Die Anzeigefunktion für die Startup-Sequence:

Diese Funktion zeigt Ihnen die Startup-Sequence.Dadurch können Sie in vielen Fällen leicht Viren erkennen.

So schreibt der Disaster Master 2 Virus folgenden String an die erste Stelle der Startup-Sequence:

"cls *"

1.41 Kickstart-Auszug-Sicherung

Die Kickstartsicherungsfunktion

Diese Funktion erlaubt dem User die wichtigsten Vektoren aus Dos Library, IntuitionLibrary, Zeropage, ExecLibrary und aus dem TrackDisk Device herauszusichern. Jeder Block ist 2 Kilobyte lang. Mit anderen Worten: das komplette File ist 10 Kilobyte lang.

Auf diese Weise kann ich VirusWorkshop schnell an neue Kickstart-versionen anpassen.

Speicherblock:
---

dos.library	-$400 - +$400 =	$800 bytes
intuition.library	-$400 - +$400 =	$800 bytes
zeropage	$000 - +$800 =	$800 bytes
exec.library	-$400 - +$400 =	$800 bytes
trackdisk.device	-$400 - +$400 =	$800 bytes
		$2800 (10240)

Wenn Sie diese Funktion benutzen wollen, stellen Sie sicher,daß keine Vektoren verbogen sind !!! Sehr wichtig !!!

1.42 KICKSAVE

The Kicksave function:

This function allows you to save the most important things in the DosLibrary, IntuitionLibrary, Zeropage, ExecLibrary and of the TrackdiskDevice. Each block is $800 bytes long. This means that the whole file is 10 kilobyte long. This function is only implented, if you use a new Kickstart version (e.g. OS41.115).

I can update the killer in this way very fast and easy.

Memblock:
---

dos.library	-$400 - +$400 = $800 bytes
intuition.library	-$400 - +$400 = $800 bytes
zeropage	$000 - +$800 = $800 bytes
exec.library	-$400 - +$400 = $800 bytes
trackdisk.device	-$400 - +$400 = $800 bytes
	$2800 (10240)

If you use this function make sure that the SetPatch command is not running and tools like the explode.library are not in the system because you would get too many changed pointers and this values are not useable ! It is the best to use the programm directly after the Systemstart.

Note for Programmers: Not all the vectors will be rewritten.I save only such a high amount of bytes to have an advantage for the future viruses.

1.43 AUTOMEMKILL

AutoVektorkiller(Preferences Menu):

Wenn Sie diese Funktion aktivieren,wird vor den meisten Funktion erst der Speicher von Viren befreit.

1.44 AUTORAMKILL

AutoRamKill (Preferences Menu):

This Viruskiller tries to kill all vectors in RAM, when you selected a function. You can allow this by activating this. It is very important that you do this. This function is included because many guys work with Kickstart versions, which will only be loaded

in the memory. In such a case your system crashes, if AutoRamKill is activated.

1.45 EXPLODE

Explode (Preferences menu):

If you activate this function, the ExplodeLibrary V6 or higher will be deactivated as long as the VirusWorkshop is active.

Just imagine the following situation:

1. The Infiltrator Virus will be installed in the system.
2. The ExplodeLibrary will be installed.
3. Programms like XXXXX are now not able to find the virus(!).

Because of this fact I have included this function! Just start the Memorycheck function. In most times you will see that the LoadSeg Vector is changed. Now start this function and you will (hopefully) see that the LoadSeg Vector is pointing in the ROM. If not, just kill it. The ExplodeLibrary will be reinstalled with all correct values after you quit the VirusWorkshop.

Important:

This function only works with Kickstart version which are higher/equal to OS 2.04. Under older Kickstart versions there are the idiotic BCPL pointers in the RAM and I cannot give you real security if you use this function!

That means, that you cannot activate this function, if you use a RAM kickfile or the "explode.library" is not installed.
If you use a tool like "MAPROM", which uses the MMU in your A4000 to make a new Kickstart resident you can use VW, of course.

Comment 06.04.1993.: Many peoply complain about the direct way of accessing to the system (all 2.x and 3.x kickstarts ALWAYS should stay at $f80000. If you are a softwarepirate and use ZKICK etc., it is not our fault. If you have problems with it, just call me.A real Viruskiller has to go deep in the system because it has to fix a

of internal adresses because many pointers can be used by a virus .

1.46 IMPLODE

Explode (Preferences menu):

Wenn Sie diese Funktion aktivieren,wird die Explode Library V6 oder höher deaktiviert.

Stellen Sie sich folgende Situation vor:

1. Der Infiltrator Virus befällt das System.
2. Die ExplodeLibrary wird installiert.
3. Viruskiller wie BootX können den Virus nicht mehr finden .

Diese Funktion arbeitet nur, wenn die Explode Library den Loadseg Vektor verändert hat.

1.47 QUIT

Quit (General menu):

After you've started this function, you can leave the viruskiller. At first a little security box will appear, which asks if you really want to quit the programm.

Then the buffers (from RequesterLibrary, FileID- and Decrunch-Library) will be given back to system and all the allocated memory will be given back to the system.
(->Filebuffer!!!)

1.48 Laufwerkinfo

Laufwerks Info (HD Tools):

Es erscheinene einige wichtige Informationen über das aktuelle Laufwerk.Wenn bei Diskstate (Status) "Problems..." erscheint,dann sollten Sie unbedingt Sectorcheck und danach den DiskDoktor bzw. Disksalv zu Rate ziehen.

Ein Weg,um an das Ziel zu kommen:

1. Take the RootNode pointer out of the DosBase (Offset 34)
2. Take the global DosInfo pointer out of the RootNode (Offset 24)
3. Take the DeviceListPtr out of the global DosInfo.

BE CAREFUL BECAUSE THERE ARE SOME bcpl POINTER HANGING AROUND!

Example in Assembler:

```
        move.l        dosbase(pc),a6
        move.l        34(a6),d0
        move.l        d0,a0           ; Pointer to the Rootnode
        move.l        24(a0),d0       ; Pointer to the global
                                      ; InfoStructur
        lsl.l        #2,d0            ; BCPL pointer *4
        move.l        d0,a0
        move.l        4(a0),d0
        lsl.l        #2,d0            ; Pointer to Devicelist*4

        move.l        d0,a0
        move.l        40(a0),d0
        lsl.l        #2,d0            ; Name of the Devices /
                                         ; Volumes etc.*4
                                         ; 1.Byte = Length of
                                         ; string...
```

The most important values are:

HEX.	DEZ.
$200	0512
$400	1024
$370	0880
$6e0	1760

When I tried to get the DosType out of the DosEnvec structure it appeared several times (under Kickstart 3.00) that the inserted floppy disk had always the DosType=0. It seems to be a bug in the DosLibrary or in the filing system. If you try to read the Dos=DiskType then you alway get the right values...

This means that Kick3.00 is bugged in this part of the filing system, too.

Another example: You formatted a disk using Kickstart 40.55 with the following command: FORMAT DF0 NAME: Leer FFS INTL .

What happens ? Dostype ist 0 and Disktype is 3 ? Crazy,isn‘t it ? (Tested on 25.07.1993. with an A4000/040 using Kick39.106)

1.49 DRIVEINFO

Drive Info (HD Tools):

Some important information will be given to the user about his actual selected drive. This routine is not written in the shortest and best way but it works and that is the most important point. If diskstate says "Problems..." then use (when using DFX) SectorCheck and afterwards the DiskDoctor from your workbench.

If you try it via DosInfo (Lock/Unlock) you can get problems. The right way:

1. Take the RootNode pointer out of the DosBase (Offset 34)
2. Take the global DosInfo pointer out of the RootNode (Offset 24)
3. Take the DeviceListPtr out of the global DosInfo.

BE CAREFUL BECAUSE THERE ARE SOME bcpl POINTER HANGING AROUND!

Example in Assembler:

```
        move.l          dosbase(pc),a6
        move.l          34(a6),d0
        move.l          d0,a0               ; Pointer to the Rootnode
        move.l          24(a0),d0           ; Pointer to the global
                                            ; InfoStructur
        lsl.l           #2,d0               ; BCPL pointer *4
        move.l          d0,a0
        move.l          4(a0),d0
        lsl.l           #2,d0               ; Pointer to Devicelist*4

        move.l          d0,a0
        move.l          40(a0),d0
        lsl.l           #2,d0               ; Name of the Devices /
                                            ; Volumes etc.*4
                                            ; 1.Byte = Length of
                                            ; string...
```

Kickstart 1.2 has some strange bugs in the DeviceStructures. It can happen that the BootPriority is extremly high. It is caused by a bug in DOS. I will search for another way to find the right value!

Another bug: It can happen that your high cylinder is at a normal 880KB diskette $370=880. This is caused by the operating system. At this routine all adresses are given as hex values.

The most important values are:

HEX.	DEZ.

```
$200                                                    0512
-------------------------------------------------------
$400                                                    1024
-------------------------------------------------------
$370                                                    0880
-------------------------------------------------------
$6e0                                                    1760
-------------------------------------------------------
```

When I tried to get the DosType out of the DosEnvec structure it appeared several times (under Kickstart 3.00) that the inserted floppy disk had always the DosType=0. It seems to be a bug in the DosLibrary or in the filing system. If you try to read the Dos=DiskType then you alway get the right values...

This means that Kick3.00 is bugged in this part of the filing system, too.

Another example: You formatted a disk using Kickstart 40.55 with the following command: FORMAT DF0 NAME: Leer FFS INTL .

What happens ? Dostype ist 0 and Disktype is 3 ? Crazy,isn't it ? (Tested on 25.07.1993. with an A4000/040 using Kick39.106)

1.50 FestplattenSUPPORT

```
  Lese, Schreibe, Zeige den physikalischen Zylinder 0:
             ---------------------------------------
```

Es gitb einige Viren,die den RDB von Ihrer Festplatte zerstören. Warum ? Entweder mit Absicht,oder sie testen nicht,ob sie das TrackDisk.Device gepatcht haben.Was passiert,wenn Sie mit dem "scsi.device" schreibend auf Block 0 einer Festplatte zugreifen ? Der RDB wird zerstört und die Festplatte nach einem Reset erst-einmal unbrauchbar.

```
Read  = Erstelle eine Sicherheitskopie des RDB.
        (Bitte auf eine einzelne Diskette!)
Write = Schreibe die Sicherheitskopie zurück auf die HD.
Show  = ASCII Darstellung des RDB
```

Benutzen Sie diese Routinen nur,wenn Sie kein spezielles Programm für solche Fälle direkt von Ihrer HD Herstellerfirma haben. BSC gibt (ALF/OCTAGON) ein sehr gutes Programm mit.
(Dies ist als reines Beispiel zu verstehen!!!)

Hier eine Liste von Viren,die den RDB vernichten können:

-Crime92 1+2,Overkill,ByteBandit,Zenker1+2,Burn 1+2

und weitere...

Da ich von dem DMU ausgehen muß, habe ich die Funktion "Zeige Physikalisch 0" mit dem Device "RAM:" gesperrt.

Logfile

Diese Funktion erlaubt es, ein Protokollfile auf einem beliebigen Laufwerk anzulegen. Alle Ausgaben auf dem Bildschirm (keine Requester) werden in dieses File geschrieben. Wenn Sie das Log-file wieder schliessen wollen, einfach ein 2.mal auf LOGFILE klicken. Ansonsten wird das Logfile automatisch beim Ende von VirusWorkshop geschlossen.

1.51 HDSUPPORT

Read, Write, Show physical cylinder 0:

There are lot of viruses hanging around which destroy the RigidDiskBlock of your HD. Why? They do not recognize that they do not use the "trackdisk.device". What happens, if they write using the "scsi.device" on the bootblock? They get the physical block of your device and destroy it. When using harddisks you surely know that the RDB is in the physical block 0. Your hd becomes unuseable. How good, if you saved the physical block 0. This function will do excatly this!

Read = Backup physical cylinder 0 to a safe disk.
Write = Restore physical cylinder 0.
Show = Comparable to the 'ASCII Dump' but you have more sectors to watch.

Especially the Read/Write parts of this routine should only be used, if you have not a special programm from your HD producer company which is surely better customized for your HD. BSC (Oktagon / ALF) is for example such a company which gives you an excellent tool to save your RidgidDiskBlock block!

List of some viruses, which can detroy the physical block 0:
-Crime92 1+2,Overkill,ByteBandit,Zenker1+2,Burn 1+2
and more...

Based on some quite crazy users, I had to prohibit the use of the function "Show physical 0" with the device "RAM:". (Vielen Dank Laserdance !)

Logfile

Do you want to have a logfile containing all actions of VW, which will be printed on the screen ? We want it. Simply start this option and select a filename. The logfile will be closed by starting again the logfile option or at the end of VirusWorkshop.

1.52 CRUNCHER

The following crunchers will be recognized:

(even some more but not listed)

PowerPacker 2.x
Imploder 1.0-3.1
Titanics Cruncher 1.1
TNM Cruncher 1.1
PowerPacker 4.1
PowerPacker 4.3b
DragPack 1.0
Master Cruncher 3.0 R
TurboSqueezer 8.0
CrunchMania 1.4 R/N
CrunchMania 1.6
Crunch O Matic 1.0 E
PP 3.0 Password
PP 4.0 Overlay/Lib
PP 4.0 Password/Lib
ByteKiller 2.0
CrunchMania 1.4 A/N
RSI Packer 1.4
Time Cruncher 1.7-2.2
Turtle Smasher 1.3
TetraPack 2.1
TetraPack 2.2
DefJam Cruncher 3.2
Defjam Cruncher 3.5 & 3.6
Crunch Master 1.0
MaxPacker 1.2
ReloKit 1.0
StoneCracker 2.70 K
StoneCracker 3.00
Super Cruncher 2.7
TryIt 1.01
TSBs Ultimate Packer 1.1b
Imploder 4.0
DMS files -1.12

PowerPacker 3.0
Imploder 4.0
Titanics Cruncher 1.2
PowerPacker 4.0
PowerPacker 4.2
PP 4.0 Library
DragPack 2.52
PackIt 1.0
Lib Imploded
CrunchMania 1.4 R/S
CrunchMania 1.8
PP 3.0 Overlayed
PP 4.0 Overlayed
PP 4.0 Password
Black&Decker 2.0
ByteKiller 3.0
High Pressure Cruncher
Master Cruncher 3.0 A
TFA Cruncher 1.54
Turtle Smasher 2.00
TetraPack 2.1 Pro
TetraPack 2.2 Pro
DefJam Cruncher 3.2 Pro
Compacker 4.2
HQC Cruncher 2.0
Mega Cruncher R
StoneCracker 2.70
StoneCracker 2.99
StoneCracker 3.10
Syncro Packer 4.6
Ultimate Cruncher 1.16
Imploder 1.0-3.1 P
LHA archives-1.42e
ZOOM files -5.4

Powerpacker Data Files	Skid Row Warper 2.0
Skid Row Warper 1.1	RAP!TOP!COP! V1.0-1.2
Crystal Warper 2.0ß	Phil Douglas Warper 2.0ß
N.O.M.A.D. Warper 1.3	N.O.M.A.D. Warper 5.1e

The power results mainly from the use of the faboulus "xfdmaster.Library" by Georg Hoermann. This fine piece of code is public domain. In the VirusWorkshop package is version 33.20 of the library included. Newer versions of the library bring you even more recognized crunchers.

This library is able to decrunch most above listed filetypes. I have included a function called "Decrunch" in the PREFERENCES menu to able/disable the decrunchroutines. If you have activatet this function every relocatible crunched file will be decrunched. Please note that decrunching will take some moments on slow 68000 AMIGAs .

Special note from Georg about the library and the library package:

This library and all documentation/include files are Freeware! Use it in your programs, spread it around the world, do whatever you want with it, but don't change or sell anything without asking him before. For bug reports/suggestions contact him at:

Georg Hoermann
Am Martinswinkel 16c
82467 Garmisch-Partenkirchen
GERMANY

If you use the decrunch.library in your own programs, please state in your documentation that it is written by Georg.

If anybody has the time and knowledge to write some 'C', Modula or whatever include files, send them to him and he'll release them together with the assembly include.

Special fileformats, which will be recognized:

Crunched File Protector 1.35 by Ikarus/Divide:

This is a special tool for PowerPacker 4 and Turbo Imploder files. It extends the first hunk to irritate the decrunching software. Thought as a protection against faked versions, this could be a danger because of the misuse. VirusWorkshop offers you the poss. to unlink the file and retest it.

TXT2Exe by Oliver Wagner:

This is a little tool, which creates from a normal textfile an executable file, which can be started from CLI/SHELL.

N.O.M.A.D. Warper 6.0 (Ixxy-TRSI version):

This is an enhanced version of the warper 5.1e, which supports XPK and other nice stuff.

N.O.M.A.D. Warper 5.1e:

This is a diskcompressing utilitie like DMS.It is a lot slower but it WARPS the tracks.If necessary, the tracks will be nibbled. I think it is a tool from crackers but it appeared on some german BBS and so I decided to include it.

There is a write included in this archiv...

Testlongwords: "Warp v1.1" Position: 0-7

N.O.M.A.D. Warper 1.3:

This is a diskcompressing utilitie like DMS.It is a lot slower but it WARPS the tracks.If necessary, the tracks will be nibbled. I think it is a tool from crackers but it appeared on some german BBS and so I decided to include it.

Testlongwords: "NOMADWAR" Position: 0-7

Prorunner V1.0 & V2.00:

Prorunner is a utilitie, which converts the original Protracker format in an own format, which can be replayed a lot faster. I had only 1 checkmark (the .SNT/SNT!) and therefore it can come to some misunderstandings.

Protracker:

All normal modules from Protracker 1.1-3.00 should be detected.

The support for the new fileformat from the Cryptoburners tracker (Protracker 3.0xb) will come, if I see the first module done with this tool.

Xlink 3.00:

This is a utilitie which enables the user to link 2 executable file together. A very fine tool. But imagine the following situation: One of the linked files contain a virus!

VirusWorkshop asks you if you want to delete Xlink files. If you want to be clever then do the following things:
1. Copy the XLINK file to a seperate disk and start the file. Then start the VirusWorkshop and look at the vectors. If the memory was clear before starting the Xlink file and now it is incorrect then you should clear the file because there could be a virus in it.

Such utilities should always contain a viruschecker, which checks the choosen files for linkviruses.

Comment 22.3.93.: The Dial2.8g Virus is a Xlink 3.00 file !!!

signed,
Markus Schmall

(23.03.1993)

1.53 FUTURE

Ideas for the future:

- A requester which cancels special directories from checking files (FONTS: ENV: etc.) Idea by Martin Spaltner ! THX !

Do you have a special thing which I could include ? An unknow patch or a new virus ? Simply write to me !

1.54 FUTURED

Ideen für die Zukunft:

-Eine Art Voreinsteller, so daß man einige Directories vom File-check ausgeschlossen werden können.

Wenn Sie weitere Ideen haben... Ich bin immer offen für sinnvolle Vorschläge !!!!

1.55 Vectors

Hi Jörg ! Nocheinmal tausend Dank für den Kontakt zu ...
Wir wissen, wer gemeint ist (ja, Knacko und Laser auch).
Speziellen Gruss an meinen Lehrmeister in Assembler auf dem
AMIGA !

Ich bin auf das neue Intro gespannt....

1.56 VHDK_G

Special thanks to all of you. Much special hellos go out to
Jan Andersen for his really great support. Thanks ! We will
meet in August‘95....

Hi to Jan Nielsen ! I will never forget this 2*Jan..Or was
it Jan*2 ?... Jan Nielsen and Jan Andersen should it be...

1.57 HELLOS

Special regards and greetings go to:

Ingo~Schmidt

Jörg~Wabbel

Virus~Help~Team~DK

Vasco~Steinmetz

Soenke~Freitag

J.Walker

Ixxy/TRSi

Bloodrock

Dave~de~Pauw

Andreas~Weyert~&~Lars~Bennecke

Blind~Guardian/TRSi

Georg~Hoermann
Rascal/HF Nice chats, talks etc. ↩
Hope to see
you soon.

Accuracy/Loons Thanks a lot for the spanish locale

	file.
Eckhard Brueggemann	Vielen Dank für die Unterstützung, die ganzen netten Talks, das Wochenede in Stade etc. Wir treffen uns mit Martin, ok ? Vielen Dank...
Edd Dumbill	For the great Heddley utility !
Thorsten Schaaps	Vielen Dank fuer den Arexx-Source.
Euronymous/TRSi	Danke für dir Warnung vor dem ConMan LoadWB Virus !
Pius Nippgen	Danke für den netten Brief. Ich kann Dich gut verstehen, daß es so nicht geht.
Ralf Thanner	Hallo Ralf ! Nettes Gespraech bei der Rainbow Party. Wenn ich Deine Adresse haette, wuerde ich mich melden... Viel Erfolg mit den Projekten...
Frank Mariak	Für den genialen Cybergraphics Treiber
Joachim Dort	Thanks for BETAtestings and your help and computer !!! (Das 9.Klasseanbaggersyndrom ist hochgradig ansteckend.)
Mike Voland	For all your support and hints... Viel Erfolg mit dem neuen Haus ! "Socke" ist ja wirklich niedlich.
Torben Danoe	For the translation of the VW locale files !
Tauno Pinni	For the swedish translation of the VW.Catalog Thanks a lot ! One day before release I recieved your letter...
Flemming Lindeblad	For the translation of VW.catalog

Kai Haseloh	Depack! ist wirklich gut ! Wieso soll ich das GUI optimieren ? Im Vergleich zu meinem alten "STIL" ist es doch schon ein großer Schritt in die richtige Richtung.
Martin Berndt	In Bezug auf Viruskiller haben wir ja absolut konträre Meinungen. Sonst bist Du ein richtig guter Programmierer. MultiCX ist wirklich sehr gut...

There's one person I DON'T want to thank:
---

* Erik Løvendahl Sørensen (you ALL surely know, why!?!)

1.58 GH

Danke für neue Viren, für die XfDMaster Library und für die Gespräche/Briefe und .....
VZ ist einer der besten Viruskiller derzeit.

1.59 BG

Hi Blind Guardian ! (Wenn ich nur Deinen Realnamen wuesste). Also vielen Dank fuer den Support. Der derzeit einzige TRSi Member, der mich unterstuetzt. Den DMS 2.13 Fake haette ich ohne Dich NIE! mehr bekommen. Viel Erfolg in TRSi und mit TRIP TO NOWHERE....

1.60 SDC2

Hi Oliver ! Danke für den schnellen Fix der Library. Ich teste jetzt wieder alle Files mit Deiner Lib. Wir sehen uns garantiert auf der Party. Es wird ja ein richtiges Familientreffen...

1.61 Osna

Hallo ! Die alte Osnabruecker Clique... Vielen Dank fuer den Support und die ganzen Meetings(Red Bull rulez).

Na, Andreas, was macht Deine Freundin ??????

1.62 LSD

Hi Dave ! The german post seems to forget some letters from me to you. I wrote you two times and no answer. Crazy. Are you still on AMIGA or pure consoles ? Greet Pazza from me ! Grapevine is cool !

1.63 An Ingo Schmidt:

Hi Ingo ! Vielen Dank für den wirklich großartigen Support und die ganzen Tips. Wenn Du nicht nur in Fernzone 3,von mir aus gesehen wohnen würdest, wäre es noch besser. Wenigstens die Telekom freut sich. Vielen Dank an meinen "Viruskiller" Vater !!!

Ohne Dich wären diverse Klippen im DOS nie von mir umschifft worden. Man denke nur an das Problem der ungueltigen Locks bzw. der Infodaten. Vielen Dank. Jetzt kann ich auch auf Eure Art Bier eingiessen...

1.64 An J.Walker:

Hi Mathias ! Schade, daß Du aufgehört hast. Trotzdem viel Erfolg mit Deinen Projekten. Es war eine gute Zeit mit Dir in TRSi (außerdem warst Du die einzige Person innerhalb von TRSi , die mir neue Viren ohne Aufforderung etc. zugeschickt hat!!!!).

1.65 Nextsys

Vielen Dank für Deinen ganzen Vorschläge. Ohne Dich würde VW anders aussehen. Viel Erfolg mit dem neuen Diskfile Device, dem Voxelspace Spiel auf unterster OS Basis und vor allen Dingen mit SpyDos !!! Ich will endlich eine Finalversion sehen ! Ähnliches wirst Du über den Prefseditor im VirusWOrkshop sagen ...

Comment 06.06.1994: Viel Erfolg im muendlichen ABI !

1.66 An Soenke Freytag:

Hi Sönke ! Vielen Dank für den Support und die gehaltvollen Msgs. im Z-Netz/Rechner/AMiga/Viren !!! Der Tag im VTC war eindrucksvoll. Zu dem Dark Avenger: Er ist polymorph, aber halt genau die andere Version !

1.67 Axnete

AmiXNet ist a network created between mailbox systems, which run under the fantastic AmiExpress mailbox system.

1.68 Kontakt-Adresse

Wie der Programmierer zu erreichen ist:

Wenn Sie Ideen, Fehlerbeschreibungen oder Viren haben, die VW nicht erkennt, dann setzen Sie sich bitte mit mir in Verbindung. Sie werden so schnell wie moeglich eine Antwort erhalten:

Markus Schmall
Katharinenstr. 17
31135 Hildesheim

+49 (0)177 2829402

oder

.....

Wenn Sie die aktuellste Version von VirusWorkshop erhalten wollen, dann schreiben Sie mir einfach. Bitte fuegen Sie einen frankierten Rueckumschlag bei und eine formatierte Diskette. Ich kann fuer Sie nicht Disketten oder fehlendes Porto bezahlen.

Achtung: Ich bin in keinster Weise an dem Austausch illegaler Programme interessiert. Ich habe immer wieder Aufforderungen mit eindeutigem Inhalt bekommen, die direkt in den Muelleimer wandern.

Die aktuellste Version von VirusWorkshop kann auf der PD Serie "TIME" der Firma APS Elektronic gefunden werden. Diese PD-Serie bekommt den Viruskiller IMMER DIREKT von mir, so daß schnellste Bearbeitung möglich ist...

VirusWorkshop sollte in aktuellen Versionen auf verschiedenen Mailboxen zu finden sein.

Das offizielle VirusWorkshop Support Board ist:

DALLAS BBS

USR V34 (FC) Dual Standard ++49[0]711588146

Dort finden Sie immer die aktuellsten Versionen diverser guter Viruskiller. Mein Username dort ist Flake. Wenn Sie Fragen etc.

haben, dann scheuen Sie sich nicht, mich ueber diese Mailbox anzuschreiben.

Andere lohnende Mailboxen sind:

Nirvana BBS

USR V34 FC Dual Standard ++49[0]511-9524227
V32 bis Node ++49[0]511-522809

Eine weitere sehr gute Mailbox ist die Box des Virus Test Centers der Universitaet Hamburg unter der Schirmherrschaft von Herrn Professor Brunnstein:

Tel.:++[0]4054715235 (V32bis modem)

Meine Kontakadressen ueber Netzwerke, wobei der Internet Account bevorzugt wird:

Flake@trsi.de

CU l8er,
Markus Schmall

Die Internet Adresse sollte eigentlich auch ueber FIDO und Z-Netz ansprechbar sein, denn es bestehen , soweit ich weiss, Gateways in das Netz an der UNI.

Tristar & Red Sector - The sleeping gods

1.69 Contact adress

How to contact the author:

If you have an idea, bugreport or a virus, which is not recognized, then please send it to me. You will get an answer as fast as possible. To contact me just write to:

Markus Schmall
Katharinenstr. 17
31135 Hildesheim

+49 (0)177 2829402
or

(this is private)

I am at this time mostly at home. Otherwise one of my parents is at home. It is nearly not possible that you reach nobody from us...

To get the latest version write me. I will send you then as soon as possible the latest version. Please include postage and lettercases! I cannot afford it to pay such things for you.

! ATTENTION !

I AM NOT INTERESTED IN ANY KIND OF SWAPPING ILLEGAL WARES!
I AM COMPLETELY LEGAL CODER!

The latest versions of the VirusWorkshop and DosTouch can be found on the TIME PD discs by A.P.S. Electronic.

You should find this viruskiller in several networks. If you are a sysop who wants to spread this piece, just contact me (I own an USR Courier DST V.34!).

This viruskiller will always be first uploaded to:

The official VirusWorkshop support mailbox is:

DALLAS BBS

USR V34 FC Dual Standard ++49[0]711588146

There you will find many new viruskillers and other interesting things. My useraccount is Flake. So, if you have any questions etc., then don't hesitate to call this great box.

Other very fine boards are

Nirvana BBS

USR V34 FC Dual Standard ++49[0]511522809

Virus Help Denmark BBS

Tel.: +45 46596867

USR DS 28.8

(Attention ! New number !)

Another very well mailbox is the mailbox from the Virus Test Center from the University of Hamburg. There you will find all actual viruskillers:

Tel.:++[0]4054715235 (V32bis modem)

You can find the VirusWorkshop in the following BBSs(a friend of me uploads the file to them):

- sorry, no special BBS this time...

My homepoint is: Flake@trsi.de (I read this account every day and you can expect to get the fastest answer from me there !)

If you have access to INTERNET, then try to reach me on:

"msch0091@rz.uni-hildesheim.de".

(You can write out of nearly every net to this adress!)

Routing Adressing
~~~~~~
Internet -> UNI Hi : msch0091@rz.uni-hildesheim.de

The contact via INTERNET is preferred, because the Z-Netz lacks sometimes and some PMs will be somewhere "forgotten"
~~~~~~

```
in the system. I wrote some messages in this  network, but
some of them are still not routed and this after 6 months.

VirusWorkshop  can be  found  on the TIME PD disks. At the
release day of VirusWorkshop it will be  mailed to  A.P.S.
Electronic !!


                                                CU l8er,
                                                      Markus Schmall


                                  Tristar & Red Sector - The sleeping gods
```

1.70 Hellos to Ixxy/TRSi

Hi Ixxy ! Ich bin ja echt auf Deine neue Frisur gespannt. Keine langen Haare mehr ? Nichts fuer ungut. Ich hoffe, dass wir uns bald mal wieder treffen...Cebit ? ... Und diesmal wieder ein VirusWorkshop release OHNE Verzoegerung...

1.71 LHA Checker - deutsch

```
Die LHA Archiv Untersuchfunktion:
---------------------------------

Diese Funktion ist ziemlich einfach implementiert.
Benötigt werden:


                sys:c/rename
                sys:c/delete
                sys:c/lha

und ein Assign mit dem Namen VWLHA:. Ich habe selbst
mir ein neues Directory auf der Festplatte erstellt
und es als VWLHA assigned:

Bsp: makedir dh0:WasWeissich
     assign  vwlha: dh0:wasweissich/

ACHTUNG ! Alle Dateien in diesem Directory werden
gelöscht bevor die Funktion arbeitet und nach
Abarbeitung werden auch alle Datein gelöscht. Nach-
dem das ausgeählte LHA Archiv entpackt wurde, wird
```

```
die Filechecker gestartet. Wenn dieser Vorgang ab-
geschlossen ist, wird der Benutzer gefragt, ob er
das Archiv wieder packen möchte. Wenn er diese
Frage mit "JA" beantwortet, wird er noch gefragt,
ob eine Sicherheitskopie des alten Archives gemacht
werden soll.

Auf diese Weise koennen sehr einfach LHA Archive
untersucht werden, was gerade Sysops etc. bestimmt
sehr zur Hilfe kommt.
```

1.72 LHA Checker- english

```
The LHA archiv checkroutine:
----------------------------

This function is implented on a quite simple way.

This function needs:

                sys:c/rename
                sys:c/delete
                sys:c/lha


and an assign with the name VWLHA:. I for myself have
created a subdirectory on my harddisc and have assigned
it to VWLHA:

E.G.: makedir dh0:WasWeissich
      assign  vwlha: dh0:wasweissich/


CAUTION: All files in this directory will be deleted
before starting this function and after the whole
process. After you have selected a archiv, it will
be tried to unpack it and the filechecker will be
started.

If this process is completed, the user will be asked,
if he wants to repack the archiv again. If you answer
with "YES", then you will be asked, if you want to
rename (backup) the original archiv.

In this way you can easily check LHA archives,
which can be very usefull for sysops etc.
```

1.73 Integrity_Checker

```
      Integrity-Checker in VirusWorkshop:
      -----------------------------------
```

Beginnend mit VirusWorkshop 5.2 werden Sie einen neuen Menupunkt
im "Misc Tools2" Menu finden. Wenn Sie diese Funktion starten, dann
wird ein Requester auftauchen, der Sie vor die folgende Möglichkeit
stellt:

1. Scan: Alle Dateien auf dem aktuellen Laufwerk werden geladen,
   ihre Laenge wird gesichert und eine Checksumme wird erstellt. Diese
   Daten werden in dem File "ram:integrity.vw" gespeichert. Warum
   gerade in diesem File in der RAMdisk ? Ganz einfach : Wuerde
   von Ihnen eine sehr grosse Festplatte gecheckt werden und
   VirusWorkshop wuerde alle Scanresultate immer auf Diskette
   schreiben, könnte es zu einer mechanischen Überbelastung kommen.

2. Compare: Ein Reuqester wird Sie auffordern, ein File mit den
   Scanresultaten anzugeben. Wenn dieses File validiert ist, dann
   wird VirusWorkshop mit seiner Arbeit beginnen, alle Dateien
   zu untersuchen.

   This should be quite easy to use (even for a beginner).

integrity=unveraendert, unmodifieziert, "die Integritaet"

Mögliche Fehlerquellen:

-die RAM Disk ist nicht vorhanden
-Sie versuchen Dateien anzusprechen, die nicht vorhanden sind bzw.
 deren Diskette nicht eingelegt ist.

1.74 Integrity_Checker

Integrity-Checker in VirusWorkshop:

Beginnend mit VirusWorkshop 5.2 werden Sie einen neuen Menupunkt
im "Misc Tools2" Menu finden. Wenn Sie diese Funktion starten, dann
wird ein Requester auftauchen, der Sie vor die folgende Möglichkeit
stellt:

1. Scan: Alle Dateien auf dem aktuellen Laufwerk werden geladen,
   ihre Laenge wird gesichert und eine Checksumme wird erstellt. Diese
   Daten werden in dem File "ram:integrity.vw" gespeichert. Warum
   gerade in diesem File in der RAMdisk ? Ganz einfach : Wuerde
   von Ihnen eine sehr grosse Festplatte gecheckt werden und
   VirusWorkshop wuerde alle Scanresultate immer auf Diskette
   schreiben, könnte es zu einer mechanischen Überbelastung kommen.

2. Compare: Ein Reuqester wird Sie auffordern, ein File mit den
   Scanresultaten anzugeben. Wenn dieses File validiert ist, dann
   wird VirusWorkshop mit seiner Arbeit beginnen, alle Dateien
   zu untersuchen.

```
         This should be quite easy to use (even for a beginner).


      integrity=unveraendert, unmodifieziert, "die Integritaet"


      Mögliche Fehlerquellen:

      -die RAM Disk ist nicht vorhanden
      -Sie versuchen Dateien anzusprechen, die nicht vorhanden sind bzw.
       deren Diskette nicht eingelegt ist.
```

1.75 Arexx_deutsch

```
Einführung zu dem Arexxport in VirusWorkshop:


Der Arexxport heisst VWPort und versteht derzeit folgende Befehle:


1.PACKMODE

  Als Rueckgabewert wird eine 20 ausgegeben, wenn die Entpackfunktion
  nicht aktiviert ist. Eine 21 wird zurückgegeben, wenn die Decrunch-
  funktion aktiviert ist. Gedacht ist dieses Kommando mehr oder weniger
  als Information für den Benutzer.


2. LFILE

  Syntax: "LFILE Filename"

  Ein LHA/LZX Archiv wird entpackt und auf Viren untersucht. Bei Befall
  wird das Archiv wieder neu gepackt, ansonsten bleibt das ursprüngliche
  Archiv intakt. Bitte lesen Sie auch die weiteren Informationen über
  die Behandlung von LHA/LZX Archive.

  Rückgabewert 1 bedeutet, daß ein Virus gefunden und geloescht wurde.
  Rückgabewert 15 bedeutet, daß es zu einem internen Fehler gekommen ist,
  der auf folgende Gründe zurückzuführen ist:

  - angegebener Filename war kein LHA Archiv
  - File nicht existent
  - kein VWLHA assign:
  - kein LHA-Archiver...


3. SFILE

  Syntax: "SFILE Filename"

  Ein ausführbares File wird auf Viren untersucht. Die Rückgabewerte
  entsprechen denen des LFILE Kommandos.
```

VirusWorkshop gibt Ihnen eine 20 zurück, wenn ein unbekanntes Kommando
an seinen Port geschickt wurde.

Bitte sehen Sie sich auch die mitgelieferten AREXX Skripte zum besseren
Verständniss an.

1.76 Arexx_english

Introduction to the Arexxport in VirusWorkshop:

The name of the Arexxport is VWPort and this port understands at the moment
the following commands:

1.PACKMODE

As returncode you will get a 20, if the decrunchfunction is not activated.
You get as a returncode a 21, if the decrunchfunction is activated. This
function is thought as information for the user.

2. LFILE

Syntax: "LFILE Filename"

A LHA/LZX will be unpacked and scanned for viruses. If a virus was
found, it will be removed and the archiv repacked. If nothing was
found, the archiv will be not repacked (not neccessary). Please read
the additional information concerning the LHA/LZX check. Thanks.

A returncode 1 means, that a virus was found and deleted.
A returncode 15 means, that someting went wrong during the LHA check.
Possible reasons are: No lha archiv, no lha archiver etc.

3. SFILE

Syntax: "SFILE Filename"

An executable files will be scanned for viruses. The returncodes are the
same as in the lfile command.

VirusWorkshop will give you back a 20, if an unknown command will be send to
the VWPort.

Please consult the supplied Arexx scripts to understand the stuff better.