

Virus_CheckerII

Alex van Niel

COLLABORATORS

	<i>TITLE :</i> Virus_CheckerII		
<i>ACTION</i>	<i>NAME</i>	<i>DATE</i>	<i>SIGNATURE</i>
WRITTEN BY	Alex van Niel	July 26, 2024	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

1	Virus_CheckerII	1
1.1	Virus_Checker II Help	1
1.2	important	2
1.3	Shareware Notice	2
1.4	Registration	3
1.5	Danish Registration	4
1.6	Presentation	5
1.7	Main Window	6
1.8	Command Line Options	7
1.9	Icon ToolTypes	9
1.10	Security	10
1.11	PGP Key servers	11
1.12	4eb9 Link Virus	13
1.13	Locale	14
1.14	How to install Virus_Checker II	14
1.15	Archives	15
1.16	AppIcon	15
1.17	Disclaimer	16
1.18	Author Info	17
1.19	Files	19
1.20	Arexx	20
1.21	Credits	22
1.22	Options	24
1.23	Watch	24
1.24	Scan	25
1.25	Quit	25
1.26	Option XFDMaster	25
1.27	Option UseWindow	25
1.28	Option IgnoreBB	25
1.29	Option Unpack	26

1.30 Option DFxBB	26
1.31 Option Scan	26
1.32 Option Capture	26
1.33 Option UseBBLib	26
1.34 Option DFxFull	27
1.35 Option	27
1.36 Option HotKey	27
1.37 Option TempDir	27
1.38 Option Save	27
1.39 Option CloseWind	28
1.40 Option ArexxScan Window	28
1.41 Option Start Iconified	28
1.42 Option AppIcon On	28
1.43 &	28
1.44 string	28
1.45 Add	29
1.46 Remove	29
1.47 CheckNow	29
1.48 Check	29
1.49 History	30
1.50 VectorShow	34
1.51 Format Protection Options	35
1.52 Archive Options	35
1.53 Future	37
1.54 UK Registration	38
1.55 VC II Related	39

Chapter 1

Virus_CheckerII

1.1 Virus_Checker II Help

Virus_Checker v7-v8.4, Copyright © 1990-1995 by John Veldthuis
 Virus_Checker II v1.1, Copyright © 1997/1998 by Alex van Niel

~Presentation~~~~~	What is Virus_Checker II
~Important~notes~~~~~	Please Read this
~Shareware~Notice~~~~~	Virus_Checker II is not free
~Registration~~~~~	Fill me out and mail me
~Danish Registration~~	Fill me out and mail me
UK Registration	How to register easy when you live in the UK
~Security/PGP~~~~~	How do I know this is not a virus
PGP Key Servers	How to get my public PGP key
~Main~Window~~~~~	Main Virus_Checker II window
~Command~Line~Options~	Start Virus_Checker II from SHELL
~Icon~ToolTypes~~~~~ ~	ToolTypes Virus_Checker II uses
~Workbench~AppIcon~~~~~	Drag and Drop checks
~Files~Needed~~~~~	Files required by Virus_Checker II
~Localization~~~~~	Yep Virus_Checker is locale aware
~Installing~~~~~	How to install Virus_Checker II
~\$4eb9~Link~Virus~~~~~	SPECIAL NOTE ON THIS VIRUS
~Archives ~~~~~~	Checking into Archives
~Arexx~Port~~~~~	Arexx commands
VC II Related how to get it	Virus_Checker II Related Addresses, where and ↔
~Disclaimer~~~~~	And now for something completely different
~Author~Info~~~~~	About the Author
~Credits~~~~~	Thanks Guys
~History~~~~~	How things got to here
To Do/Future	What will come and what great plans I have

1.2 important

Some important notes for Virus_Checker
=====

The old keyfile that was valid for versions 1.0 of Virus_CheckerII and 8.4 and down of Virus_Checker is NO LONGER VALID!

Some registered users have already received a new keyfile which unlocks the special features. They don't need to contact me.

The old keyfile is now considered a cracked/bad keyfile and is treated as such. You will be able to acces the Archive Options, but you won't be able to check into archives, so it won't do anything. If you are a registered user and don't have the new keyfile, please feel free to contact me. Already registered users can get a free update (excl. possible postage and package if not send through e-mail) from me personally. To do this, fill out the reg. form again with the data you send to John and if it has changed since then, also add the current valid data (in case you moved for instance).

If you would like to receive your keyfile through e-mail, then please also add you pgp public key, so I can encode it and send it to you as soon as possible.

Virus_Checker II will pick up all the files that it requires from at least 2 places. It will first try PROGDIR: then the alternative place. Virus_Checker will save any of the files it needs to back from where it read it from.

See Virus_Checker Files for details

Please send bug reports/suggestions/ideas/whatevers to pinkie@dds.nl

1.3 Shareware Notice

This program is SHAREWARE.

Virus_Checker II for me is mainly a hobby but it does cost quite a bit. Therefore I took the decision to make Virus_Checker II SHAREWARE.

The cost is a very small US\$20 or NFL 40. For this you get some key details that will unlock a few features in Virus_Checker II. The future key is only valid ←
from
VirusChecker II version 2.0 and up. If for some reason, hackers are able and willing to crack the key however, already registered users will have to get a new keyfile. This 'update' will be completely free (except for possible postage and package).

The best way to send this to me is in cash. I prefer NFL (dutch money) because I don't have to change that at the bank. EuroCheques are the only cheques I can accept since the bank here charges really much for foreign cheques (not euro)

If you send a cheque, please put dutch guilders (NFL) on it and not dollars, this will save me the currency change costs.

If you cannot send cash or eurocheques then please send a bank draft drawn on a major bank. I cannot accept postal money orders. Our banks will just not accept them.

For my e-mail/postal address refer to the Author~Info.
And please, include YOUR e-mail address if you send me letters.

If you are in a hurry to get your keyfile and have an internet e-mail address and have a PGP public key then e-mail me your public key and I can send the keyfile afap (as fast as possible :)) over the internet.

Please fill out the Registration form and mail it to me with payment Please make sure that name and address is clear as it takes ages sometimes to decypher some peoples scrawls.

1.4 Registration

```
*****  
**      Virus_Checker II Registration Form      **  
*****
```

Mail to: Alex van Niel
Billie Holiday straat 116
2551 WK Den Haag
Netherlands

First Name: _____ Last Name: _____

Street: _____

City: _____

State/Province: _____

Country: _____

Email: _____

Registration of Virus_Checker II will unlock a few features that are present in Virus_Checker II that will not work unless you have a key. At present this is the ability to check files inside archives, but will be expanded,

viruschecker is supposed to become a full online BBS virus checking tool and those features will be locked by a keyfile.

This key will only work under WB2.04 or better. When you register you will receive in the mail (or email if you have a PGP public key) a by me created keyfile which will for now be valid for most of the VirusChecker versions but will be updated from time to time. Updates are completely free for already registered users. This also means that current registered users using old keyfiles can get a new keyfile for free. Only condition is that you fill out the registration form again and send it to me.

The cost of the Shareware fee is US\$20, NL 40 or equivalent. By this I mean I can take other money as long as it is in notes. No coins will be accepted. Postal money orders are not accepted either due to our banks not taking them. Any bank drafts or eurocheques must be in US funds or Dutch funds. If you are not sure I can take your money, please consult with me first.

Signature

Date

1.5 Danish Registration

Virus Checker Registreringsformular

Ja, send mig straks mine personlige koder, saa jeg kan bruge Virus CheckerII fuldt ud.

Personlige data (disse data vil blive opbevaret paa elektronisk form af Virus Help Team Denmark, og Alex van Niel. De videregives IKKE).

FORNAVN : _____

EFTERNAVN : _____

GADE : _____

POSTNUMMER : _____

BY : _____

EMAIL (evt.) : _____

TLF. (evt.) : _____

Prisen er dkr. 140,-, som jeg vedlaegger paa check, eller i kontanter
(BEMAERK: Virus Help Team Denmark paatager sig intet ansvar for kontanter der
ikke er sendt anbefalet).

Leveringsform, afkryds venligst:

- ☐ Send mig koderne i et almindeligt brev.
- ☐ Send mig koderne til min Internetadresse (PGP kodet)
- ☐ Send mig koderne crash til min fidonetadresse (PGP kodet).

Koderne vil blive leveret saa hurtigt som muligt, men det kan tage op til 4
uger at behandle registreringen.

OBS!! Hvis koderne skal sendes via email vil brevet blive kodet med PGP,
saa send et netmail med din publickey (til enten hlau@scientist.com eller
2:237/30.2).

Jeg er inforstaaet med ovenstaaende samt at de tilsendte koder KUN er til
personligt brug.

Formularen sendes til:

Henrik Lauridsen
Baunebakkevej 4 1 th
2650 Hvidovre

1.6 Presentation

This piece of software is Shareware !

Virus_Checker II

Virus_Checker, Copyright (c) 1990-1995 by John~Veldthuis
Virus_Checker II, Copyright (c) 1997/1998 by Alex van Niel
=====
(pinkie@dds.nl)

Virus_Checker II is a program that can be used on any Amiga that is running
Workbench 2.04 or better. Versions BEFORE version 7.0 will run on any Amiga
regardless of the Workbench. Yep it should even work on 1.1

Virus_Checker II is designed to hunt out Amiga viri and kill them dead. It also
scans memory on startup and checks all suspect vectors. It also checks
certain memory locations every 2 seconds for infection. It is also possible
to use VirusChecker online with a BBS to check incoming archives IMMEDIATELY.
This can be done by using the Rexx port of Virus_Checker II in combination with
the extraction tool (DVCPlugin) which in combination with the Archive Options

MENUS

Project/File Scan

This menu will bring up the Scan Requester so that you can enter a file or directory name to scan for viri.

Project/Full Memory Check

This menu will cause Virus_Checker II to do another complete memory check. This is the same one that is done at start up.

Project/Vector Show

This menu will cause Virus_Checker II to open a scrollable window with information about the system vectors. See @{"Vector Show Options" link " ← VectorShow" 0} for more information.

Project/Save Config

This menu will cause Virus_Checker II to save it's current configuration to it's configure file.

Project/Stats

This menu just gives you some data on the disks checked, files scanned and viri found since it was started.

Project/About

This menu tells you what version you are using of different things.

Project/Quit

Causes Virus_Checker II to stop and remove itself from memory.

Window/Snapshot window

This menu takes a snapshot of Virus_Checker II's current window position and saves it to it's internal data table. If you then select Save Config then Virus_Checker II will open up in the state that you snapshotted it in.

1.8 Command Line Options

Command Line Options =====

Usage: Virus_Checker II U=UNPACKOFF/S,B=BOOTBLOCKLIB/S,N=NOWINDOW/S,
CBB=CHECKRADBB/S,XFD/S,STDOUT/S,AUTOSCAN/S,CX_POPKEY/K,
A=APPICONNAME/K,QUIT/S,D=DIR/M

Available options: -----

U=UNPACKOFF

This option turns off the unpacking of the archives.
This can be also turned off using the Options Window.

B=BOOTBLOCKLIB

Using this option will tell Virus_Checker II to use BootBlock.library to check for bootblock viri. There are many viri in this library that Virus_Checker II does not know about so it is best to leave this on all the time anyway.
This can also be changed in the Options Window

N=NOWINDOW

This overrides the normal Virus_Checker II options and causes Virus_Checker II to run without opening it's window
This option can be set in the Options Window and saved

CBB=CHECKRADBB

This option makes Virus_Checker II check the RAD: bootblock for any viri. RAD: is a normal disk and can be infected as well.

XFD

This option turns on XFDMaster.library checking. It handles crunched files as well

STDOUT

This option works in tandem with the D=DIR/M keyword. If you give this option then Virus_Checker II will output anything it would normally display through a requester out through the shell it was started from. This includes virus information and error messages.

AUTOSCAN

This option affects what happens when Virus_Checker II gets a message from AmigaDOS that a file or directory has been changed. If this option is given then Virus_Checker II will automatically scan the file/dir before telling you that it changed.
This option can be changed in the Option Window

CX_POPKEY

Using this you can tell Virus_Checker II which key you wish to use to pop up the interface.

A=APPICONNAME

Using this you can tell Virus_Checker II what to use as a name for it's AppIcon

QUIT

This option can be used to make an already running Virus_Checker II quit

DIR

If you supply a directory or file using this option then Virus_Checker II will start scanning it as soon as it has started up.

1.9 Icon ToolTypes

Workbench ToolTypes
=====

Virus_Checker II can also be started from Workbench either through it's icon or in the WBStartup drawer. In this case Virus_Checker II will then get it's commands through icon ToolTypes.

All of the ToolTypes are already in the Virus_Checker II.info file. They have been disabled (except 1) by putting a () around them. To enable a ToolType simply remove the () and save it.

ToolTypes available are

DONOTWAIT

This is a Workbench ToolType and is required to be left enabled so that Workbench does not wait for Virus_Checker II to finish.

UNPACKOFF

This option turns off the unpacking of archives.
This can be also turned off using the Options Window.

BOOTBLOCKLIB

Using this option will tell Virus_Checker II to use BootBlock.library to check for bootblock viri. There are many viri in this library that Virus_Checker II does not know about so it is best to leave this on all the time anyway.
This can also be changed in the Options Window

NOWINDOW

This overrides the normal Virus_Checker II options and causes Virus_Checker II to run without opening it's window
This option can be set in the Options Window and saved

XFD

This turns on xfdmaster.library which handles uncrunching packed files

CHECKRADBB

This option makes Virus_Checker II check the RAD: bootblock for any viri. RAD: is a normal disk and can be infected as well.

AUTOSCAN

This option affects what happens when Virus_Checker II gets a message from AmigaDOS that a file or directory has been changed. If this option is given then Virus_Checker II will automatically scan the file/dir before telling you that it changed.

This option can be changed in the Option Window

CX_POPKEY

Using this you can tell Virus_Checker II which key you wish to use to pop up the interface.

APPICONNAME

Using this you can tell Virus_Checker II what to use as a name for it's AppIcon

QUIT

This tells Virus_Checker II to preform it's checks and quit as soon as it is done instead of hanging around.

DIR

If you supply a directory or file using this option then Virus_Checker II will start scanning it as soon as it has started up.

1.10 Security

Security/PGP

=====

All versions of Virus_Checker II since 6.44 have PGP sig files in the archive. This enables pgp to check that the file is in fact the same one I released.

Below you will find my signed public key. Save this to a file and then enter pgp <filename> to add it to your keyring. Follow the PGP instructions to add it.

If you do not trust this key (it can be substituted by someone) then get my current key from one of the pgp key servers
Or from one of the UBS bulletin systems in the Netherlands. You can always get my pgp from me personally through e-mail.

To check that the signature matches the file simply do
PGP <filename>.sig <filename>
PGP will warn you if the signature does not match the file.

An example of this is a the hoax version of 6.6 which quick formats drives. If you had done the test above it would have told you it was fake.

Virus_Checker II also has it's own internal checking for changes as well. Again this is not 100% but guards against the simple changing of version numbers. It also means it takes a better hacker to change the checksums.

Virus_Checker II will warn you of both checksum errors on itself and on the file VirusChecker.brain which holds the most recent virus recog and removing routines.

Public Key details:

Type	Bits/KeyID	Date	User ID
pub	1024/F47EFCF1	1997/12/25	Alex M. H. van Niel <pinkie@dds.nl>

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: 2.6.3i

Comment: Requires PGP version 2.6 or later.

```
mQCNAzSiq38AAAEAAK6uPZPDGxhgKfZqIbFWstCt5QsSRQGLlF++E/rlAbWWWaip
a8vSfQDcy96+QOcmFMWIKL58YJislwZj06Fenw+8WrDsPcizWsSORX+8h8opjqop
R3o0l33uI4EnmczpyjI8GhA75D46fHiI1KyZrarBKfdmUXHSP4GFUWH0fvzxAAUR
tCNBbGV4IE0uIEguIHZhbiBOaWVsIDxwaW5raWVAZGRzLm5sPokAlQMFEDSiq4CB
hVFh9H788QEB87AD/0YTqzc7JhUH05Ll50kHciep8keTg893xe+zAMNhB9ssa9yM
NMXZ+GYQ3mzzZTLCB/9E8E542KVLmZ5Cevdb/nIlKJyR4CUuWjQo7BnUuBnESbLA
vK1M0Bfu3rEkKUY786ZupzBMNEjA2cWyq8szApPDbo9bLw3AtTDKcCPDrQkD
=bxon
```

-----END PGP PUBLIC KEY BLOCK-----

1.11 PGP Key servers

PGP Public Keyservers

There are PGP public key servers which allow one to exchange public keys running through the Internet and UUCP mail systems.

NOTE!

This service is NOT supported in any way whatsoever by the schools or organizations on which these servers run. It is here only to help transfer keys between PGP users. It does NOT attempt to guarantee that a key is a valid key; use the signators on a key for that kind of security. This service can be discontinued at any time without prior notification.

Each keyserver processes requests in the form of mail messages. The commands for the server are entered on the Subject: line.

```
To: pgp-public-keys@pgp.mit.edu
From: johndoe@some.site.edu
Subject: help
```

Sending your key to ONE server is enough. After it processes your key, it will forward your add request to other servers automatically.

For example, to add your key to the keyserver, or to update your key if it is already there, send a message similar to the following to any server:

To: pgp-public-keys@pgp.mit.edu
 From: johndoe@some.site.edu
 Subject: add

-----BEGIN PGP PUBLIC KEY BLOCK-----
 Version: 2.6.2i

<blah blah blah>
 -----END PGP PUBLIC KEY BLOCK-----

COMPROMISED KEYS: Create a Key Revocation Certificate (read the PGP docs on how to do that) and mail your key to the server once again, with the ADD command.

Valid commands are:

Command	Message body contains
ADD	Your PGP public key (key to add is body of msg) (-ka)
INDEX	List all PGP keys the server knows about (-kv)
VERBOSE INDEX	List all PGP keys, verbose format (-kvv)
GET	Get the whole public key ring (-kxa *)
GET <userid>	Get just that one key (-kxa <userid>)
MGET <userid>	Get all keys which match <userid>
LAST <n>	Get all keys uploaded during last <n> days

Examples for the MGET command:

MGET michael	Gets all keys which have "michael" in them
MGET iastate	All keys which contain "iastate"
MGET 0AF605A5 683A738B	Those two keyids

If you wish to get the entire key ring and have access to FTP, it would be a lot more efficient to use FTP rather than e-mail. Using e-mail, the entire key ring can generate a many part message, which you will have to reconstruct into a single file before adding it to your key ring.

As of 21-Apr-95, these sites are running this system:

pgp-public-keys@pgp.mit.edu
 Derek Atkins <warlord@mit.edu>

pgp-public-keys@pgp.iastate.edu
 Michael Graff <explorer@iastate.edu>

pgp-public-keys@burn.ucsd.edu
 Andy Howard <ahoward@ucsd.edu>

pgp-public-keys@fbihh.informatik.uni-hamburg.de
 Vesselin V. Bontchev <bontchev@fbihh.informatik.uni-hamburg.de>

public-key-server@martigny.ai.mit.edu
 Brian A. LaMacchia <public-key-server-request@martigny.ai.mit.edu>

pgp-public-keys@pgp.ox.ac.uk
Paul Leyland <pcl@ox.ac.uk>

pgp-public-keys@dsi.unimi.it
David Vincenzetti <vince@dsi.unimi.it>

pgp-public-keys@kub.nl
Teun Nijssen <teun@kub.nl>

pgp-public-keys@ext221.sra.co.jp
Hironobu Suzuki <hironobu@sra.co.jp>

pgp-public-keys@sw.oz.au
Jeremy Fitzhardinge <jeremy@sw.oz.au>

pgp-public-keys@kiae.su
<blaster@rd.relcom.msk.su>

pgp-public-keys@srce.hr
Cedomir Igaly <cigaly@srce.hr>

pgp-public-keys@pgp.pipex.net
Mark Turner <markt@pipex.net>

Sites accessible via WWW:

<http://martigny.ai.mit.edu/~bal/pks-toplev.html>
<http://ibd.ar.com/PublicKeys.html>

Key server keyrings accessible via FTP:

<ftp://pgp.iastate.edu/pub/pgp/public-keys.pgp>
<ftp://pgp.mit.edu/pub/keys/public-keys.pgp>
<ftp://burn.ucsd.edu/Crypto/public-keys.pgp>
<ftp://alex.sp.cs.cmu.edu/links/security/pubring.pgp>
<ftp://ftp.informatik.uni-hamburg.de/pub/virus/misc/pubkring.pgp>
<ftp://ftp.dsi.unimi.it/pub/security/crypt/PGP/public-keys.pgp>

1.12 4eb9 Link Virus

Possible \$4eb9 Link Virus
=====

This is a special check.

It warns you of a possible virus. The current practice in viri is to use a normal program of some fame, link in a virus and then call it something new and better. The lzx, dopus, etc fakes are all examples of this.

When you get this message come up it does not mean that the program is a virus but to be safe be extremely careful with it. Write protect all drives, switch off the computer for at least 30 seconds after you have finished running the program.

1.13 Locale

Localization =====

Virus_Checker II is now localized and about 146 odd text strings can be altered. If you wish to translate these strings into another language then please contact me and I will send the information over to you.

Locale already done are

Nederlands	
Danish	
Swedish	Not Available Yet for Virus_CheckerII v1.1+
Norwegian	
German	
Serbian	Not Available Yet
Italian	Not Available Yet
French	
Spanish	Not Available Yet
Portuguese	Not Available Yet

If you plan to translate any of the strings, please contact me first so I can tell you if someone is already on this project and if not, to receive the latest ↵
catalog

information. If you have translated the catalog, please send at least the .ct file (translated file) to me. If you are able to compile the catalog, feel free to do so. Be aware that I have from version 1.1 started at 1.00 with the catalog since a lot has changed and the catalog had not been changed dramatically. Now it has and the catalog also should be called Virus_CheckerII.catalog with at least version ↵
1.00.

Do NOT! rename the old Virus_Checker.catalog to Virus_CheckerII.catalog and change ↵
the

version string, since side-effects could occur from strange enforcer hits to hard crashes which might scare even the most advanced users.

1.14 How to install Virus_Checker II

Installing Virus_Checker II =====

Virus_Checker II comes with it's own installer script. This installs Virus_Checker II onto the disk of your choice. It then asks where you want to run it from. The choices are S:\User-Startup, SYS:\WBStartup or Manually. It does NOT have to move files around anymore, it uses a project icon to start Virus_CheckerII from WBStartup.

I have heard of some complaints about this script, if someone has problems with the script, please notify me KINDLY of this fact. I heard from John that some people acted very violently through e-mail about stuff not working. Remember that programmers are people too and that every piece of software can have bugs or problems.

Though, a lot of problems that have been occurring have been fixed now.

1.15 Archives

Checking into Archives =====

This option is only possible if you are registered. Once registered you can get Virus_Checker II to look into these files.

Virus_Checker II can not (yet) remove any viri that are in the files but will warn you. When it finds one it will give a special out to the Scan window or the Arexx variables in the format

Lhafile.lha = SCA Virus

The Lhafile.lha is the filename of the infected archive, which file is infected is shown in the requester. This may be refined in the future.

You can now, with the help of the Archive Options window, have Virus_CheckerII check inside EVERY archive you desire. For now a few restrictions apply to the addition of new types. LHA and LZX archives are really easy so they have been added by default although they can be removed. Restrictions occur in the form of the command which is started to unpack an archive. You HAVE to have two %s wildcards in the command string and the first is always the wildcard that is replaced with the location and name of the archive. The second is always the wildcard that is replaced with the name of the destination directory. This might not seem like a problem, it does create one when handling ZIP archives. My version of UnZip unarchives the archive to the current directory and only accepts the archive name (not the destination directory). You can however work around this by making a script and giving Virus_CheckerII what it wants.

in the future I will probably add a example script and make the wildcards position independent by using %f %p but this is NOT the case at the moment.

1.16 AppIcon

Virus_Checker II AppIcon =====

If Workbench is running when Virus_Checker II starts up it will put an Application Icon on the main Workbench Window. The reason for this AppIcon is for Workbench users who want to check files. Simply select the files/dirs you want to check, then drag them over to the Virus_Checker II AppIcon and drop them on it. Virus_Checker II will immediately start checking those things dropped on it.

*****NOTE*****

If Virus_Checker II finds a file called Virus_Checker II_AppIcon.info in it's PROGDIR: then it will use this icon for the AppIcon instead of it's

internal default one.

*****NOTE*****

Included in this archive you will also find a small collection of NewIcons, these Icons have especially been designed for Virus_Checker II by Lyle Zapato, he holds the complete copyright of these icons. You will find, next to a few drawers and a few main executable icons, two AppIcons in NewIcon style.

1.17 Disclaimer

Virus_Checker is (c) Copyright 1990-1995
by John Veldthuis, all rights reserved.

Virus_Checker II is (c) Copyright 1997/1998
by Alex van Niel, all rights reserved.

Any possesor of this version "Virus_Checker II" for the Amiga is hereby granted a non-exclusive license permitting its use and/or redistribution, subject to the following terms and conditions.

Permission is hereby granted to freely redistribute this version of "Virus_Checker II" via electronic bulletin board systems (BBS's), freely redistributable disk collections (such as provided by Fred Fish), service bureaus (BiX, GENie, CompuServe, etc), and networks such as USENET, BITNET, and Internet, provided that such distribution includes this unmodified License, and all of the documentation files (README and .doc files), in addition to the executable, and with all copyright notices intact. Access to the source code must also be available and allowed.

This archive may be freely redistributed, but only in totally unchanged state, i.e. no files can be added, deleted, modified etc. All copyright notices in the program and its documentation must remain on their places. Also ".displayme" and other files, usually with "wonderful" ANSI graphics, so obvious at various BBS's, cannot be added.

Without prior written permission from the author, it is prohibited to sell or otherwise convey this version of "Virus_Checker II" for monetary or other forms of compensation, other than the customary service and/or duplication fees as may be charged by the distribution mechanisms identified above.

It is further prohibited, without prior written permission from the author, to include this version of "Virus_Checker II" in whole or in part, in the distribution of any commercial hardware or software package, or component thereof.

This version of "Virus_Checker II" is provided "as is", without express or implied warranty. The author makes no claim or representation about the suitability of this software for any purpose.

The author disclaims any and all warranties with regard to this

software, including all implied warranties of merchantability and fitness. In no event shall the author be liable for any special, indirect, or consequential damages, or any damages whatsoever resulting from loss of use, data, or profits, whether in an action of contract, negligence, or other tortious action, arising out of or in connection with the use or performance of this software.

AmigaGuide, AmigaGuide.info, amigaguide.library, WDisplay, WDisplay.info
(c) Copyright 1992 Commodore-Amiga, Inc. All Rights Reserved.
Reproduced and distributed under license from Commodore.

AMIGAGUIDE SOFTWARE IS PROVIDED "AS-IS" AND SUBJECT TO CHANGE;
NO WARRANTIES ARE MADE. ALL USE IS AT YOUR OWN RISK. NO LIABILITY
OR RESPONSIBILITY IS ASSUMED.

1.18 Author Info

Here is, for fast reference, how to contact me, below I will tell something about myself and then some:

Snail mail:

Alex van Niel
Billie Holiday str. 116
2551 WK Den Haag
Netherlands

Phone: +31-(0)70-3682789

UUCP/Internet:

pinkie@dds.nl

Well, it all started back then. When I was merely 8 years old and my dear ol' dad bought his first and last Amiga (who can blame the damned and condemn the fool? I know better after having been touched by the PC and Mac... I RAN to the Amiga :)) which was the Amiga 1000 which then was shipped with the 1.1 kickstart. Now that was real cool, we had had a c64 before but now we could use icons and press them and multitask and wow and so on.

Well, a new world opened itself up and it did not take long before I was charmed by this delightfull electronical woman and had me so wound up around her finger that I learned English really fast. Like: say, Alex, what the hell are you doing? Shouldn't you be studying English or something like your other 10/11 year old classmates? Er, well miss, I have already finished. Say WHAT?... Er... well, go play then.. And I played a lot back then :) Anyway, basic was IT you know back then for me I could not wish for more. Although playing Larry (which kid didn't? :)) and for 3 years SpaceQuest 1 (hey, you can't be a fast learner in EVERY field :)), I realised I wanted to do the same, but with basic? Well, that gave me some disadvantages since AmigaBasic was the only shit I knew and assembler was something geniuses used. So I started making ascii games (damn, were they UGLY!) anyway, that

was not enough so I bought Amos Classic a few years later (through a Magazine) and created some nice thingies, but GFX (strangely enough) in the computer I could not create (although I am studying animation right now which has something to do with that :)).

I somewhere got to know dudes from AGABBS. I started with a simple tool: AgaPoll. This tool would make it possible for MaxsBBS users (which I used at that time) and sysops to have MaxsBBS use an external mailer to call out and send it's mail. From there a lot of products followed, starting in Hisoft Basic which could be compiled but was slow, to programs in Amiga_E. Some have seen the public, some have seen a few systems and some have not even seen the light (my computer is very dark :)). Not much later when I was working on DevilCheck and LiquidStyler, I realised that I had to buy Amiga_E because the demo version which could handle up to 32k source files could not handle my code anymore (i had a some what old registered version which I got with a magazine but things get outdated and upgraded and bugfixed), so I bought it and was happily amused to see that my huge DVC code was compiled succesfully. However DevilCheck did not receive lot's of response so I lost my interest in that project (as had happened with a lot of other products) especially since most of the stuff I wanted in, myself, had been put in already.

The DayDream BBS had been sold and the new author contacted me since something that I had created apparently had reached him (I had by then created a few DayDream BBS doors) and so I offered to help him. He said he could use some help in the Fidonet area since he had no idea what to do with this whatsoever. I myself was connected to a lot of networks at that time and so started to recode the DreamToss utility which handled importing and exporting of fidonet-compatible mail-packets since the old util had not been updated since the stone-age and a lot of bugs were still in there. I did not know anything about assembler at the time and since DreamToss was written in Asm I just HAD to recode it. Next to the fact that there were nearly NO comments in it. I realise now, that I might be able to figure it out at present (viri don't come with handy comments you know :)) but back then I had no clue. Well, I had been extremely active at school and with my hobby but two years ago this all changed. Things started to get really busy at our school. In the first year I had already had the pleasure of experiencing the pressure that comes with a deadline. 12 or 16 hour days were very common and two years ago this started again right after the summer vacation when I and a friend of mine started to animate two animations for the KRO (television station here in the Netherlands) not at the same time but had a deadline set at 3 weeks from the starting date.

Well, this resulted in neglections of my projects and after this busy period, I had to recode a lot of DevilCheck and complete recode of TicMover (a tic file manager for a.o. DayDream BBS) since I forgot what most of the stuff did. TicMover had been finished but again no reaction, same as with the new update of DevilCheck which got a new feature and some bugfixes. Well, DreamToss was going very well but after a while I got bored with it since I could not fix a lot of problems occuring as a result of the difficult structure of fidonet stuff. Then last year Jan Andersen contacted Cor de Bruin who had heard fom us apparently and asked if we could create a new VHT here in the Netherlands adn if we could supply a coder.

Well, we were glad to help and a coder was no problem. I gave ALL the code of DreamToss as well as ALL research material (5 mb or so) to Theofiel, a friend of again a new coder of DayDream BBS who had been waiting for the

new DreamToss for a long time now. So this project I bounced and after ditching some other stuff I started doing some research on Assembler and started looking at some assembler stuff. At first I did not understand anything but as the days and weeks went by, I grew in to it and in (I guess) 3 months I learned myself to code in Assembler. Well, a little bit. When I got the Virus_Checker code I still did not understand a lot of it but after studying most of the things became apparent. Jaap v.d. Bos helped me a lot especially in mastering stuff on the binary level, but most of it I had to do myself. I still don't understand everything and I learn a lot each day as I go through the code and create a new feature (or bug, or both :)) which causes the compiler to scream for longer jumps and causes me to go through the code again. But I am learning and with your help, I can become an experienced assembler coder.

1.19 Files

Files "required" by Virus_Checker II and where they hide
=====

Virus_Checker II needs quite a few other files to function.

xfdmaster.library

This library is used to uncrunch packed files. If you want to use it then it must be in LIBS: as well. Also needed in LIBS: is the sub-directory XFD. This is where some of the decrunchers are held.

BootBlock.library

This library must also go into LIBS: it is used to check bootblocks of disks. See Bootblock.brain as well

BootBlock.brain

This file is used with BootBlock.library and must go into the L: directory to be of use.

Virus_Checker.config

This holds the configuration data for Virus_Checker II. Once saved Virus_Checker II reads it on startup and sets it self up the way you tell it to. This file can be in one of 2 places. PROGDIR: or S:.. Virus_Checker II knows where it loaded it from and will save it back there when told to. If the file does not exist at all and you save it it will be placed into PROGDIR:

Virus_Checker.watch

This file is a text file and can be changed with just a normal text editor. It holds the names of the files/directories being watched for changes. This file does NOT have to be present for Virus_CheckerII to run. This file will be in either PROGDIR: or S: Again Virus_Checker II knows where it loaded it from and will save it there. If it did not exist then it is saved to PROGDIR:

Virus_Checker.check

This file is a plain textfile and can be changed with just a normal text editor. It holds the names of the files/directories beeing checked for virus upon start-up. This file does NOT have to be present for Virus_CheckerII to run. This file will be in either PROGDIR: or S: Again Virus_Checker II knows where it loaded it from and will save it there. If it did not exist then it is saved to PROGDIR:

Virus_Checker.Arc

This file contains by default the LHA, LZX and ZIP specifications needed and used by the archive checking of Virus_CheckerII and will contain all future specifications of other archivers you add to it. This file is NOT a plain textfile, it also contains binary and should NOT be edited manually! This file also doesn't have to be present for Virus_CheckerII to run, but if not found or found empty, Archive CHecking will not be possible. This file will be in either PROGDIR: or S: Again Virus_Checker II knows where it loaded it from and will save it there. If it did not exist then it is saved to PROGDIR:

VirusChecker.brain

This file contains the latest bootblock, link and file virus recognition streams, routines and removal codes. In fact, this file will probably be updated the most so that one does not have to download the complete archive everytime as is the case with some major viruskillers. This file should be put in either L: or PROGDIR:

VCBrain

This file is found in PROGDIR: or s: and holds the Bootblocks learned

Virus_Checker.key

This is the keyfile for Virus_Checker II and you should only have one of these if you have registered. It can be in one of 3 places. PROGDIR:, The directory pointed to by the ENV: variable KEYPATH or in S:

1.20 Arexx

Virus_Checker II Arexx commands
=====

Virus_Checker II does have an Arexx port and the name of the port is Virus_CheckerII. With this port you can get Virus_Checker II to do things from external programs. Commands supported so far are

QUIT

eg. address 'Virus_CheckerII' 'quit'

This causes Virus_CheckerII to shut down and quit

RELOADBRAIN

eg address 'Virus_CheckerII' 'reloadbrain'

This will cause Virus_Checker II to reload it's brain file. With this command you can update the brain and get Virus_Checker II to reload it without having to get Virus_Checker II to stop

SCAN

eg address 'Virus_CheckerII' 'scan filename'

This command causes Virus_Checker II to go out and scan the file or directory given. All requesters will be turned off so it can be used un-attended. The get the results back to the program Virus_Checker II sets some ARexx variables. These are a stem variable called VCHECK

VCHECK.0.0 holds how many viri where found. 0 = none.

VCHECK.i.1 holds the file names of the files infected

VCHECK.i.2 holds the name of the virus that infected the file

for example if Virus_Checker II found 2 files infected.

1. SYS:C/LIST infected with the SCA virus

2. SYS:WBStartup/runme infected with the Saddam virus and

SYS: was scanned the results would be

VCHECK.0.0 = 2

VCHECK.1.1 = SYS:C/LIST

VCHECK.1.2 = SCA

VCHECK.2.1 = SYS:WBStartup/runme

VCHECK.2.2 = Saddam

NOTIFYWATCH

eg address 'Virus_CheckerII' 'NOTIFYWATCH password'

This command and the next are very special. They work in conjunction with the file watch list. Whenever Virus_Checker II gets a signal that a file or directory that it is watching has changed it will warn you. If you have Autoscan turned on and give this command to Virus_Checker II it will report to you the results. The command will not return to you until something has happened and that is why the following command is for.

If you need to cancel the notifywatch then you will need to use the following command to get it to release your script.

This command is of ideal use for BBS systems. You could set Virus_Checker II to watch your uploads: directory and when a user uploads a file it will scan it and return the results to you.

An example is

```
/* Notifywatch example */
```

```

options results
address 'Virus_CheckerII' 'NOTIFYWATCH Mypassword'
if VCHECK.0.0 = 0 then do
    say 'No viruses found in scan'
    exit
end
say 'Viruses found: ='VCHECK.0.0
do i o 1 to VCHECK.0.0
    say 'Filename was 'VCHECK.i.1' and virus was 'VCHECK.i.2
end
exit

```

STOPNOTIFYWATCH

eg. address 'Virus_CheckerII' 'STOPNOTIFYWATCH Mypassword'

This command will free a watch started by the NOTIFYWATCH command. You only need to give it the password given in the command above. You will need to do it from a separate script as the other one will be waiting for the return still.

NOTE: The password is case sensitive and needs to match the one given in the NOTIFYWATCH command

1.21 Credits

CREDITS

=====

My thanks go out to...

Georg Hörmann	For the inclusion of xfdmaster.library. Also, I looked at the vector show of VirusZ II and used the layout in my own program to setup a Vector Show routine. The ROUTINES however are 100% mine!
Leo Davidson	For Arexx script for use with Virus_Checker II and DOpus 5
ARexx	Developed on an Amiga 1000 and is a 100% Amiga product.
Jan Andersen	For sending all those new viruses and helping me get information everywhere. For getting Macro68 for me, sending the manual of Macro68, getting translators for the catalogs, finding bugs, checking infections and recognitions and lots and lots more..
Dave Jones	For sending the removal and recognition code of: <ul style="list-style-type: none"> - ZIB virus - BOKOR 1.01/1.05/1.06/1.1 Information and help on the Happy New Year 96 virus. Help with the ShortenHunk code for removing viri from Hunks and lots more.
Michael Knoke	For allowing me to have and use of his FormatProtection

routines which were taken from his great program:
Master Control Program

Dave Dustin Sorry that I forgot you the previous time,
 90 percent of all my thanks go out to you offcourse for donating
 the VirusChecker source to the Virus Help Team DK. If it wasn't
 for you, VirusChecker would still be a two years old outdated
 virus hunting utility. So please accept my apologies for ←
 forgetting
 I won't pretend to have a lot of reasons, I just forgot.

John Veldthuis Offcourse, for creating VirusChecker and supporting me with a lot
 of help and providing all the data I needed, especially for his ←
 help
 with Macro68 and the includes

Jan v/d Baard For creating BGUI.library which gives VirusChecker it's great
 easy to use interface (although some think otherwise)

Heiner Schneegold
 For help with HitchHiker 2.01, ZIB link virus and a few hints and
 tips.

Locale translations

Nederlands	Jan Hendrik Lots, Updated by Alex van Niel
Danish	Jan Andersen
Swedish	Fredrik Ismyren
Norwegian	Helge Syre
German	Dirk Stoecker
Serbian	Petar Cuckovic
Italian	Giacomo Magnini
French	Didier Giron
Spanish	Ricardo Fitzgerald
Portuguese	Ricardo Fitzgerald

All other catalogs will follow soon (I hope :))

And especially to my Beta Testers who put up with me everytime.
In no particular order

Lars Kristensen
Torben Danoe
Jim
Jan Andersen
Perry van Haastrecht
Michel Beij
Willem van Dijk
Remko Wiersma
Sieger Meerenboer
Henrik Lauridsen
Bastiaan Bakker

And further to all registered users for their loyalty and everybody I forgot...

Alex van Niel

```
|
|      ~~Add~~~   ~~~Remove~~~   ~~Close~Window~~   |
|
|-----|
```

1.24 Scan

```
Scan Files
=====
```

Clicking on this button will bring up the ASL Requester. You can then select a drive/directory/file to check for viri.

Clicking on cancel will cause the scan to be aborted.

Click on Okay once you have selected what you want scanned.

1.25 Quit

```
Quit
=====
```

Pretty obvious what this button does

1.26 Option XFDMaster

```
XFDMaster
```

Turning this Checkbox gadget on will cause Virus_Checker II to use the xfdmaster.library. This library is used to uncrunch files that are packed to save space. A virus could be packed inside one of these files.

1.27 Option UseWindow

```
Use Window
```

Setting this option causes Virus_Checker II to open it's main window when it starts up. With it off the window will not open

1.28 Option IgnoreBB

Ignore BB Read Error

By turning this Checkbox gadget on it will tell Virus_Checker II to ignore putting up a requester when it can't read a BootBlock from a disk. This is extremely handy if you use MSDos disks as Virus_Checker II cannot read them normally

1.29 Option Unpack

Unpack & Check into Archives

Turning this Checkbox gadget on/off causes Virus_Checker II to unpack archives which have been specified by using the Archive Options window and automatically check inside for viruses. This option is only active when you are a registered user.

1.30 Option DFxBB

Check DFx Bootblock

Selecting these Checkbox gadgets tells Virus_Checker II to check the bootblock and the first file in the startup-sequence, plus a few other special files for viruses on any disk inserted into a floppy

1.31 Option Scan

Scan Watch Change

Selecting this Checkbox gadget tells Virus_Checker II to automatically scan any file or Directory that is being watched by Virus_Checker II should it change

1.32 Option Capture

Ignore Capture Vectors

Setting this Checkbox gadget tells Virus_Checker II to ignore anything in the capture vectors. These vectors are used to survive reboots so viri usually go for them.

1.33 Option UseBBLib

Use BootBlock.library

Setting this Checkbox gadget tells Virus_Checker II to use the BootBlock.library when checking Bootblocks for viri. This library knows about some viri that Virus_Checker II does not so it is best left on.

1.34 Option DFxFull

Check DFx Full

Selecting these Checkbox gadgets compliments the bootblock checks. If selected and a floppy is put in the drive then Virus_Checker II will automatically start scanning the whole disk for viri.

1.35 Option

Check Files for BootBlock viri

Selecting this CheckBok gadget will activate the checking for BootBlock viri in "normal" files. This has especially been added for Anti-Virus Teams, the regular user does not need to activate this since all current known viri do not save their code to a bootblock structured file.

Virus_CheckerII does not check EVERY file deeply for bootblock viri. It first tries to identify if it is a bootblock file by testing the first three bytes for the occurrence of the string 'DOS'. If present, this file is considered a bootblock, it is checked for BB viri, if none are found, the file is normally checked for Link and File viri.

1.36 Option HotKey

Popup HotKey

This is the key combination that is used to POP the Virus_Checker II main window open if it is not open already.

1.37 Option TempDir

Tempory Directory

This string gadget is only of use to registered users. When unpack.library looks into LHA/LZH files it requires a tempory directory to do so. This is that directory.

WARNING: WARNING: WARNING: VirusChecker II deletes anything in this directory when it removes it's files so make sure that nothing of importance is in them. You have been warned.

1.38 Option Save

Save Options

This will save all the options to the file PROGDIR:Virus_Checker.config or S:Virus_Checker.config depending on where it was loaded from.

1.39 Option CloseWind

Close Window

Pretty obvious what this one does. Closes the window

1.40 Option ArexxScan Window

Arexx Scan Window

Setting this button will tell Virus_Checker II to open the Scan display window when scanning files by ARexx. Turning it off will not see the files as they are scanned.

1.41 Option Start Iconified

Start Iconified

Selecting this CheckBox will cause Virus_CheckerII to NOT open it's main window after startup but only a mere titlebar.

1.42 Option AppIcon On

AppIcon On

Turning this gadget on will allow Virus_Checker II to create an AppIcon on your Workbench. Workbench has to be running before Virus_Checker II so that the AppIcon can be made. However if you start Workbench after Virus_Checker II has been started you can get Virus_Checker II to create an AppIcon by turning this option off (if needed) and then back on.

1.43 &

&

This gadget will bring up the ASL File Requester and you can enter a file or directory to watch. Selecting it will automatically enable the string gadget and enter the dir/file name in there. Then simply hit the return key to enter the name.

1.44 string

This string gadget is used to enter the name of the file or directory to be watched. If you selected a name in the ListView gadget then the name will automatically be put in here as well.

1.49 History

6/12/97

Until this date a lot of stuff has been done, I have had better things to do then keep a diary of what I did what day for how long so I'll just dump here what I have done, will be stylised next time.

Removed Unpack.library, it was unstable, caused systems to crash and eat amounts of memory without returning it, etc etc, so it had to be removed.

Added internal LHA checking tool, this is not yet as I want it but is a good workable version, it extracts lh5 archives, checks them and deletes the temporary directory (unfortunately had no time to make this deletion internal, so Delete command from C is used, sorry, does not remove viruses yet, sorry again.)

Changes to VirusChecker.brain:

- Added "Lisa Fuckup v3.0" Trojan (ScanEbola97)
- Added "BOKOR 1.01" Virus
- Added "BOKOR 1.05" Virus
- Added "BOKOR 1.06" Virus
- Added "BOKOR 1.1" Virus
- Added "Happy New Year 96" Virus
- Added "ZIB" Virus
- Added "ZIB" Trojan (Spatch)

Detected one Enforcer hit (but can not find it) in BGUI Main Window.
(no ill effects and will soon be fixed)

10/12/97

Jan Andersen already found a bug (wow that was fast :), in the archive checking routines. Forgot to get a register from stack... Thanks Jan.
Also added support for lha compressions 0 to 4 (so 0 to 5 is now supported)
Added option button for FormatProtection (not yet implemented).

12/12/97 (very, very, very early in the morning)

Fixed the ShortenHunk routine finally, thanks Dave.
Fixed a really NASTY bug in the ZIB removal routine, some BRAnches were not set to RTS. Fixed immediately :) resulted in 3 hours of hard labour.
HNY96 fixing routine made flexible, sometimes other variants were fixed the wrong way and caused crashes like the ones occuring in the "fixed" ZIB programs. All fixed now. Removed some kludgy code (my own :)) and changed also some internal variables.

14/12/97

LHA archive checking caused sometimes crashes or loops, fixed.
LHA can now also be used if you are not registered, this will ONLY be until the new version of VirusChecker has been released (together with completion of Archive Checking).

16/12/97

Fixed ZIB recognition, now also LoadWB infected files are fixed ok.

21/12/97

Added HNY96 Installer recognition code to Brainfile.

24/12/97

Rapidly added "HNY Installer 2" and the fake MUI patch, these will be done properly at a later date. ↵

Version 1.0 of Virus_Checker II Released 25/12/97 Size 61776
(Special "Hurry Up It's Christmas Time" Edition)

Here it is.. Added some locales... Lost the Nowegian catalog due to disk errors... Sorry, will be added next time.

26/12/97

Changed HNY Clone Installer detection. Picked up wrong files sometimes, sorry 'bout that, thanks to Karl P Schmidt for finding this bug. ↵

27/12/97

Added HitchHiker 2.01 Installer Virus to brain
Added HitchHiker 2.01 Virus to brain

Fixed a really nasty bug in the archive checking. It would lock the complete system up when started from User-Startup and later an archive was checked. This has been fixed, found out that the output was expected to go to a window (woops) well this is not possible when VC is started from a script which closes it's window later so it is redirected to a temp file. If for some reason the tempfile can not be written, the program just tells the user that the archive could not be unpacked and checked, no possible bugs there either. All should work well now. ↵

28/12/97

Fixed a minor bug occuring when zerobyte files were checked. VirusChecker II reported that the file could not be read (offcourse) but tells the user also that it has not been checked for viruses. This has been fixed. VirusCheckerII just skips those files now. Sorry for any confusion that has occured. Thanks to Lars Kirstensen and Dale Frameli for reporting this to me. ↵

Fixed a minor bug in the installer script. It would install Virus_Checker in the user-startup instead of Virus_CheckerII .. Removed a space and now it is ok. Thanks to Ross Deeley for reporting this bug. ↵

29/12/97

Added LisaFuckup v2.0. After hours of coding and crashing I finally cracked the little bugger. I made it completely safe, i.e.: other compiled Arexx scripts won't be falsely recognised since the brainfile tries to decode the encoded stuff inside and searches for the specific stuff of Lisa FuckUp v2.0. Thanks to Stephan van Maris for sending me the archive. ↵

30/12/97

Fixed a big bug in the beta version of VirusChecker.brain v2.2b2. HitchHiker 2.01 was not recognising the other version of HH2.01. I knew this but could not do anything ↵

about it until Jan Andersen told me the bug was there and gave me some material to ←
work
with. Thanks Jan!

Fixed a version check bug. I found the AutoRequest() used to notify 1.3 users that VirusCheckerII is a 2.04+ only utility, not that great to say the least. I just removed the code, replaced it with a 'simple' message output and debugged it a lot using a softkicked 1.3 kickstart. Please report any problem that might occur.

31/12/97

Fixed a nasty little bug concerning the bgui.library. Whenever the bgui.library (←
or
any other for that matter, but mostly BGUI) was not detected, VirusCheckerII ←
reported
this nicely and then caused some severe enforcer hits. I did not get them at first because BGUI was still hanging around in memory but when I removed it with flush and tried again (after removing it from LIBS: also) I got serious problems. It seemed that whenever a library error occurred, VirusCheckerII still tried to remove all system resources it thought it had opened but which it really hadn't. In short: it tried to close stuff that was not open therefore trashing memory. Sorry about this. Thanks to a lot of guys who reported this to me and especially to Xavier Messersmith for supplying the enforcer hit list which I could not create at first.

1/1/98

Fixed a little locale error. The ToolTipHelp option (a help text that pops up when you leave the mouse pointer over a button for a few seconds) was only displayed on two buttons in the main window and were NOT localized. Thanks to Dirk Stoecker for reporting this. I have even gone a bit further and gave ALL buttons a ←
localized
pop up message (same as the message that pops up when HELP is pressed).

Also "fixed" the fake "bgui.library missing" message a lot of people got. After ←
testing
and debugging I discovered in the docs of BGUI that BGUI itself needs commodities.library, asl.library and I think it was the gadtools.library. Anyway, when testing the bgui.library wouldn't open (offcourse since the commodities lib was missing) so I decided to let VCII open the other libs BGUI needs first and if one of them is not present, VC II will report this before claiming not to be able to open BGUI. I hope a lot of problems concerning the libs are fixed now. Thanks go out to a lot of you out there, too many to mention here.

Changed the locale strings a LOT! If you are planning to translate the catalogs or have done this already, check the .cd file again. A lot of error messages have been removed (especially the library error messages) and have been replaced by just one string. Thanks go out to Dirk Stoecker for his suggestion to remove most of those ERROR|Could not... etc. messages. More optimisations will follow.

3/1/98

Did some preparations for the Archive Options Window. Window is now finished, program mechanics only have to be created and adjusted to fit in. Already registered users can take a look but can not do anything with it alas.

Fixed also a possible problem. Vector Window was not closed automatically when someone pressed QUIT when the window was still open. Window is now closed if it was opened.

6/1/98

Fixed a really serious problem with the Vector Show feature.
Added Happy New year 98 link virus to the Brainfile.
Fixed some smaller problems with VirusChecker II (internal).

7/1/98

Fixed memory disabling of HitchHiker 2.01 link virus to brain
Fixed memory disabling of Happy New Year 98 link virus
Added Happy New Year 98 BootBlock virus recognition to brain
Finally fixed the big bug in VectorShow, pushed the stack too far back.. woops.

8/1/98

Fixed ZIB link virus removal for LoadWB files infected by the ZIB installer.
Fixed some possible future bugs in HitchHiker 2.01 link virus removal.

9/1/98

Fixed a few severe enforcer hits caused by the checking for Infiltrator virus.
Expanded Archive Checking a lot! Added the use of an external configfile which will later on be editable (I do NOT suggest you edit this file manually)
Removed the two year old history information in this guide.

10/1/98

Finished Archive Options window. New archive entries can be added or removed.
Not yet edited but that can you can work around that by removing the entry that has to be edited and add it again.

11/1/98

Optimised and debugged the Installer script. Found a few bugs reported by a lot of you out there, thank you very much. I think you will like what I have done to the installer. Someone reported to me that Virus_CheckerII was not started ↩ correctly
from the WBStartup, this has been fixed by the use of a Project icon.
The bug occuring when VC_II was installed in the User-Startup has now also been removed, it now properly adds 'Virus_CheckerII' to the file instead of 'Virus_Checker'.

A few other bugs have been removed and the supplied icons are also copied to ↩ wherever
you want it to be copied.
The complete script should now work a-ok again.

20/1/98

Added ADO! 1,2 and 3 Trojan Virus to brain

Fixed a bug occuring in comparing of strings. This sometimes caused unwanted ↩ removals
of CheckNow and Watch entries but has been fixed now, it should even work faster now since I optimised the code a bit.

Also optimised CheckNow routine, double instructions removed. Should even make it more stable.

CheckNow button ghosted when list is empty. If I remember correctly, I have Lars Kristensen to thank for this suggestion.

Optimised Archive checking a little. Replaced Read() for FGetC() command since ID

strings are sometimes not bigger then 3 or 4 bytes and would cause unneeded ↵
overhead
with the conventional unbuffered Read() compared to the buffered FGetC(), I put ↵
the
FGetC() command in.

21/01/98

Did some optimisation of the code itself. Some minor problems and bugs repaired.

Done some extra work on the CheckNow and Watch windows. Remove buttons are also
ghosted when list is empty.

Optimised and removed some code.

22/01/98

Fixed a small bug in the ArcOpts window. Sometimes a flag was cleared which should
not and unsaved data would go lost.

Adjusted size of iconified window a bit.

Fixed a small bug in the CheckFile routine. Sometimes a FreeMem() was given ↵
instead
of a FreeVec(). Was the result of removing the unpack.library.

Fixed a really stupid bug in the Arexx port. After I had optimised the Strcmp
routine, which was not working correctly with the list entries, the Arexx
string commands were not recognised anymore. Created a special Strcmp routine for
the Arexx port and Arexx works ok again.

25/01/98

Fixed a tiny little bug in the memory check.

Added recog for SnoopDos 3.0 in memory. If SnoopDos 3.0 changes the LoadSeg,
Virus_CheckerII will know about this and will NOT ask you if you want to Restore
the LoadSeg. I don't know if this works with all Snoopdos versions. I KNOW it
does NOT!!! work with 1.7 because 1.7 works a lot different from 3.0 and I have
not been able to find a way to detect it's presence SAFELY. Other versions I
don't have acces to, so it might only work with 3.0.

Added also the 'Checking Disk in drive xxx:' to the Iconified window.

26/01/98

Worked very late to include another feature (0:34am). Added font sensitivity
concerning the titles of the main windows. Idea suggested by Jan Andersen.

```
*****  
**  Version 1.1 of Virus_CheckerII & Version 2.2 of VirusChecker.brain  **  
**  Released:   26/01/98                                           **  
**  Size       :   68.008 (Virus_CheckerII)                        **  
**                               15.284 (VirusChecker.brain)        **  
*****
```

1.50 VectorShow

Vector Show =====

This is a new option which will during the developement of VirusChecker II be extended, updated and refined.

This option has been added to the menu as well as to the main window for easy acces. It shows some important vectors and memory addresses that generally are frequently infected by viruses. Showing such an address does NOT mean that this position has been infected. For now just a few vectors are showed indifferent of a possible infection or not. In other words, these vectors are ALWAYS shown by VirusChecker II. This might soon change. It also enables some advanced users to check these vectors manually so that they can identify possible future virusses/problems etc.

Remember, any serious problem like patching of LoadSeg() or DoIO() and the like are monitored and reported so there is little need to worry when finding different altered vectors.

1.51 Format Protection Options

Format Protection Options =====

This feature has not been implemented yet but will be added very soon. This button will, in the future, open a options window for this new feature in which it will be possible to specify which device(s) to protect from formatting and probably also which unit and if any boot writes, formatting and RDBs should be protected.

The idea behind this feature is to prevent viruses from doing some really nasty jobs like formatting the harddisk, writing to the bot sector or removing the RDBs (which equals in some cases to formatting the HD, mostly indirectly because of unrecoverable disk information).

I can however not take any credit for this future feature (wow) since the idea itself came to me when I had used MCP (Master Control Program by Michael Knoke) which has this feature in itself. The routines which will be inserted to enable this feature came from Michael who also gave me permission to use these and also make them part of the ShareWare part of VirusChecker II. Sit tight, you probably won't be disappointed. :)

1.52 Archive Options

Archive Options =====

This button gives you acces to the Archive Options window which contains four buttons and a scrolling list. This window is only accesable if you are a registered user.

New

Clicking this button opens up another window with which you can add a new Archiver to the list.

Label

In this string gadget you can enter the label of the archiver entry. To add an archive entry successfully to the list this entry must be set.

Offset

In this integer gadget you can enter the offset of the ID string in the file. LHA for instance has it's ID string at offset 2 and LZX at offset 0. This gadget defaults to 0 and does not have to be set.

ID String

This string gadget has to be set to create a succesfull entry. It holds the ID string used to identify an archive. LHA for instance has as ID string -lh and LZX has as ID string LZX

Cli Command

This string gadget must definitely be set since it is used to unpack the archive. LHA for instance can be unpacked with the following cli command:
LHA x -m -M -q "%s" "%s"
The first %s is the wildcard for the archive which has to be unpacked and the second %s is the destination directory. Make sure the wildcards are placed between two " else the unpack command might get confused when dealing with pathnames like: Ram Disk:

Accept

Pressing this gadget will cause the data to be added to the list. If you forgot to set one or more string gadgets, VirusCheckerII will warn you and return you to the window with the data.

Abort

Pressing this gadget will (obviously) stop configuring the archiver and discard all entered data.

Remove

Pressing this gadget will cause a selected entry to be removed from the list.

Save Options

Pressing this gadget causes the list to be saved to disc. BEWARE! Do NOT adjust the list (Virus_Checker.Arc) since manual editing may cause VirusCheckerII to crash or something far worst.

Close Window

Pressing this gadget causes the window to close.

When you have added or removed an entry from the lis, have not saved the list and cause VirusCheckerII to quit (one way or another), VirusCheckerII will ask if you want to save the list or ignore the changes.

BEWARE!

Although this code has been optimised a lot, it is possible that your machine gets slowed down pretty bad because of this function. This is very likely when you have entered a lot of entries in the list, and/or if you have some kind of

debugging and/or snoop task running. If you this is the case, then you can offcourse turn it off in the options window, or try to remove some of the entries, or quit the debugging/snoop task.

1.53 Future

To Do List =====

Note: Any item that has been placed on this list will be implemented, although I can not be and will not be pressured to add such a feature any faster then I see fit. When I put any item in this list I am considering if I can already do some work in order to satisfy those who requested the feature or are waiting for it but I will do this only on free will. I can not and will not guarantee that a feature will be implemented in the next version unless I mention this somewhere and even then I can not be held responsible for not implementing a certain feature. You have to realise that coding VirusChecker II is purely a hobby of mine and although I throw myself sometimes for days on a row on VirusChecker II it mainly is something I like to do and so I don't really like to be pushed. However, people that want to ask about or request a certain feature can always do so, even if the feature is already on the list I will answer any question/request/etc.

To Do/Future developement ideas in no particular order:

- More levels of archive checking (only one level supported now)
 - Vector Show expand and refined so that it contains at least the changed vectors and hides those which are considered "save". And add the showing of the KickMemList and KickTagList entries if present.
 - Device formatting protection and RDB protection (possibly also saving of this file in order to back this up and store it for repair usage)
 - Fix BOKOR 1.1 type B detection (type A is detected)
 - Fix 68000 "bug", for some reason Virus_CheckerII crashes on this cpu Thanks to a LOT of users out there who reported this to me.
 - Add possibility to predetermine if a virus should be removed/killed or ignored OR if a requester should pop up. Thanks to Micael Johnstone for this good idea ↩
 - Make the entries in ArchiveOptions editable
 - Add possibility to have Virus_Checker create a logfile. Thanks to Remko Wiersma ↩ for this great idea.
 - Add recognition for any version of Snoopdos so that the user will not be ↩ bothered with a requester asking to restore the LoadSeg.
 - Add all the older viruses.
-

If you have any suggestions or questions please write to me.

1.54 UK Registration

UK Registration =====

Don't you just hate going to the bank, changing your UK pounds to foreign currency paying more then the actual registration fee? I myself like to avoid going to the bank when it is not extremely necessary since client friendliness is something ←
they

have not written in their dictionaries. So why bother?

Thanks to Paul Compton you can register VirusCheckerII the easy way, just contact him, he will contact me and after paying him in UK pounds, you will be a fully registered VirusCheckerII user within days.

But how does it all start? Well, there are two possibilities:

1) you are an already registered user of VirusChecker

or

2) you want to become a registered user of VirusCheckerII

In the first case, you probably have registered yourself with John Veldthuis and ←
are

now wondering if you are beeing supported by me. Well, as I mentioned in the ←
ShareWare

section, every user that has registered him or herself with John, can get his/her new keyfile for free. You then only have to fill out the request form,

contact Paul, tell him that you are a already registered user and send the form ←
either

printed or digitally to Paul Compton. He will then send it to me, I will check the ←
data you

filled in. When the new keyfile is available, you will then receive the keyfile ←
automatically

and for free.

In the second case, you will have to contact Paul Compton and agree upon a way of ←
payment.

Then you will have to send the completely filled out request form to Paul.

After I have received your request form and heard from Paul that

you have payed your fee, you will receive an old keyfile if the new version is not ←
available

yet, or the new keyfile. This will be done either through e-mail, Paul's BBS or by ←
snail-mail

(You will have to pay for the Postage and Package however).

In short:

I suggest you fill out the registration request form, contact Paul Compton and print the request form, out of send it digitally to him.

Here is how you can reach him:

You can call his Bulletin Board System (BBS):

Elevate BBS
+44 (0) 1329319028

Write a netmail to the following address:

2:251/18.0@Fidonet

Write an e-mail to the following address:

pwcomp@elevate.demon.co.uk

Or write to his snail mail address at:

Paul Compton
36 Priory Road
Fareham
Hants PO15 5HT
UK

Paul also has a website, why don't you take a look at his site? His url is:

www.elevate.demon.co.uk

1.55 VC II Related

Bulletin Boards:

Virus Help Team Denmark's support BBS

Name.....: XPoint BBS
SysOp.....: Benny Pedersen
Phone Number....: +45 6381 8005
Open.....: 24 Hours
Modem type.....: 33.600 v.34+ & ISDN
Country.....: Denmark
Request.....: Viruschecker
Note.....: Always the newest viruskillers. Modem users all over the world
now know where they can find a clean copy of the newest VC_II.
With magic request name _VIRUSCHECKER_

Virus Help Team Netherlands' support BBS

Name.....: United Bulletin System 1
Sysop.....: Willem van Dijk
Phone.....: +31 (0)70 4450416
Open.....: 24hrs
Modem.....: 28k8 & soon ISDN
Country.....: Netherlands
Request.....:
Note.....: Almost all possible known echo mailnetworks in the netherlands
available here aswell as the latest software and offcourse
the latest version of VirusCheckerII and it's brainfile can be

found here.

Also official registration site for VirusCheckerII for the Netherlands, easy registration can be done through this board when living in the Netherlands.

Official VirusCheckerII UK Registration Site

Name.....: Elevate BBS

Sysop.....: Paul Compton

Phone.....: +44 (0) 1329319028

Open.....: 24hrs

Modem.....:

Country.....: United Kingdom

Request.....:

Note.....: The official registration site for VirusChecker II for the United-Kingdom. If you are living in the UK and want to register the easy way, then try and contact this BBS.

Internet:

www.elevate.demon.co.uk

Elevate BBS, Official UK Registration site for VirusCheckerII

home4.inet.tele.dk/vht-dk

Home of Virus Help Team Denmark, free PC, Amiga and Mac AV utilities. You can also find the latest updates of VirusCheckerII and the brainfile here.

And at most Aminet mirrors offcourse.

If you have any VirusChecker related addresses that are not on this list, please pass them through so that I can add them to the list after I have checked them out offcourse :).
