Virus_Checker

John Veldthuis

COLLABORATORS			
	TITLE : Virus_Checker		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	John Veldthuis	February 12, 2023	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

1 Virus_Checker **1**

1.1 Virus_Checker 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 . . . 14
1.13 Locale . . . 14
1.14 How to install Virus_Checker . . . 14
1.15 Lha . . . 15
1.16 AppIcon . . . 15
1.17 Disclaimer . . . 16
1.18 Author Info . . . 17
1.19 Files . . . 17
1.20 Arexx . . . 18
1.21 Credits . . . 20
1.22 Options . . . 21
1.23 Watch . . . 22
1.24 Scan . . . 23
1.25 Quit . . . 23
1.26 Option XFDMaster . . . 23
1.27 Option UseWindow . . . 23
1.28 Option IgnoreBB . . . 23
1.29 Option Unpack . . . 24

1.30 Option DFxBB . . . 24
1.31 Option Scan . . . 24
1.32 Option Capture . . . 24
1.33 Option UseBBLib . . . 24
1.34 Option LHA . . . 25
1.35 Option DFxFull . . . 25
1.36 Option HotKey . . . 25
1.37 Option TempDir . . . 25
1.38 Option Save . . . 25
1.39 Option CloseWind . . . 26
1.40 Option ArexxScan Window . . . 26
1.41 Option AppIcon On . . . 26
1.42 & . . . 26
1.43 string . . . 26
1.44 Add . . . 26
1.45 Remove . . . 27
1.46 CheckNow . . . 27
1.47 Check . . . 28
1.48 History . . . 28

Chapter 1

Virus_Checker

1.1 Virus_Checker Help

~Presentation~~~~~~~~~
        What is Virus_Checker

~Important~notes~~~~~~
        Please Read this

~Shareware~Notice~~~~~
        Virus_Checker is not free

~Security/PGP~~~~~~~~~
        How do I know this is not a virus

 PGP Key Servers
        How to get my public PGP key

~Registration~~~~~~~~~
        Fill me out and mail me

~Danish Registration~~
        Fill me out and mail me

~Main~Window~~~~~~~~~~
        Main Virus_Checker window

~Command~Line~Options~
        Start Virus_Checker from SHELL

~Icon~ToolTypes~~~~~~~
        ToolTypes Virus_Checker uses

~Workbench~AppIcon~~~~
        Drag and Drop checks

~Files~Needed~~~~~~~~~

Files required by Virus_Checker

~Localization~~~~~~~~~
Yep Virus_Checker is locale aware

~Installing~~~~~~~~~~
How to install Virus_Checker

~$4eb9~Link~Virus~~~~~
SPECIAL NOTE ON THIS VIRUS

~LHA/LZH~Files~~~~~~~~
Checking into LHA/LZH files

~Arexx~Port~~~~~~~~~~
Arexx commands

~Disclaimer~~~~~~~~~~
And now for something completely different

~Author~Info~~~~~~~~~
About the Author

~Credits~~~~~~~~~~~~~
Thanks Guys

~History~~~~~~~~~~~~~
How things got to here

1.2 important

Some important notes for Virus_Checker
==========

The configuration file has changed for version 7 of Virus_Checker. The old one is no longer valid so please delete the file s:Virus_Checker.config

Also Virus_Checker will now 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 to vcbugs@tower.actrix.gen.nz
Please send suggestions to vcsuggestions@tower.actrix.gen.nz

1.3 Shareware Notice

This program is SHAREWARE.

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

The cost is a very small US$20. For this you get some key details that will unlock a feature in Virus_Checker. The key will be valid for all releases of Virus_Checker so you don't need to get new details each time a new release is put out

The best way to send this to me is in cash. I can take just about any kind of cash as long as they are notes. Our banks will not take coins. Thus if you are in Australia then send Australian dollars. I prefer US dollars however.

If you cannot send cash 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 adddress 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 details 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 details over 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 Registration Form       **
**********************************************

Mail to:     John Veldthuis
             21 Ngatai Street
             Manaia, Taranaki, 4851
             New Zealand


First Name: _________________          Last Name: ____________________


Street:          ____________________________________________


City:            ____________________________________________
```

State/Province: _____

Country: _____

Email: _____

****

Registration of Virus_Checker will unlock a few features that are present in Virus_Checker that will not work unless you have a key. At present this is the ability to check files inside LHA/LZH files.

This key will only work under WB2.04 or better but if you have WB1.3 then you can still send the fee in and I will send you a key. It will of course not do much. You will receive in the mail (or email if you have a PGP public key) details to enter into the MakeKey program that comes with the Virus_Checker archive.

The cost of the Shareware fee is US$20 or equivilent. 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 cheques must be in US funds or New Zealand funds.

****

_____ _____

Signature Date

1.5 Danish Registration

Virus Checker Registreringsformular

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

Personlige data (disse data vil blive opbevaret paa elektronisk form af Virus Help Team Denmark, og John Veldthuis. 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:

O Send mig koderne i et almindeligt brev.

O Send mig koderne til min Internetadresse (PGP kodet)

O 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 registeringen.

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

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

1.6 Presentation

This piece of software is
Shareware
!

Virus_Checker

Virus_Checker, Copyright (c) 1990-1995 by
John~Veldthuis
==========

(johnv@tower.actrix.gen.nz)

Virus_Checker 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 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.

You will be able to use the program without reading this file but for best advantage you should read it all.

Any comments or problems with any of the documentation or the program itself are welcome; if you can't get electronic mail to me, please feel free instead to drop me a note via the overland
mail~address
given below.

Virus_Checker is written in 100% Assembly code using Cygnus Ed, Macro68, and Debugged using Powervisor. Metascope is just not up with it anymore

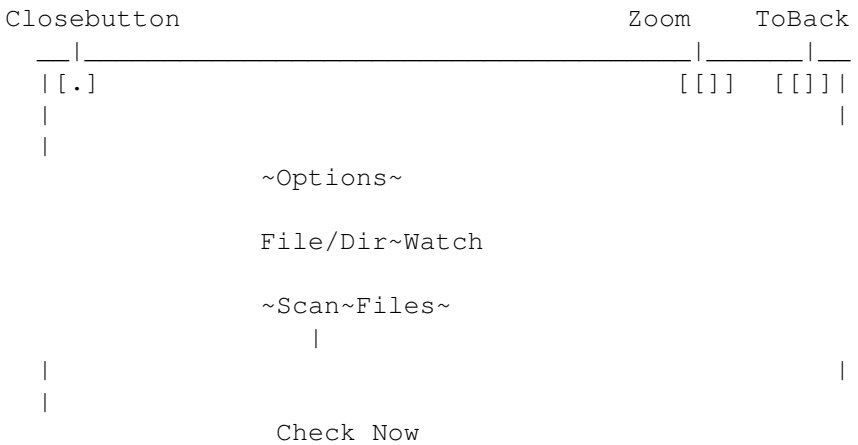
1.7 Main Window

Main Window and short intro
==========

When Virus_Checker starts up it will do a number of things before you even see anything appear. First thing it does is initialise itself and then checks itself for changes that have been made. It then loads the files it needs and checks them. Next it checks memory for any infection. Next on the list is to see if the user gave it a file to scan. If yes then it scans these file/files. Next it checks the first file in s:startup-sequence for any viri. This is a common place for infection. Last thing it does is check any floppy disks that may be in the drives.

At this stage the main window will open. It will not open if you told it not to though. The main window can open in 2 states. Full or ICON mode.

The layout is below



Clicking on the close gadget will make all the open Virus_Checker windows close. This does not actually stop Virus_Checker but just makes all the windows close. Virus_Checker is still on guard.

Clicking on the Zoom gadget will make Virus_Checker change back and forth from between it's normal open state and it's ICON state. The ICON state is basically just a TitleBar.

Clicking on the ToBack gadget will send the Virus_Checker Main window behind all the other open windows.

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 to do another complete memory check. This is the same one that is done at start up.

Project/Save Config

This menu will cause Virus_Checker 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 to stop and remove itself from memory.

Window/Snapshot window

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

1.8 Command Line Options

Command Line Options

```
Usage: Virus_Checker 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 use of unpack.library for uncrunching files. It does not affect the LHA/ZOO unpacking in the registered version. The reason for this option is that unpack.library sometimes will crash the machine on certain crunched files it thinks it knows about but does not. If you have trouble with Virus_Checker crashing try this one and see if it fixes the problems.
This can be also turned off using the Options Window.

B=BOOTBLOCKLIB

Using this option will tell Virus_Checker to use BootBlock.library to check for bootblock viri. There are many viri in this library that Virus_Checker 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 options and causes Virus_Checker 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 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 will output anything it would normally display through a requester out throught the shell it was started from. This includes virus information and error messages.

AUTOSCAN

This option affects what happens when Virus_Checker gets a message from AmigaDOS that a file or directory has been changed. If this option is

given then Virus_Checker 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 which key you wish to use to pop up the interface.

A=APPICONNAME

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

QUIT

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

DIR

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

1.9 Icon ToolTypes

Workbench ToolTypes
==========

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

All of the ToolTypes are already in the Virus_Checker.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 to finish.

UNPACKOFF

This option turns off the use of unpack.library for uncrunching files. It does not affect the LHA/ZOO unpacking in the registered version. The reason for this option is that unpack.library sometimes will crash the machine on certain crunched files it thinks it knows about but does not. If you have trouble with Virus_Checker crashing try this one and see if it fixes the problems.
This can be also turned off using the Options Window.

BOOTBLOCKLIB

```
    Using this option will tell Virus_Checker to use BootBlock.library to
    check for bootblock viri.  There are many viri in this library
    that Virus_Checker 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 options and causes
    Virus_Checker 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 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 gets a message from
    AmigaDOS that a file or directory has been changed. If this option is
    given then Virus_Checker 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 which key you wish to use to pop
    up the interface.

APPICONNAME

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

QUIT

    This tells Virus_Checker 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
    will start scanning it as soon as it has started up.
```

1.10 Security

```
                                        Security/PGP
                                ============

All versions of Virus_Checker since 6.44 hav 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
                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 recent 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 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 will warn you of both checksum errors on itself and on the
file VirusChecker.brain.


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

mQCNAi6h70wAAAEEANWu8csrvc6Z/JY21kiJwklSIDVltJKlxNGU47AFrIGUTcSD
12WNXFKSn/wdjVLJ6ATgRBeErtxPj8t9p7ple4/cN8uziYzC0gFbQdfH/CmcrM0e
sPQJxcmkUiFG7BpENF9uqS2hNyL1HL4xHOwFXcN1PUZflGxtaQ0mtYy7jZfBAAUR
tCpKb2huIFZlbGR0aHVpcyA8am9obnZAdG93ZXIuYWN0cml4Lmdlbi5uej6JAHUD
BRAurJ3meXjB5OBD6aEBASAQAv46FGU1aiWZv3YCPsyDxUIfYe7Lz8iPnyJmLKec
QDlESHfac/9OuBQvp1KIUWDBFFLt+jOpEzZbCHkNWmgJtF8JhGjzJ6EUn3Z75nps
BbT6MJNYGptCQ3+xhTuTGBdun4CJAJUCBRAuskv2oNrznbERpEEBAS2qA/9GpqEY
N43g7kDZbWN8kxlFPhcIuDRRnZquLu/kdCyPMW0ZQ6SNWp+1+1J/MNdPVVmRvzxa
csnAmeKFDGfWATr3v5Z9aWRsfxCUQI0+lT5IAqzxyjlD5vexvd1+wytXVisDcqMD
djoZqbZmCL7cMBGerh1oWOD9AhiHqzTCx6/x44kAlQIFEC6wfvMNJrWMu42XwQEB
oBsD/0xFuFxRRBvd1d94oTbMyBYensOB8iVPEE06W4Ai+CN4bUrwsEH0bossz51p
XtekSA4BgpTWt9xthr0S2N1jQwNbcmBOG+rkA0hrhTafX1jRr55zNJk38eeCwJCm
dGI5Z5xYLnzYe4hP5ToL1vTYQq+ZkMGZeZxTE/MAT5rr/I1F
=1nZv
-----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 automagically.

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 is now localized and about 80 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

                Swedish

                Italian

                French

                Norwegian

                Danish

                Deutsch
```

1.14 How to install Virus_Checker

```
                          Installing Virus_Checker
                          ========================


Virus_Checker comes with it's own installer script. This installs
Virus_Checker 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.
Depending on your choice Virus_Checker may have to move a few files but it
does tell you about this first.
```

1.15 Lha

```
                                    Checking into LHA/LZH Files
                           ============================

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

Virus_Checker cannot 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
                 varibles in the format

Lhafile.lha->infected = SCA Virus

The Lhafile.lha is the filename of the infected archive and infected is the
name of the file inside the archive. It may be several directories down but
it is the name.
```

1.16 AppIcon

```
                            Virus_Checker AppIcon
                            =====================

If Workbench is running when Virus_Checker 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 AppIcon and drop
them on it. Virus_Checker will immediately start checking those things
dropped on it.

*****NOTE******

If Virus_Checker finds a file called Virus_Checker_AppIcon.info in it's
PROGDIR: then it will use this icon for the AppIcon instead of it's
internal default one.
```

1.17 Disclaimer

OR RESPONSIBILITY IS ASSUMED.

1.18 Author Info

Snail mail:

John Veldthuis
21 Ngatai Street
Manaia, Taranaki, 4851
New Zealand
New Zealand~

Phone: +64-(0)6-274-8409

UUCP/Internet:

johnv@tower.actrix.gen.nz

Internet Relay Chat (IRC) nick:

VirKiller or JohnV

1.19 Files

Files required by Virus_Checker and where they hide

Virus_Checker needs quite a few other files to function.

unpack.library

This library needs to be in LIBS: and is used for uncrunching packed files. It is also used to check into LHA/LZH files in the registered version.

xfdmaster.library

This library is used to also 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. Once saved
Virus_Checker 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 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 will be in either PROGDIR: or S: Again Virus_Checker
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 is used by Virus_Checker to keep track of the non-standard
bootblocks you tell Virus_Checker to learn. It will be loaded from either
PROGDIR: or L:. Again it will be saved back from where it was loaded from.

VCBrain

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

Virus_Checker.key

   This is the keyfile for Virus_Checker 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 Arexx commands
                    ============================

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

QUIT

eg. address 'Virus_Checker' 'quit'

This causes Virus_Checker to shut down and quit

RELOADBRAIN

eg address 'Virus_Checker' 'reloadbrain'

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

SCAN

eg address 'Virus_Checker' 'scan filename'

This command causes Virus_Checker 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 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 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_Checker' 'NOTIFYWATCH password'

This command and the next are very special. They work in conjunction with
the file watch list. Whenever Virus_Checker 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 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
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_Checker' '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_Checker' '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 seperate 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
```

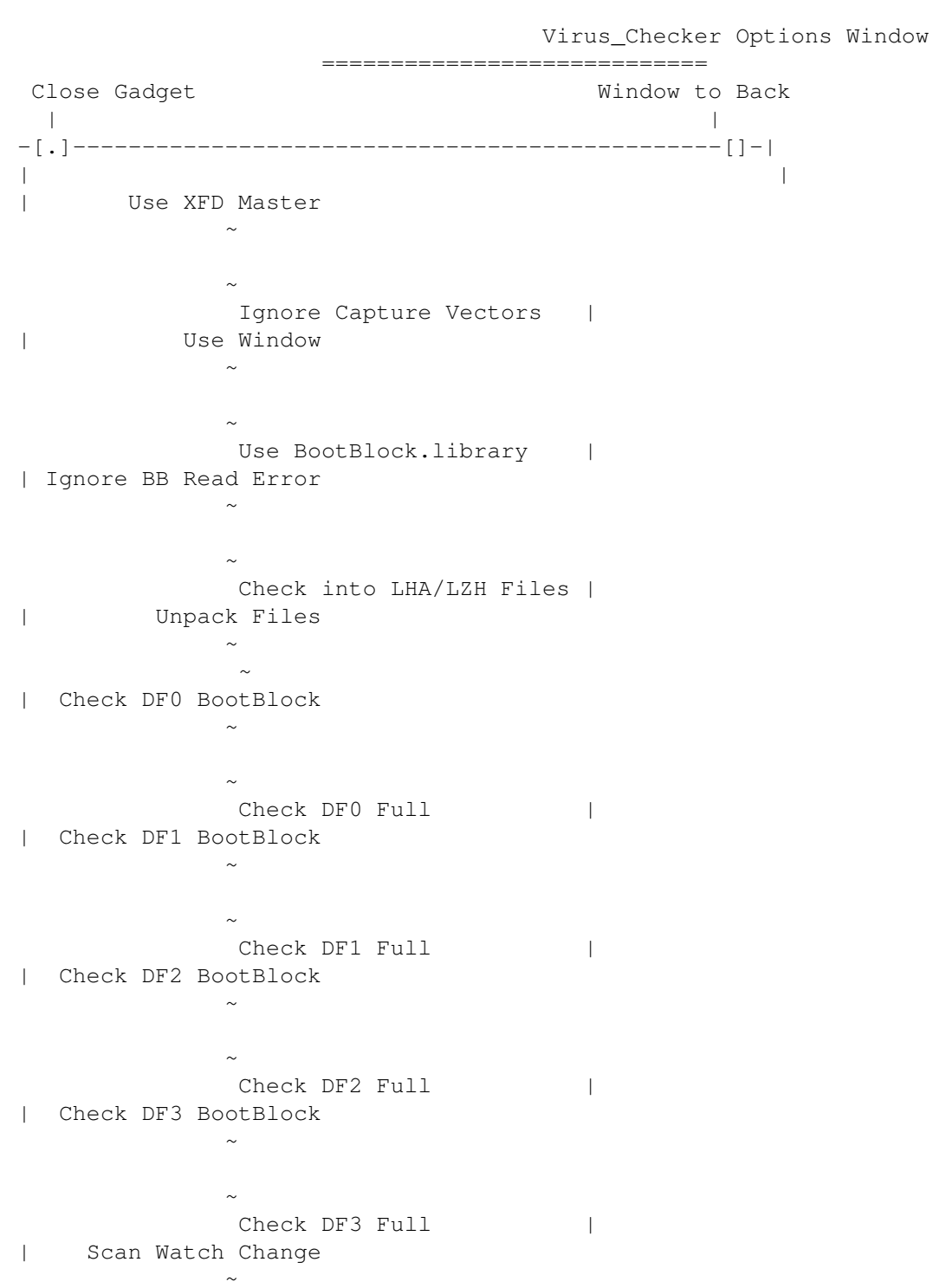
1.21 Credits

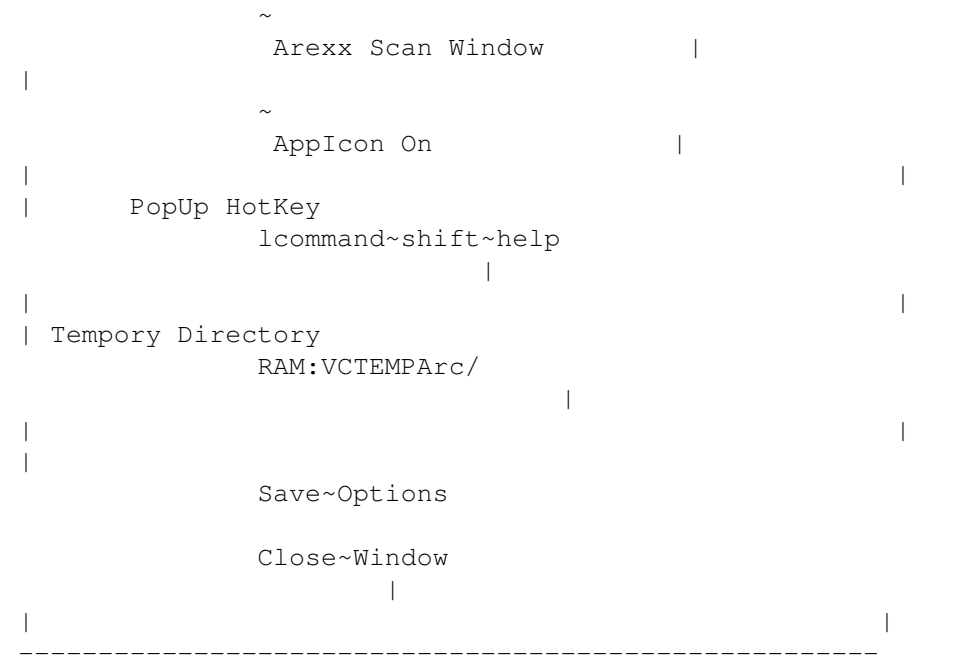
```
                                  CREDITS
                                  =======
 My thanks go out to...

 Thomas Neumann For the inclusion of unpack.library

 Georg Hörmann  For the inclusion of xfdmaster.library.

 David Dustin   For the assembly code for the MakeKey program.
                and heaps of help with docs for WB3.1

 Leo Davidson   For Arexx script for use with Virus_Checker and DOpus 5

 ARexx          Developed on an Amiga 1000 and is a 100% Amiga product.

 Tim Nugent     For picture of where I live

 Markus Schmall For help with the Illegal Access virus


Locale translations

 Nederlands  Jan Hendrik Lots (jhl@grafix.xs4all.nl)
 Swedish     Jon Malmquist (jon.malmquist@mailbox.swipnet.se)
 Italian     Francesco Dipietromaria (dpm@ns.sinet.it)
 French      Florent Monteilhet (florent.monteilhet@ramses.fdn.org)
 Norwegian   Morgan Jakobsen (remija@login.eunet.no)
 Danish      Henrik Lauridsen (hlau@dou.dk)
 Deutsch     Kersten Emmrich (emmy@ramses.fdn.org)
 Deutsch     Torsten Hiddessen (torsten.hiddessen@tu-clausthal.de)



And especially to my Beta Testers who found heaps of bugs and made many a
good suggestion. In no particular order

Leo Davidson       Ben D. Rogers       David Oakes
```

Andrew Dowds Brad Rogers

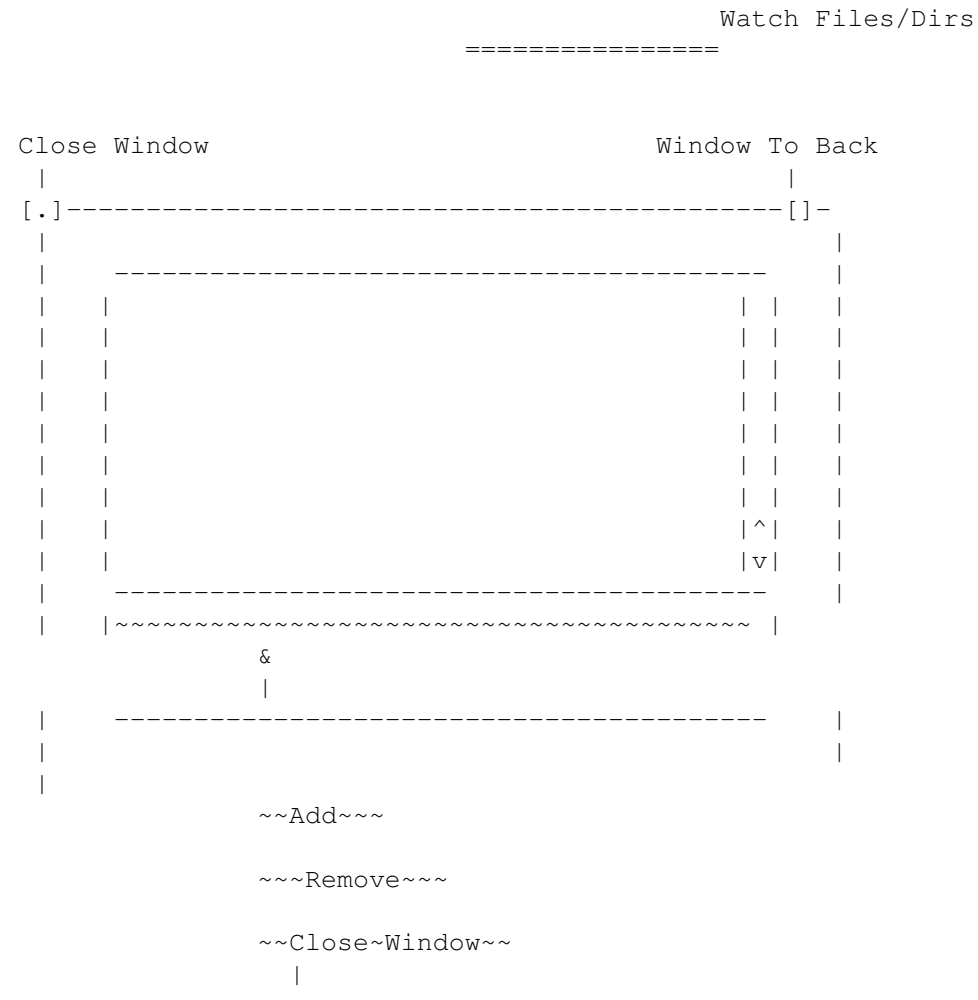
John Veldthuis
==========

1.22 Options




~
Arexx Scan Window
~
AppIcon On
PopUp HotKey
lcommand~shift~help
Tempory Directory
RAM:VCTEMPArc/
Save~Options
Close~Window

1.23 Watch


Watch Files/Dirs
Close Window
Window To Back
&
~~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 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 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 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 cannot read them normally

1.29 Option Unpack

Unpack Files

Turning this Checkbox gadget off causes Virus_Checker not to use unpack.library at all when loading files to be checked. unpack.library can cause crashes on some crunched files due to it thinking it knows what the cruncher is when it is in fact a diffrent one (usually newer ones)

1.30 Option DFxBB

Check DFx Bootblock

Selecting these Checkbox gadgets tells Virus_Checker 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 to automatically scan any file or Directory that is being watched by Virus_Checker should it change

1.32 Option Capture

Ignore Capture Vectors

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

1.34 Option LHA

```
Check Into LHA/LZH Files
```

This Checkbox gadget is only active if you are a registered user.
Selecting it will tell Virus_Checker to look into the archive for any viri
hiding there. Saves having to unpack the whole archive.

1.35 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 will
automatically start scanning the whole disk for viri.

1.36 Option HotKey

```
Popup HotKey
```

This is the key combination that is used to POP the Virus_Checker 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: unpack.library 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 obivous what this one does. Closes the window

1.40 Option ArexxScan Window

Arexx Scan Window

Setting this button will tell Virus_Checker 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 AppIcon On

AppIcon On

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

1.42 &

&

This gadget will bring up the ASL File Requester and you can enter a file or diretory 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.

1.43 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.

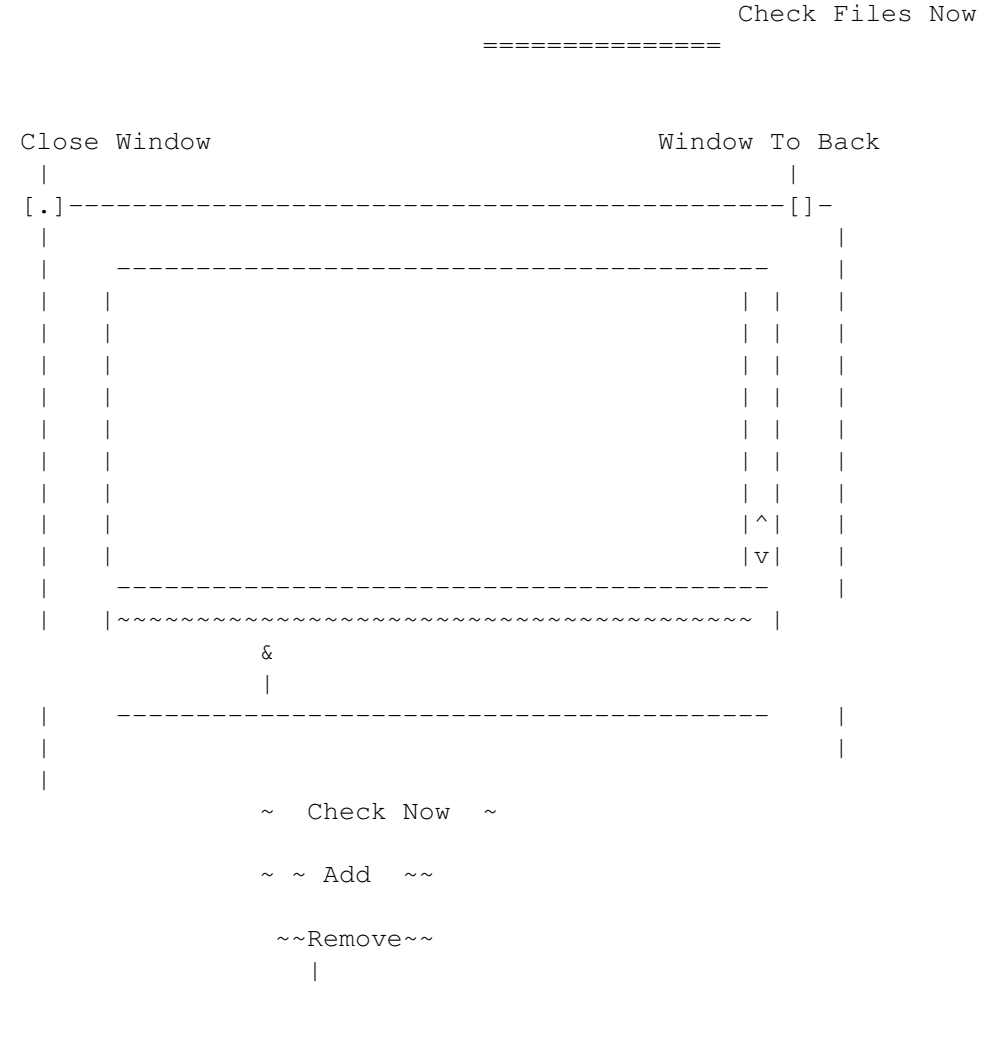
1.44 Add

```
                Add

Clicking on this gadget will activate the
                string
                 gadget above it and allow
you to enter the name of a file or directory to watch
```

1.45 Remove

```
                Remove

Clicking on this gadget will delete the name from the list of watched
files/directories that is specified in the
                string
                 gadget above it.
```

1.46 CheckNow



```
  |                                                |
   ------------------------------------------------
```

1.47 Check

```
Check Now

Selecting this gadget will start Virus_Checker checking all files and
directories listed in the Check Files Now Listview gadget.
```

1.48 History

```
Version 7.0

Internal release only. First runable version after re-write.
Done are Locale support, Options window, WatchList window, File Check
requester, memory checks, bootblock checks.
All files related to Virus_Checker such as it's config, brain, and key
files will be got first from PROGDIR: then from the default location.
Libraries still need to be in libs:

Version 7.1

7/7/95

Got Display option working for Bootblock virus find. Found a buffer too
small and overwriting memory not used by VC. Did not cause problems till
something else tried to run.

8/7/95

Finished off bootblock stuff. learning stuff was last to go in. Maybe need
better error messages. Sent out to beta testers for a try and look

Version 7.2

9/7/95

Put in Zoom gadget so can be used as titlebar again.
Added Snapshot window and Save config to Main menu.
Fixed up Gadget display on GUI. Overlapped in topaz 8. Simple maths fault.
However it did bring to light a new problem when window too big and dropped
back to topaz 8. When window closed and another gadget clicked it changed
to the font just used. Re-programmed Openwindow to correct.

10/7/95

Found bug in menu colors. Set the wrong Tags for LayoutMenuA(). That took
alot of searching and head scratching.
Added close button to file/dir window. Enabled R key in this window as well
May have found bug in Enforcer hit with this window as well
```

```
Started on adding file scanning in. Uses in the following manner. Check if
XFD turned on. If on check if file crunched, if not then try to use
unpack.library to read file, if unpack.library not there just read file in
as is and check.
Sent out for Beta testing

Version 7.3

11/7/95 -> 14/7/95

Away at a course for the next 4 days for work. Wont be doing much on this

15/7/95

Found bug causing crash when all windows closed and hide interface selected
in commodities exchange program.
Finally found bug in File/Dir watch window for enforcer hits. It was a call
to FreeGadgets(). The gadget pointer should have been in A0. I had it in
A1. I thought I checked that one 4 times as well.
Now I can get back to the serious work. Yeaaaa!
Redid gui/font layout calculations. Looks okay in 6/8/9/11 point fonts.
Added code to pop windows to front if already open when selected.

16/7/95

Worked on File checking stuff. Got basic 1 file check routine working. Have
added Saddam virus check to floppy check.
Added RLamer checking to floppy check.

Version 7.4

17/7/95

Added link virus tests to check1file code. Now can start adding in main
scanning code. Will do multiscan first
Found bug in Bootblock remove code. Installing either 1.3 or 2.0 bootblock
would cause a read from a random address and stuff up the bootblock.
Added single file check. If Scan Files selected om Main window and a file
is selected then that file will be checked for file/link viruses.

18/7/95

Skiing today. Great weather but -12 was a bit cold.
Added in Busy pointer/Gadget inhibit while scanning directories.
Added in File scanning code. Works until it hits a virus

19/7/95

Fixed bug in scanning code. Register got corrupted in another routine.
Added scan window to scanning code. Seems to be working 100%. Looking good
so far.

Version 7.5

20/7/95

Added STDOUT option. This will run Virus_Checker in a one shot mode. You
```

need to give it a directory to scan. All stuff that would normally come up in a requester will be output to STDOUT. eg.
Virus_Checker stdout ram:
would check ram: and exit. With the CCCP virus in ram: the following is output to the shell window
WARNING The File "ram:CCCP" is infected with the "CCCP" virus
ALL error messages will also go out to the shell
Added Bootblock virus checking in files. That is now all the file scanning stuff working as in the old version.
Added Stats menu option. Gives a few numbers
Added in checking of first file in startup-sequence
Added option to SHELL. if AUTOSCAN is on command line then when VC gets a signal saying a watched file/dir has changed then it will scan it before displaying requester.
Put Options button for previous on.
Started on Arexx stuff. Added QUIT arexx command. See notes
Added in SCAN arexx command.See Notes
Added in RELOADBRAIN arexx command. Forces a reload of the brainfile
Added in popup when hidden and program run again.
Added in Scan if running and run again with a dir given

21/7/95

Changed action of Exchange Hide Interface. Will close all windows open.
Also changed close gadget on main window. Clicking it will close all windows
Added in Icon stuff. Turned up a few new bugs as well. Getting close to a release though.
Added keyfile checking back into checker. Even closer

22/7/95

Worked on the *.guide most of day.
Found a few small bugs going through when doing the docs.
Fixed a bug with the default configuration. It was giving a legal path in the LHAPath.

Version 7.6

23/7/95

Added $4eb9 Link detection to Link virus code. Will say Possible $4eb9 Link Virus it it finds the right code
Spent most of afternoon tracking done a bug with the File watching. If you watched any file and changed it the warning would be given. Then several false warnings. Changed it so that the Notify was ended then restarted but then got crashes all the time. So cleared out Notify structure after EndNotify() and StartNotify(). Seems to have cleared the problem
Got installer script working (I hope)

24/7/95

Bug with $4eb9 link detection.
Bug in LHA checking. It was actually a bug in the key checking. Checked the key to late so that it was never initialised.
Corrected a few spelling mistakes.
Corrected bug if first file in startup-sequence was not in SYS:c/

```
Version 7.7

25/7/95

Fixed a few enforcer hits. Also some more work on guide.
Added XFD command line and WB options.

26/7/95

Fixed a few minor spelling mistakes.
Got catalogs for dutch and swedish languages in.
Seems to be good so far

27/7/95

Only a few bits on the guide file today. Things must be just about ready
for a release.
Started work on adding an AppIcon. May be in or not. Depends how it works.

28/7/95

Spent hours looking for a bug in the Notify code only to find it a simple
exchange of registers. I used the wrong one again. Assembly is hard at
times.
Added online help (sortof). pressing Help in Main window will spawn
Multiview. The Virus_Checker.guide has to be in HELP:

Version 7.8

29/7/95

Added Option to turn off Scan window when scanning files from Arexx.
Some more work on guide file
Fixed bug in Watch save. When no files to save it did not delete the old
file. So when re-started it would reload the file again.

30/7/95

Worked on AppIcon. Seems to be working well. Dropping icons onto it checks
them for viruses okay.
Put Checksum checking back into code. For those hackers who don't know what
they are doing.

Version 7.9

31/7/95

Started working on ARexx interface to Autoscanning of changed files.
Had to send this out due to a faulty script before

Version 7.10

1/8/95

Worked more on Arexx inface and autoscanning
```

2/8/95

Worked on bug with XFD and unpack both turned off.
Added option to turn AppIcon on/off
Fixed bug in Arexx Scan Window. If off then no scan window at all.
Worked on guide file again as well

Version 7.11

5/8/95

Made it so help could be found in PROGDIR: or HELP:english/
Fixed up Install script again.
Finally got Notify watching working in a way that seems good.
Fixed up guide file again.

6/8/95

Fixed up bug in first file check. Was causing odd address error
Internal release only

Version 7.12

8/8/95

Changed install script to find VirusChecker.brain in L: and warn user if
remove it or leave it. Leave only if running from WBStartup.

9/8/95

Found small bug in ASL code. d0 being set instead of d3. Didn't seem to do
anything though. Crashes after ASL file selected and before scan window
opens on WB2.1 machine???

10/8/95

Found bug. I was using a WB3.0 or better routine to set the busy pointer.
In WB2.04 and WB2.1 it was not there so crash!. Will check for any others

Version 7.13

Obviously my maths is no good and I got the test around the wrong way.
WB3.0 uses the WB2 code and WB2 uses the WB3 code. Result Boom! again.
Fixed this time hopefully.

Version 7.14

12/8/95

Fixed bug when deselecting LHA/LZH. It would crash when checking a LHA file
Corrected guide file again and fixed a few spelling mistakes in main file.

13/8/95

Started work on Check Now stuff. May not be in release version as
functioning. After 4 hours got it completely working. Seems good.

Version 7.15

15/8/95

Corrected small problem with File Watch window gadgets appearing to high
under WB2.04 and 2.1. gadtools.library must handle things differently in 3
Updated nederlands catalog.

17/8/95

Changed how requester is displayed. Text is formatted first, then centred.
Looks alot nicer. No bugs reports from beta testers yet.

22/8/95

Corrected small bug in Arexx interface. Not setting variables.

29/8/95

Corrected small mistake with CheckNow loading option. Watch file would save
to PROGDIR: no matter what.

First release of file. Brainfile 1.22 in this version may vary from the
released version but it is the same one.

Version 7.16

31/8/95

Added Illegal access virus to checker. Seems to detect it okay but stuffs
up the removal. Time for real work so will work on it later

1/9/95

Fixed problem with crashing on 68000 machines when scanning bootblocks
(I hope)
Fixed illegal acces virus problems. Removes it now

2/9/95

Added FileGhost 2 virus to checker. Memory checks in brain file
Fixed WatchNow window not closing on main window closure

3/9/95

Fixed problem where you could open CheckNow window multiple times

Version 7.17 Released 13 September 1995

Added Debugger virus to code
Fixed problem with CheckNow window. Optimizing it I somehow stuffed it up.
Changed size of CheckNow Window for NTSC 640x200 window. Should fit.
Added a special feature to the brain so that it can handle strange checks
Fixed problem with Locale not working. After I tested the locale files I
changed the version numbers but forgot them in the program.
Spelled an Arexx command in the guide the wrong way.
Fixed a possible source of Can’t lock "" requester

Fixed enforcer hit when CMDline Virus_Checker cx_popkey="alt r" given
Fixed bug with Blank requester if ASL.library not found.
Fixed so VC opens version 36 of DiskFont.library which WB2.04 uses unless version 37 has been installed manually
Fixed IgnoreCapture vectors. It was not ignoring them.
Added info to guide on PGP key servers to help getting my key.

Version 7.18 Released 30 September 1995

Small bug in installer. Was putting language files into LOCALE: instead of LOCALE:Catalogs/ when WBStartup given
Added Italian local to archive
Found bug in Icon tool types. Where parsed before the config was loaded so when config loaded it would overwrite changes
Fixed problem with NOWINDOW being ignored as a tooltype
Made Menus Locale aware
Added A=APPICONNAME to SHELL and ICON to set AppIcon name
Added QUIT to ICON type.
Added AppMenuItem. Now can select Check for Viruses from Workbench menu
Removed BootBlock File check. Every man and his dog where turning it on without reading the warnings and then emailing me when they keep getting the UltraFox BootBlock virus in all sorts of files. It is gone and wont be back.

Version 7.19 Not Released. Internal only

Found problem with AFS partition and requesters about "" files and buffers.

Version 8.1 Beta

6/10/95
Have added Main window to checker and removed original. Added help to all buttons. 100% function Next is options window. Fully localised

7/10/95
Have added options window to code. Got it working and removed old options window. Tried with various fonts and falls back to topaz 8 if problems. No help added to buttons yet. 100% function. Works like a charm. Wow this BGUI is easy to program. Should have tried it years ago :-)
Fully localised. Next the hard ones. :-)

8/10/95
Have got File Watch window working. Invisible key added to getfile gadget. It is the G key. F key cycles thru listview but does not actvate it. You have to click on the string with the mouse. Bummer
Must be a good day. Also did Check Now window. Looking good
Started on BBDump window. Should be able to get rid of quite a bit of code with this one gone.
Listview GUI’s look 100% now with a little info from the author of BGUI. He sent me 2 examples. Now thats what I call support.

9/10/95
Got BBDump going okay. alot of shit code taken out. Only window left to do is the Scanning one. Also have to do an iconify mode seeing as BGUI can’t do it. 1am Time for bed
10:30am and time for more work. Got Iconify mode working. If Iconified VC

goes into a small Titlebar. Pressing the right mouse button when window selected will pop it up to full size again.
Will have to add another option though I think. Start Iconfied?
Added another button to options. Start Iconified. This will start VC in the titlebar mode

Version 8.3 Released 16/11/95

Corrected bug in AppIconName. Got BGUI interface working okay. Nothing else done on this.
Due to many things work on VC will be very little. There will be an announcement coming soon on the future of VC.
Anyway enjoy the BGUI interface. It looks much better than the one I did

Version 8.4 Released 10/11/95

Fixed bug with ARexx variable not being returned. Was caused by a register being changed. Program is getting oversized for 16 bit relocatable size. There where reports of Enforcer hits with 8.3. The brainfile although the same number has had some bugs taken out. This was propably the cause. Use this version. I can get no enforcer hits at all.
New version of unpack.library included. many thanks to Thomas.