Virus Scanner

Gabriele Greco

COLLABORATORS

	TITLE : Virus Scanner	

ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY	Gabriele Greco	March 1, 2022	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

1 Virus Scanner **1**

1.1 Contents" . . . 1
1.2 Distribution . . . 1
1.3 concept" . . . 2
1.4 Installation" . . . 2
1.5 notes . . . 2
1.6 is . . . 3
1.7 Localization" . . . 3
1.8 Configuration" . . . 3
1.9 Configuration . . . 4
1.10 Tooltypes" . . . 4
1.11 Tooltypes" . . . 4
1.12 Tooltypes" . . . 5
1.13 Tooltypes" . . . 5
1.14 Tooltypes" . . . 5
1.15 Tooltypes" . . . 6
1.16 Tooltypes" . . . 6
1.17 Tooltypes" . . . 6
1.18 Tooltypes" . . . 7
1.19 Tooltypes" . . . 7
1.20 Tooltypes" . . . 7
1.21 Tooltypes" . . . 7
1.22 Tooltypes" . . . 8
1.23 Tooltypes" . . . 8
1.24 Tooltypes" . . . 8
1.25 Tooltypes" . . . 8
1.26 Tooltypes" . . . 8
1.27 Configuration . . . 9
1.28 Configuration . . . 10
1.29 Features" . . . 10

1.30 Working . . . 11
1.31 New . . . 11
1.32 CheckList" . . . 13
1.33 Gadget . . . 14
1.34 Gadgets" . . . 14
1.35 Gadgets" . . . 15
1.36 Gadgets" . . . 15
1.37 Gadgets" . . . 15
1.38 Gadgets" . . . 15
1.39 Gadgets" . . . 15
1.40 Gadgets" . . . 16
1.41 Gadgets" . . . 16
1.42 Gadgets" . . . 16
1.43 Gadgets" . . . 16
1.44 Gadgets" . . . 17
1.45 Gadgets" . . . 17
1.46 Gadgets" . . . 17
1.47 Gadgets" . . . 17
1.48 Gadgets" . . . 18
1.49 Gadgets" . . . 18
1.50 Gadgets" . . . 18
1.51 Gadgets" . . . 18
1.52 Arexx . . . 19
1.53 Arexx . . . 19
1.54 Arexx . . . 19
1.55 Arexx . . . 20
1.56 Arexx . . . 20
1.57 Arexx . . . 20
1.58 Arexx . . . 20
1.59 Arexx . . . 21
1.60 Arexx . . . 21
1.61 Arexx . . . 21
1.62 Arexx . . . 21
1.63 Known . . . 22
1.64 report . . . 22
1.65 new . . . 24
1.66 to..." . . . 24
1.67 removelink.library" . . . 25
1.68 unpack.library" . . . 25

1.69 bootblock.library" 25
1.70 Safe 25
1.71 Address" 27
1.72 History 27
1.73 Virus 28

Chapter 1

Virus Scanner

1.1 Contents"

```
Virus Scanner v1.04 by Gabriele Greco
-------------------------------------

  What is Virus Scanner?
  Distribution
  Installation
  Configuration
  Features
  Working Method
  Arexx Port
  About new Viruses
  Known Bugs
  Enforcer users...
  Virus Info Base
  Thanks to...
  About SHI
  History Log
```

1.2 Distribution

```
DISTRIBUTION NOTES
------------------

Virus Scanner is freely distributable through BBS, PD collections or cover
disks.

You  can give a copy of VS to a friend without restriction. The only thing
I  ask to the users is to send me or to SHI new viruses and to support the
SafeWare concept, but this is optional.

The  only  important  thing  is  to  keep  safe  your  datas against virus
infections.
```

1.3 concept"

```
WHAT IS SAFEWARE
----------------
'SafeWare'  is a new word I create to describe the condition of use of VS.
If  your  datas are saved from the distruction by my killer please send to
me  10$ (or the equivalent in other currencies, for instance if  you  live
in Italy you can send a "Vaglia" of 15000 Lire) or more and I will send to
you  the  last Virus Scanner version.  Please note that it isn't very much
and you will receive at home a disk.  You can send your cash in any way to

my address,  obviously  specifying  the  address where I
have to send the update.
```

1.4 Installation"

```
INSTALLATION
------------

From version 2.0 Virus Scanner is distributed with a standard C= installer
script to make the installation faster and easy to any user.

To install manually Virus Scanner in your system disk you have to:

1) Drag  the  VS  icon  in the WBStartup drawer or copy VS in C: and add a
   "VS [options]" in your user-startup. (From version 2.0 the program
   detaches itself from the CLI)

2) Copy the removelink.library in your LIBS: assignment.

3) Copy the reqtools.library in your LIBS: assignment.

4) (Optional)  Copy  the  unpack.library  in your LIBS: assignment, if you
   want to turn on the crunched files check capability.

5) (Optional)  Copy  the  bootblock.library in  your  LIBS: assignment and
   copy  the  bootblock.brainfile  in  your L: assignment,  if you want to
   turn on the bootblock viruses check capability.

6) (Optional) If you have Kickstart 2.1 copy the catalog of your favourite
   language in the right place.

   Example: Copy the italiano/VirusScanner.catalog in your locale:catalogs
   /italiano/

7) (Optional)  If  you  want  to use the "install fuckchecker" option, not
   needed  anymore  if  you  let  VS resident, copy fuckchecker in your c:
   directory
```

1.5 notes

NOTES FOR ENFORCER USERS

If you use enforcer you will found VS causes two enforcer hits every <n> seconds, where <n> is the number specified by CHECK_DELAY (default 15). This is due to the access of a function to the page zero that it's illegal. Unfortunately many viruses install themselves in the page zero vectors, then I HAVE to check this vectors.

If you don't want enforcer hits you can of course disable them with the NO_ENFORCER_HITS tooltype, but in this way you loose the possibility of find many (but not all) virus in memory. So if you aren't an enforcer fanatic disable it instead of the memory scan of VS....

1.6 is

WHAT IS VIRUS SCANNER

Virus Scanner is a new conception antivirus commodity for Kickstart 2.0+. It recognises more than 260 viruses (click on the "About" gadget for knowing of how many viruses recognise the current version) and checks also system vectors for possible alteration.

VS is the first fully modular virus checker, copying new versions of the removelink.library, bootblock.library or unpack.library in your libs directory VS will recognise automatically new file or link viruses and new crunchers or archiviers. Obviously it has also his internal virus checking routines that let me update the killer to recognise new viruses without waiting for SHI library updates.

1.7 Localization"

LOCALIZATION

If you use WB 2.1+ the program is also localized. Actually there is only the italian and the german localization, but in the distruibution are included also the ".cd" file and an empty ".ct", so, if you own catcomp you can create your own localization.

Please send me the ".ct" file you create so that I can include it in the distribution of VS.

You can send it to me via e-mail with a matrix to my address.

1.8 Configuration"

CONFIGURATION

THERE ARE THREE WAYS TO CONFIGURE VIRUS SCANNER:

1) Icon Tooltypes
2) CLI arguments
3) GUI and Preferences

1.9 Configuration

1) ICON TOOLTYPES

The tooltypes may be inserted through the "Icon info" option on the Workbench screen.
The tooltype names are case sensitive.

VIRUS SCANNER ACCEPTS THE FOLLOWING TOOLTYPES:

CX_POPUP
CX_PRIORITY
DONOTWAIT
STARTPRI
TOPEDGE
LEFTEDGE
SCREEN
HOTKEY
CHECK_DELAY
USE_UNPACK_LIB
NO_ENFORCER_HITS
DONT_CHECK_MEMORY
CHECK_COLDCAPTURE
STAY_RESIDENT
PROGRESS_WINDOW
USE_SCREEN_FONT
HIDE_REQUESTERS

1.10 Tooltypes"

HIDE_REQUESTERS

USAGE: HIDE_REQUESTERS

If this tooltype is specified some requesters (the close requester and the file scan results) will not be displayed.

1.11 Tooltypes"

PROGRESS_WINDOW

USAGE: PROGRESS_WINDOW=(YES|NO)

If you select "YES" on this tooltype every time you perform an option it will be opened a small window making you known of what VS is doing.

1.12 Tooltypes"

STAY_RESIDENT

USAGE: STAY_RESIDENT=(YES|NO)

If you set this to "NO" VS will check every devices for bootblock and file viruses and than it will exit freeing your memory.
Default is "YES".

1.13 Tooltypes"

CHECK_COLDCAPTURE

USAGE: CHECK_COLDCAPTURE=(YES|NO)

This is for the people who uses Skick or Zkick or other programs that use the coldcapture vector to stay resident after a reset.
If you run a similar program and you hate "Warning, the coldcapture vector is not zero..." requester every time you run VS with the tooltype: CHECK_COLDCAPTURE=NO you will not be disturbed anymore by that requester.
Default is "YES".

From version 1.03 this tooltype stops also the KickTagPtr checking for people with a A1200 with a non autoconfig memory expansion.

1.14 Tooltypes"

DONT_CHECK_MEMORY

USAGE: DONT_CHECK_MEMORY

If you do not want to waste a little of your cpu time with a periodical check of memory for viruses (about the 0.5% on a 68030 if you perform the check every two seconds, see the CHECK_DELAY tooltype)

1.15 Tooltypes"

```
USE_SCREEN_FONT
---------------

USAGE: USE_SCREEN_FONT

If you select  this tooltype all Virus Scanner windows will use the default
screen font instead of the system font used by default.
The  screen  font is generally bigger than the default font, so I prefer to
use as default font the system font to make the vs gui smaller.
In  my  interlaced  system I use a xfont 9 as system font and a times 13 as
screen font. You can change the  settings  of  your system with the program
"prefs/font".
In a non-interlaced system ntsc system I doubt that VS will be open  with a
font with height >8, if you select a font too big to make the window fit in
screen VS will be automatically open with a topaz 8 font.
```

1.16 Tooltypes"

```
NO_ENFORCER_HITS
----------------

USAGE: NO_ENFORCER_HITS

If  you  specify  this  tooltype  in  the  VS  icon  it  will  disable  the
removelink.library scan memory function.
This  operation causes two enforcer hits because  of the access to location
in the page 0  of  the memory and usually it's performed every five seconds.
If you set this tooltype there will be not enforcer hits but you will loose
the possibility of  removing  many  virus  from  the  memory  ( all the ones
that uses to live in the page 0 vectors).
```

1.17 Tooltypes"

```
USE_UNPACK_LIB
--------------

USAGE: USE_UNPACK_LIB

I have included this tooltype because of the not very high stability of the
current  version of the unpack.library.  It  has  some  problems  on  68000
machines and can cause crashes during the file scan.
Previously  this tooltype was DONT_USE_UNPACK_LIB, but with the new  switch
in the GUI I've disabled the unpack.library by default.
Specifying  the  tooltype the unpack.library will be enabled by default and
VS will check all the crunched files...

Without  the  unpack.library  the  VS check files  process never fall (with
it sometimes with  some  configurations  can  crash  the machine), but  VS
 will not be able to check crunched  files.  If  you aren't working on very
important datas you can use unpack.library.
```

This option can be accessed also through gui with the switch:
"Check Crunched Files".

From version 1.50 I've revert to an older, but more stable, version of unpack.library, waiting a new update.
I any case DON'T use unpack v39.50 because it's a beta version...

1.18 Tooltypes"

CHECK_DELAY

USAGE: CHECK_DELAY=seconds

This tooltype let you choose how many seconds will divide one memory check to the other. The default value if you don't specify this tooltype is 5. You can insert values from 2 to 60, if you specify values out of this range will be used the default value.

1.19 Tooltypes"

TOPEDGE

USAGE: TOPEDGE=y coordinate

The vertical position in which VS window will appear on the WB screen. Default is 0.

1.20 Tooltypes"

LEFTEDGE

USAGE: LEFTEDGE=x coordinate

The horizontal position in which VS window will appear on the WB screen. Default is 0.

1.21 Tooltypes"

HOTKEY

USAGE: HOTKEY=<hotkey format>

This is the combination of keys that will popup VS window if it's hidden.

Default is <control+V>.

Example: HOTKEY="control v"

1.22 Tooltypes"

USAGE: CX_PRIORITY=(from -5 to +5)

CX_PRIORITY

Sets the priority of the commodity.
Default is 0.

1.23 Tooltypes"

STARTPRI

USAGE: STARTPRI=(from -20 to +20)

Set it to an high value if you want VS starting before others commodities.
Default is 0.

1.24 Tooltypes"

DONOTWAIT

USAGE: DONOTWAIT

Use it if you want to put VS into WB startup.

1.25 Tooltypes"

CX_POPUP

USAGE: CX_POPUP=(YES|NO)
If it's YES when VS boots it will popup his window.
Default is YES.

1.26 Tooltypes"

```
SCREEN
------

USAGE: SCREEN=<Public Screen Name>

Name of the public screen in which VS will be opened.
Default "Workbench".
```

1.27 Configuration

```
2) CLI ARGUMENTS
----------------

If you run VS from CLI or in the user-startup you may need to configure VS
via command line.

VS does not need the run command it detaches itself from the CLI.

If you type "VS ?" from the shell you will see the available options...

PRI=PRIORITY/N,CE=CHECK_EVERY/N,NR=NORES/S,NP=NOPOPUP/S,NC=NOCHECKCOLD/S,
NU=NOUNPACK/S,NH=NOENFORCERHITS/S,NM=NOMEMORYCHECK/S,PWIN=PROGRESSWINDOW/S,
TOP=TOPEDGE/N,LEFT=LEFTEDGE/N,HK=HOTKEY/K,,SC=SCREEN/K,SF=SCREENFONT/S

PRI or PRIORITY   (from -128 to 127) - Alter the priority of the commodity.

CE or CHECK_EVERY (from 2 to 60) - Change the distance between two memory
                                   check. (default 5 seconds)
NU or NOUNPACK - If this option is specified the unpack library will be
                 ignored.

NH or NOENFORCERHITS - This option disable the page zero memory check, that
                       cause enforcer hits...

NR or NORES - If this option is specified VS will check the memory, every
              disk drive bootblock, the startup-sequence and the it will
              quit.

NP or NOPOPUP - Use this to start VS with the program window hided.

NC or NOCHECKCOLD - This tooltype prevent VS to check the ColdCapture
                    vector and the KickTagPtr, for compatibility with
                    some cards and rekickers.

LEFT or LEFTEDGE (y coordinate) - Left coordinate of the main window.
                                  Default 0.

TOP or TOPEDGE (x coordinate) - Top coordinate of the main window.
                                Default 0.

HK or HOTKEY (hotkey string) - Specify the key combination to popup the
                               program window. Default <control v>

SC or SCREEN (screen name) - Public Screen Name in which open VS.
```

SF or SCREENFONT - VS will use the screen font.

Example:

VS NOPOPUP LEFT 100 TOPEDGE=50 CHECK_EVERY 10 HK "shift control s" NU

This example shows the way you can use the various keyword in the standard 2.0 format...

1.28 Configuration

3) GUI & PREFS

Through the "configuration panel" of the GUI you can configure practically every aspect of the program.

You can set the boolean gadget as you want and then you can save the configuration that will be automatically loaded the next time you load VS.

The setting are saved in a file called s:vscan.prefs, in the distribution there is an example.

1.29 Features"

VIRUS SCANNER FEATURES

Virus Scanner has many usefull features as the periodical check of every memory vector, of the startup-sequence and of the process you have in background. This operations are performed without any loss of processor speed, unlike Virus Checker.

VS can remove Fuck Virus from memory and from disk.

VS recognises every file/link virus available at the moment and using if possible the New Virus Database feature let VS knows also virus that it originally doesn’t know. For the news ones look at the virus wanted list.

VS uses the SHI bootblock.library, so with an update of the bootblock. brainfile it can recognise and delete any new bootblock virus.

VS uses the SHI removelink.library, so with a new version of the library you can kill new viruses.

Using the SHI unpack.library VS can decrunch and check files compressed withmore than 100 different crunchers.

VS can be localized.

VS has a complete AREXX port.

VS has a complete system vectors and function call table in a superbitmap window.

VS checks the memory every n seconds (where n is a number between 5 e 60 at your choice, see CHECK_DELAY).

VS has a known virus list and a known cruncher list.

VS has a feature that automatically check at each access to a disk if a file, in a list you make, has been modified.

VS is the only VirusKiller that can determine if a disk was FFS or OFS after the infection by a bootvirus checking the files structure on the disk before installing a new bootblock.

VS has a new feature for Amiga antivirus, but already present on some MS-DOS programs that let the user specify in a file called s:vscan.viruses the datas of new viruses (New Virus Database).

1.30 Working

WORKING METHOD

After the execution VS will:

1) Load prefs file.
2) Load the list of files to check
3) Check every disk-drive for a bootblock virus.
4) Check every system device (df0: dh1: ram: pc0:...) for a startup-sequence infected.
5) Check exec vectors(Cold,Cool,WarmCapture,kick,memtagptr...)
6) Check for memory infections.
7) Check the files in the CheckList.

Then during the execution VS will check:

1) every time a disk is inserted if it's infected by a bootblock virus.
2) every second if an exec vector has been altered.
3) every second if a process virus has been added to the process list.
4) every second if a new virus is installed in memory.
5) every disk access if a file in the CheckList has been altered.

The other action are available through the GUI, or through the arexx port.

1.31 New

NEW VIRUS DATABASE

This is a absolutly new feature for amiga antivirus, let you specify in a file (s:Vscan.viruses) the datas of viruses that the vs version you own

doesn't recognise. This datas will be spread through the SHI warnings and through the various network (internet, fidonet, amiganet). The new virus datas will be spread only by authorized people and SHI members in the following format:

Message about the virus type and what does it do...

<Virus Name> ASCII

<Offset> Decimal string (if from the beginning positive, if from the end negative)

<Buffer Length> Decimal string

<Buffer> Hex description of the buffer

For example you can find in the fidonet area amiga.eur:

From: Gabriele Greco
To: All
Subject: New Virus!!!
Date: 1-1-94

Warning there is a new very dangerous virus, we call it "dir" virus for the TERRIBLE damage that it do:

If this virus (present in every amiga OS version) is executed without parameter it will list on a console window every file or dir present in the current directory, TERRIBLE! :-))

These are the virus datas:

dir command v40
672
11
444952532f532c46494c45

....or something like this :-)

This data must be inserted in your file in the following format:

filename s:vscan.viruses

line 1: number of virus datas contained in the file
line 2: Virus name 1
line 3: Offset 1
line 4: Buffer Length 1
line 5: Buffer 1
line 6: virus name 2
line 7: Offset 2
[.....]

This is a vscan.viruses example (the files aren't real viruses):

--cut-----cut-----cut--
3

```
dir command v40
672
11
444952532f532c46494c45
rename command v40
992
8
2f412f4d2c544f3d
assign command v40
-12
6
4a0166d44e75

--cut-----cut-----cut--
```

The virus inserted in the file in this way will be recognised in a scan like a normal VS internal file/link virus.

In a next future this feature will be upgraded to have in the hex buffer also wildcard capabilities.

1.32 CheckList"

```
CHECK LIST
----------
```

With the menu option 'automatic check...' you can edit a list of files to check at every disk access.

You can add items to the list or remove them. The total number of items must not be more than 40. But if you use more than 15 items your disk operations may be slowed a lot.

To save your changes you have to return to the main menu and perform a "Save Prefs".

Alternatively you can directly edit the following file that is the one VS load and save.

This is an example file:

```
-----File: Vscan.files------
4
s:user-startup
s:shell-startup
s:startup-sequence
c:loadwb
```

the first line show the number of files in the list.

The other lines are the full path file names to check.

If you have a file like this named "Vscan.files" in your s: directory VS will load it and then at every disk access it will check if any of these files has been modified. It recognise also if the modify is made by CED and doesn't report it. If you or a virus modify one of the selected files, for example with an ' echo >>s:user-startup "dir" ', VS will report

a requester warning you that s:user-startup has been modified. In the distribution there is an example s:vscan.files

1.33 Gadget

GUI

GENERAL GADGETS

Quit
Hide
About
Save Prefs

CONFIGURATION GADGETS

Check ColdCapture
Check Crounched Files
Show Progress Window
Window Popup
Popup Key

ACTION GADGETS

Check Files
Check All Devices
Check Sectors
Check Vectors

MENU ONLY

List Crunchers
Install a FuckChecker
List Viruses
New Virus Database
Automatic Check

1.34 Gadgets"

Quit

Quit VS and free his resources.
You can also quit with the "Remove" option of Commodities Exchange or similar programs.

Available from menu or gadget.

1.35 Gadgets"

```
Hide
----

Hide VS, you can recall it pressing the Hotkey (default ctrl+v) or through
commodities exchange.
You can also hide the GUI with the "Hide Interface" option of  Commodities
Exchange or similar programs.

Available from gadget.
```

1.36 Gadgets"

```
About
-----

Show  some  informations  about the program including  the number of virus
detected and the actually used brainfile version.

Available from menu or gadget.
```

1.37 Gadgets"

```
Save Prefs
----------

Save the current setting.

Available from menu or gadget.
```

1.38 Gadgets"

```
Check ColdCapture
-----------------

If deselected disable the coldcapture check, thought for SKick users.
See also CHECK_COLDCAPTURE tooltype.

Available from gadget, tooltype or CLI argument.
```

1.39 Gadgets"

```
Check Crunched Files
--------------------

Enable the unpack.library crunched file check. If you enable it the  files
```

crunched with one of the about 100 packers recognised will be decrunched and checked, but obviously the scan will be slower than the one without crunched file check.
See also the USE_UNPACK_LIB tooltype.

Available from gadget.

1.40 Gadgets"

Show Progress Window

If selected every option will show with a string what the program is doing. See also the PROGRESS_WINDOW tooltype.

Available from gadget, tooltype or CLI argument.

1.41 Gadgets"

Window Popup

If selected the program will popup his window after the execution. See also the CX_POPUP tooltype.

Available from gadget, tooltype or CLI argument.

1.42 Gadgets"

Popup Key

Let you choose your favourite popup key for VS. It accepts the standard C= hotkeys format. See also the HOTKEY tooltype.

Available from gadget, tooltype or CLI argument.

1.43 Gadgets"

Check Sectors

Check for sector infection a disk drive unit (0..3), it's useful to see if your disk has be infected by a saddam, lamer, fuck or other sector destroyer viruses. In some cases (Saddam) can recover the datas encoded by the virus. In future this feature will work also on hd.

Available from gadget.

1.44 Gadgets"

```
Check Files
-----------
```

This option will let you check the files of a directory. You have to choose a directory (use shift to select more than one at once or "all" to scan the entire device) and press ok on the file requester.
During the file scan you can skip a directory, pause the scan or abort the scan clicking on the "VS Report" window.

Available from gadget or menu.

1.45 Gadgets"

```
Install a FuckChecker
---------------------
```

It Installs in a device you are prompted to select a copy of FuckChecker, a little program that checks if your LoadWB is infected before running it.

Now it isn't of many use because the latest VS versions will kill the virus without problems, but it's useful for the disk users that can install only the little fuckchecker instead of a copy of VS in each system disk...

Available from menu only.

1.46 Gadgets"

```
Check Vectors
-------------
```

Open a window that show the status of all the system vectors and of all the libraries patches (skick, zkick and rekick compatible).

1.47 Gadgets"

```
List Crunchers
--------------
```

Open a window containing the names of all the file crunchers/archivier VS is able to recognise and decrunch for check compressed files, it will work if the unpack.library is installed.

Available from menu only.

1.48 Gadgets"

List Viruses

Open a window containing the names of all the viruses VS recognises:
(link+file+bootblock).

Available from menu only.

1.49 Gadgets"

Automatic Check

Let you edit the CheckList items through an easy to use ListView kind gadget. Use "Add" to add a file to the check list and "Delete" to delete an exising one.
Once a filename is added at the list it will checked at every disk access.

Available from menu only.

1.50 Gadgets"

New Virus Database

This is the GUI of the New Virus Database i've introduced from version 2.00 of the program, look also at this section for more info.
To insert a new virus you have to click on the "Add" gadget and to enter the virus name, then you'll have to enter the hex string, obviously an even number of digits and finally to enter the offset in which the string has to be searched.
To delete a virus simply select the virus name and then click on the "Delete" gadget.

1.51 Gadgets"

Check All Devices

Checks all devices of the system for bootblock infection, if you select "yes" in the requester also the files of the device will be scanned.
With the "Skip Device" gadget on the "Report" window you can skip the file scan of the current device, with "Abort" you can skip the entire scan process.

Available from menu or gadget.

1.52 Arexx

AREXX COMMANDS

Virus Scanner own also, as every respectable 2.0 program, an Arexx port that let you drive many operations of the program via arexx. These are the Arexx command you can send to Virus Scanner after an: address "VS_Port"
Many commands that usually display requesters to confirm actions if executed through arexx will not pop any requester then if a file is infected will be automatically processed and if a trojan is found will be automatically deleted and so on.

Command list

 SHOWGUI
 HIDEGUI
 VECTORS
 CHECKALL
 CHECKBOOTBLOCK
 CHECKFILES
 SHOWPROGRESS
 ABOUT
 QUIT
 CHECKFILE

The default extension of Virus Scanner Arexx scripts is .VS

If the argument of a command requires colon (':') you have to enclose it into ('') this is a limit of the arexx syntax.

Examples:
checkfiles dh2:prova/ (DOESN'T WORK)
checkfiles 'dh2:prova/' (THIS WORKS FINE)
checkfiles dh2 (WILL WORK TOO)

1.53 Arexx

Syntax: SHOWGUI

Action

Shows the program GUI.

1.54 Arexx

Syntax: HIDEGUI

Action

Hide the program GUI.

1.55 Arexx

```
Syntax: CHECKBOOTBLOCK (DF0|DF1|DF2|DF3)

Action
------
With this command you can check the bootblock of an ALREADY inserted disk.
Infact when a disk is inserted it's checked automatically.

Examples:
rx "address 'VS_Port' checkbootblock df0"
rx "address 'VS_Port' checkbootblock df0:"
```

1.56 Arexx

```
Syntax: VECTORS

Action
------
Make  a  check of all system vectors. These vectors are also automatically
checked every 2 seconds.
```

1.57 Arexx

```
Syntax: CHECKALL

Action
------
Check Everything (Files & bootblocks of every device).

IF A VIRUS IS FOUND it's automatically deleted without requesters, because
this command is made for a script execution.

If  an  archived or crunched file contains a virus it will be deleted too,
In the case of an archive the entire archive will be deleted.

So if you plan to check archivied files it's better to check them directly
with the "check a disk" option.
```

1.58 Arexx

```
Syntax: CHECKFILES <DeviceName>

Action
------
With  this  command  you  can  check  the  files  of  a  selected  device.

If  a  device  name  contains  colon you will have to enclose it into (').
```

If a virus is found it's automatically deleted (or processed if it's a link) without requesters, because this command is made for script execution.

If an archived or crunched file contains a virus it will be deleted too, in the case of an archive the entire archive will be deleted.

So if you plan to check archivied files it's better to check them directly with the "check a disk" option.

Examples:
rx "address 'VS_Port' checkfiles sys"
rx "address 'VS_Port' checkfiles 'dh2:work/'"

1.59 Arexx

Syntax: ABOUT

Action

Same as clicking on the About gadget. Display program informations.

1.60 Arexx

Syntax: SHOWPROGRESS (ON|OFF)

Action

This command turns on/off the progress window.
See also the gui and configuration sections for more details.

1.61 Arexx

Syntax: QUIT

Action

Quits Virus Scanner from Arexx. Useful if you want to perform some checks and then free the memory for others applications.

1.62 Arexx

Syntax: CHECKFILE <filename>

Action

For BBS use, to check a file for file and link viruses. It is very power-

ful because can check also files crunched with LHA/LZH or DMS using the unpack.library.

The filename must be enclosed within (') if it contains colon (:). If the file checked is infected by a virus the command will return a return code of 10. So you can use it also in a DOS script.

This is valid both for normal files than for compressed ones. So if an archive uploaded to your bbs contains a virus you can copy it to a personal directory containing bad uploads.

The file isn't deleted by VS. You have to do it of your own in the arexx/-dos script.

Examples:
rx "address 'VS_Port' checkfile 'dh1:loadwb'"
rx "address 'VS_Port' checkfile 'dh1:uploads/stuff.lha'"

1.63 Known

KNOWN BUGS

Actually VS has not known bug, if you find one please report it to me, but the current unpack.library version has some problem with some crunched files but only on certain configurations.

To avoid this problem I've choose to disable the unpack,library by defaut and to permit to use it through a switch in the gui "Check Crunched Files" a tooltype in the icon (USE_UNPACK_LIB) or an argument on the command line UU=USEUNPACK.

These are the first versions of my program and so also if Giuseppe Vicari and I have longely tested the program it is surely not bug free so if you find new bugs use The bug report form and send it to me or
send me an E-Mail!

1.64 report

BUG REPORT FORM

Well, I really hope I don't see too many of these come back, but here it is anyway.

If you should happen to find a bug in any of the programs as supplied, AND.... you've taken ALL....the time to thoroughly read the documentation.

If you still mean there is a bug, then PLEASE.... take your time to print out the bug report form shown below, fill out the details and return it to me or send the bug report form to the actual SHI library programmer,

```
if one of these  anti-virus libraries mabe have a bug.

Cut here <
--------------------------------------------------------------------------------

                              BUG RAPPORT FORM            DATE:

--------------------------------------------------------------------------------
NAME:
--------------------------------------------------------------------------------
ADDRESS:
--------------------------------------------------------------------------------
COUNTRY:                                      PHONE:
--------------------------------------------------------------------------------
WHICH PROGRAM:                                  REVISION:
--------------------------------------------------------------------------------

YOUR MACHINE CONFIGURATION (use e.g. Sysinfo):
----------------------------------------
1.  Amiga 500               Amiga 600                Amiga 1000
    Amiga 2000 A            Amiga 2000 B             Amiga 2000 C
    Amiga 2500              Amiga 3000               Amiga 4030
    Amiga 4040              Amiga 1200               Amiga CD 32


2.  1/2 MB chipmem                      Fat Agnus (old) 8371 A
    1/1 MB chipmem                      Big Agnus (Fatter) 8372 A
    2/1 MB chipmem                      ECS Agnus (Hires) 8372 B
    Fast RAM                            Total RAM

3.  Denise (old) 8362                  ECS Denise (new) 8363

4.  Kickstart 2.0     Kickstart 3.0     Kickstart 3.1     Kickstart

5.  Special Boards and like (e.g. AT-Card, Action Replay, Turbo Card) :




6.  Your motherboard revision

7.  How old is your Amiga

--------------------------------------------------------------------------------

Details of the bug:
------------------
```

```
------------------------------------------------------------------------
Cut here <
```

1.65 new

```
IF YOU ARE INFECTED WITH A NEW VIRUS
------------------------------------
```

If your believe your amiga is getting mad, if a disk full is reported as empty, if you believe your amiga is infected by a virus you can send it to me, or to SHI (if you send it to me I'll send it as soon as possible). I'll try to fix your disk and if it's infected with a new virus your name will be written into the documentation.

THE CONTENTS OF THE DISK ARE IRRILEVANT, I DON'T LOOK IF IT'S A PIRATE DISK OR NOT. I'M INTRESTED ONLY BY THE VIRUS.
Then send your infected disks to my address.

1.66 to..."

```
Thanx to:
---------
```

* Giuseppe Vicari, my first betatester, but more than that. Many of the features of this killer are his ideas, and he help me also with some programming problem.

* Luca Spada, for the fuck virus infection in his BBS that make me decide to write a killer. :-)

* Marco Lizza, my second betatester.

* Max Zuercher, for the german catalog.

* Flavio Stanchina, for useful programming tips and the G-zus packer.

* Erik Loevendahl Soerensen, for the SHI support.

* Paul Browne, for putting me in contact with SHI.

* Nico François, for the reqtools.library.

* Jan Van Den Baard, for GadtoolsBox I use to make the VS gui.

* Thomas Neumann, for his excellent unpacker.library

* Johan Eliasson, for his excellent bootvirus.library

* Johan Ohrman, for his excellent removelink.library

* Flemming Lindeblad, for the danish catalog.

* Marco Van Der Heide, for the dutch catalog.

* Stephan Schüerholz, for german catalog improvements.

1.67 removelink.library"

REMOVElINK.LIBRARY BY JOHAN OHMAN

This library can detect more than 90 file/link viruses (and their clones) and disable it, from memory or from disk.

1.68 unpack.library"

UNPACK.LIBRARY BY THOMAS NEUMANN

The unpack.library let VS recognise more than 100 different packers and unpack their crunched files to check if them are infected by a virus.

1.69 bootblock.library"

BOOTBLOCK.LIBRARY BY JOHAN ELIASSON

This library in conjunction with the L:bootblock.brainfile can recognise more than 200 bootblock viruses.
From version 1.06 I'm doing the new bootblock.brainfile updates, so if you find some new virus you can send them also to my address.

1.70 Safe

ABOUT SAFE HEX INTERNATIONAL

If you know a virus programmer you can get a reward of $1000 for supplying his name and address. The fact is that the law punishes data crime very severely (5 years in jail in most countries).

We are an international group with more than 500 members who are trying

to stop the spread of computer viruses. Let me give you some examples:

1. Our motto is: "Safe Hex, who dares do anything else today?"

2. We run a virus bank containing more than 1800 Amiga and PC viruses for supporting good shareware anti-virus programs.

3. We help people to reclaim money lost by virus infection.

4. We write articles about virus problems for about 20 computer magazines worldwide.

5. We release the newest and the best virus killers around from about 25 well-known programmers worldwide.

6. We have more than 35 PC and Amiga "Virus Centres" worldwide where you can get free virus help by phoning our "Hotline", and the newest killers translated into your own language at very little cost.

7. Of course we hope you can see how important your support is for the global anti-virus fight, (please remember to send new viruses).

As an example of our efforts the following programs currently use SHI anti-virus libraries:

* Virus Checker by Johan Veldthuis

* Virus Scanner by Gabriele Greco

* DMS by ParCon Software

* D-Copy by Stefan Bernbo

* XCopy from April 93 Cachet Software (commercial)

* Fides Professional by John Lohmeyer

* Fides Checker by John Lohmeyer

* Xtruder BBS virus killer by Martin Wulffeld

* MT-Copy by Gert-Jan Strik

For more information contact:

SAFE HEX INTERNATIONAL
Erik Loevendahl Soerensen
Snaphanevej 10
DK-4720 Praestoe
Denmark

Phone: + 45 55 99 25 12

(Please send 2 "Coupon-Response International" and a self addressed envelope, if you want information about SHI by letter).

Fax : + 45 55 99 34 98

1.71 Address"

You can write to me or send to me infected disk, new translations, contributions or bug reports at the following address:

Gabriele Greco
Via Banchi 12
I-16030 Uscio (GE)
Italy

You can write to me also via e-mail or send me uuencoded virus or crunchers at the following addresses:

Gabriele Greco
Fidonet : 2:331/106.7@fidonet.org
Internet: gabry@grifone.skylink.aare.net.ch

1.72 History

History Log

A bit short now....

02-01-94 1.0 First Version, not publically released.

26-01-94 1.01 Fixed some bugs and modified the "list virus" option, added german and french catalogs. Reduced the code of about 2K, with optimization and replacing some ansi C functions with custom ones.

23-02-94 1.02 Modified the Check Disk option, now check files, can check also a dir. Modified the menu routine, now it uses the screen font. Some little bugs removed. Some little catalog modifications.
Now distribute with unpack.library 38.40

09-03-94 1.03 Lot of little bugs fixed from user reports, some internal changes, now the Automatic Check option should works properly...
Now distribute with unpack.library 39.50 and with danish catalog by Flemming Lindeblad of SHI.

12-03-94 1.04 Some update to the documentation and a totally new "Check Files" selection routine with multiselect capabilities. "Cruncher list" option rewritten.

15-04-94 1.50 Not released, added more improvements and made major internal changes and this version became the...

```
(From version 2.0 the version number is in the C= Standard (2.12 > 2.2)

25-06-94        2.0  New  font sensitive  modified  GUI, totally rewritten
                     startup  and CloseDown  routines,  new option: "Check
                     Sectors",  new GUI to edit the "new virus"  file, new
                     tooltype SCREEN to  open VS on a public  screen, some
                     changes  and speed up to the "Check Files" and "Check
                     All" options,  improved  menu  layout,  new language:
                     dutch  catalog  by  Marco  Van  Der Heide, new  shell
                     interface (no more with tooltypes), many little  bugs
                     fixed.
         New tooltype USE_SCREEN_FONT (default is system font)
         New Brainfile 1.05 recognising  about 30 new  viruses
                     and 50 clones. The brainfile version 1.05 is the
                     first realized by me, now the new bootblock.library
                     updater.
                     New version of unpack.library 39.51, hangs no more on
                     68000 machines.
                     New  internal  support for Eleni link/file/boot virus
                     and other 11 file/link viruses.
         --NOT RELEASED--

22-09-94        2.1  New unpack.library (39.53), new brainfile (1.07),  5
                     new misc viruses supported and 4 new bootviruses.
         Some  internal  revisions, updated documentation, new
                     installer script. New tooltype HIDE_REQUESTERS.
```

1.73 Virus

```
 VIRUS INFO BASE
 ---------------

Virus Info Base is the SHI official Virus  Database,  it is continuosly
updated to give information about effects and way of elimination of all
the amiga viruses.
```