# VirusExecutor

| COLLABORATORS | | | |
|---|---|---|---|
| | *TITLE* :<br><br>VirusExecutor | | |
| *ACTION* | *NAME* | *DATE* | *SIGNATURE* |
| WRITTEN BY | | July 31, 2024 | |

| REVISION HISTORY | | | |
|---|---|---|---|
| NUMBER | DATE | DESCRIPTION | NAME |
| | | | |

# Contents

# Chapter 1

# VirusExecutor

## 1.1 VirusExecutor.guide

VirusExecutor v2.17
1992 © 2001 by Jan Erik Olausen
All Rights Reserved



## 1.2 install

HOW TO INSTALL VIRUSEXECUTOR

Just start the VE_Install program and follow the instructions...

That's it!

## 1.3 copyright note

COPYRIGHT NOTE
---



VirusExecutor is FREEWARE. This program may be freely distributed as long as:
- the executable and documentation remain unchanged and are included in the distribution

```
   - no other charge is made than to cover time and copying costs
```

## 1.4 disclaimer

```
DISCLAIMER
----------
No warranties of any kind are made as to the functionality of this
program. You are using it ENTIRE at your own risk.
VirusExecutor has no known bugs and no Enforcer hits!
```

## 1.5 system requirements

```
SYSTEM REQUIREMENTS
-------------------
 * All Amigas with OS2.04 or higher

 * xvs.library
   Copyright Georg Hörmann and Alex van Niel
   Included within this archive
   Used for finding and removing virus
   VirusExecutor will not run without it

 * xfdmaster.library
   Copyright Georg Hörmann and Dirk Stöcker
   Not included within this archive
   Used for decrunching crunched files
   VirusExecutor can also run without this library, but then you can't
   check crunched files for virus

 * xadmaster.library
   Copyright Dirk Stöcker
   Not included within this archive
   Used for extracting archives
   VirusExecutor can also run without this library, but then you can't
   extract and check archives for virus

 * reqtools.library v38.11 or higher
   Copyright Nico François
   Not included within this archive
   Used for requesters.
   VirusExecutor will not run without it
```

## 1.6 features

```
FEATURES
--------
VirusExecutor (VE) is a virus killer that's meant to be easy to use. There's
no 'advanced' options in the program that you almost never use anyway.
This doesn't mean that VE is in the lack of power!
```

```
 * Easy to use (hopefully) ;)

 * Checks and download new versions of important files from Aminet

 * Automatically analyzes an unknown bootblock. Detects 99% of any new virus.

 * Bootblock database for recording of utilities boots, loaders etc.

 * Checks executables and data files

 * Checks files in LHA/LZX/ZIP archives (more to come)

 * Checks memory every 3 seconds for viruses

 * 'File watch' feature

 * A huge patch brain with over 1.600 known patch entries

 * Locale support
```

## 1.7 getting started

```
GETTING STARTED
---------------
Try it out and ask me if there's something that you don't understand...
This guide is very simple. I will write a better one later...

 STARTING
 ********
 When you start VE you will see some information about VE. Versions of the
 libraries that VE use, how many bootblocks/files VE has checked etc.
 Press "Ok" to continue.

 Next, the memory check windows will appear.

 Next, VE loads the bootblock database, if any.

 If you start VE for the first time, a prefs window will pop up.

 BOOTBLOCK CHECKING
 ******************
 Every time you insert a floppy disk into any drive, VE will check and display
 the bootblock from that disk.
 A star (*) after the text DF0: - DF3: shows the bootblock which are currently
 displayed on the screen.

 Comment: Here you can install a standard AmigaDOS bootblock or a bootblock
          from the database.


                                    MENUS
                                    *****

 Project
```

```
 File watch
 Show
 Install
 Bootblock database
 Utilities

                                  BUTTONS
                                  *******
 Click me
```

## 1.8 project

```
                            The 'Project' menu
                            ******************

About
  This opens a window viewing all important information like external
  libraries in use, PatchBrain version etc...

Prefs
  A new window is poping up where you can select some flags...
  Press the 'Esc'-key to quit and save the new preferences.

  Decrunch files
  --------------
  If selected, VE will decrunch all crunched files supported by
  the xfdmaster.library. If you don't have this library this box is ghosted.
  The latest xfdmaster.library is found on aminet. Just search for
  xfdmaster.lha

  Overwrite crunched files
  ------------------------
  If selected, VE automatically rewrites the decrunched file buffer over the
  original crunched file... This is useful if you have a lot of crunched,
  files but really don't want them to be crunched.
  VE asks just ONE time if you want to preform this operation if a crunched
  file is found.
  If you check non-writable devices, like CD-ROMs etc, VE turns off this
  selection during this check and turns it back on next time you do a file scan
  on a writable device.

  Skip encrypted files
  --------------------
  If selected, VE skips all encrypted files...
  Those are files that requires a password to run.
  If not selected you have to enter the right password in order to check
  encrypted files.

  Check data files
  ----------------
  If selected, VE checks all no-executable files as well.
  You should only have this flag selected once in a while just to check
  all data files.

  Extract LHA, LZX, ZIP
```

```
  ---------------------
  When selected, VE unpacks all #?.LHA|LZX|ZIP files and check inside them.
  If a virus is found, you have to unpack this file after the check and do
  a new file check in order to remove the virus.

  VE don't check archives in an archive! I will try to fix this later...
  You MUST have the LHA, LZX and the UnZip programs located your C: directory.

  Skip files older than [] day(s)
  -------------------------------
  If selected, VE don't check files that are older than # days.
  You also have to specify who many days to skip.
  0 = Only checks files that is new to the device TODAY.


  Hide known patches
  ------------------
  If selected, VE only shows unknown patches to the system.
  If you choose the menu command 'Check memory' VE shows all patches always!
  This flag should always be selected, or else the patch window pops up every
  time a patch is changed, and that happens a lot on my system :)

  Fast startup
  ------------
  If selected, VE don't show the about window or the patch window at startup.

Memory check
  Some window pops up telling some usefull stuff!

  1. window (Memory check)
  First a window pops up showing information about the kickstart version and
  ROMUpdates. If there is a known virus in memory VE will tell you so.

  2. window (Vector check)
  Here VE tells you which program that are using the vectors for resident code
  etc.
  List KickTagPtr: Shows programs using the KickTag pointer. Most of the
                   programs listed here survives a warm reboot.
  List KickMemPtr: Shows programs using the KickMem pointer. These programs
                   don't survive a warm reboot.
  Restore Vectors: Resets all vectors/residents files in memory.
                   All programs are still working in memory, but will not
                   survive a warm reboot. If VE can't restore these vectors
                   it might be a virus fooling around, and VE asks you if you
                   want to do a CoolReboot.

  2. window (CPU Interrupts Vectors)
  Just shows the status of the CPU interrupts vectors.

  3. window (Exec Interrupts Vectors)
  Just shows the status of the exec interrupts vectors.

  4. window (Device/library Vectors)
  Here you can see what function that is patches by a number of programs.
  If you click a function a new window will pop up showing an Hex/ASCII view
  from that address. VE knows a lot of programs that patches the system using
  the PatchBrain file (VirusExecutor.patches). For now the PatchBrain
```

recognize over 1600 patches from over 200 programs. And the PatchBrain will be updated a lot so be sure to check AmiNet or the Virus Help Denmark's homepage to see if any new brain is released.

ColdReboot
NOTE! All external memory and peripherals will be RESET!
And the machine will start its power up diagnostics.

File check
A file requester pops up and you can select which device/drawer you want to be checked using the options from the prefs setings.
During file checking you can press the 'Esc'-key to pause/abort this check.
I will explain more later...

Sector check
Checks for virus within the sectors of a floppy disk.
Not fully tested. Use it on your own risk!

Select screen mode
Here you can select your own screen mode.
I will explain more later...

Quit
This will quit VE and save the prefs settings.

## 1.9 file watch

The 'File watch' menu
**********

Check now
Goes through all the files that you have added to the file watch data base and check if there's a different in the file size. If the file size has not changed it checks if the CRC-32 has changed...

If there's a different a requester pops up asking you if you want to save these changes. If the file C:Dir has changed and you are 100% sure that you haven't replaced it with a newer version etc, it might be a virus somewhere. If a lot of files has changed it's probably some virus.
Please do a file scan of that dir and send some of the changed files to me if the file scan couldn't help you out.

Pressing the Esc-key aborts the file watch checking

NOTE
A requester pops up if a file that is in the data base has been deleted from your device so you can remove it from the file watch data base.

Add a directory

Add files from a directory to the file watch data base.

A small window pops up:

'Include data files'

```
  Select this flag If you want to include data files.

  'Include icons (.info)'
  Select this flag if you want to add icons to the file watch.
  Only availible when 'Include data files' is checked.

  'Confirm every file'
  Select this flag if you want to manually confirm which files that should
  be added to the file watch data base.

  'Add'
  Choose a directory to add files from using the file requester.
  You can use assigns as they will be converted to their original path in
  the data base
  After selecting a directory the files will be added to the data base using
  the flag settings above.

  'Done'
  Closes this window.

Add/update startup files

  Scans the s:startup-sequence and s:user-startup script for files and adding
  them to the file watch data base. Files in the WBStartUp directory will also
  be added.

Remove files

  A window with all files added to the file watch data base opens and you can
  just click the file you want to remove from the data base.
```

## 1.10 show

```
                          The 'Show' menu
                          ***************

Bootblock virus

  All boot block virus known by the xvs.library will be listed.

Link virus

  All link virus known by the xvs.library will be listed.

File virus

  All file virus known by the xvs.library will be listed.

Tasks

  All tasks (programs) running will be listed.

Libraries

  All libraries in memory will be listed.
```

Devices

  All devices in memory will be listed.

Patches

  All patches known by VirusExecutors patch brain will be listed.

## 1.11 install bootblock

                          The 'Install' menu
                          ******************

DF0: - DF3:

  Install a bootblock to the drive DFx:

  Select type of bootblock or a bootblock from the bootblock database
  and click the 'Install' button.

## 1.12 bootblock database

                     The 'Bootblock database' menu
                     *****************************

Record

  Records a bootblock from any drive to the bootblock data base.

View

  A window pops up and you can click a recorded bootblock to view.
  Press the close window button to exit.

Edit name

  If you want to change the name of a recorded bootblock this might help
  you out.

Merge

  Merges another bootblock data base to your own data base.

Delete one

  Deletes a recorded bootblock from the bootblock data base.

Delete all

  Clears the entire bootblock data base.

Save

If changes has been made this will save the bootblock database.

## 1.13 utilities

The 'Utilities' menu
********************

Rename pictures

Just choose one image and VirusExecutor does the renaming for you...

Examples:
Image0 -> Image.00000
Image1 -> Image.00001
Image03 -> Image.00003
Image15 -> Image.00015

Convert IBN/IBM/IBMM to ISO

Converts a PC ASCII text file to plain Amiga text

Save ROM to file

Writes the entire ROM that you are using, and saves it as a file.
You can then use this ROM file with Amiga emulators on other platforms etc.

Update files

When you are on internet you can use this option to get the latest versions of the following:

VirusExecutor main archive, VirusExecutors patch brain, xvs.libray, xfdmaster.library and xfdmaster.library

Just select the nearest Aminet site, and if a newer version is availible you can download the file from VirusExecutor. Note that the VirusExecutor download files to RAM:

## 1.14 buttons

KEYS
----

* Esc - Pauses fil checking and asks if you want to abort...

* Numeric 0-3 - Shows bootblock of that drive if you have more than one drive on your system.

* F5 - Quits VE. Next time you start VE it will use the WB-screen... This will be added to the prefs window later.

## 1.15 to do

```
TO DO
-----
* More patches :)

* Better prefs
```

## 1.16 thanks

```
THANKS
------
Many thanks to following persons which helped to improve VirusExecutor:

 Jan Andersen for sending me new virus

 Georg Hörmann and Alex van Niel for the xvs.library
 Georg Hörmann and Dirk Stöcker for the xfdmaster.library
 Dirk Stöcker for the xadmaster.library
 Nico Françies for the reqtools.library

 And thanks to all who translated VirusExecutor...

 The BETA testing crew:
 Philip Bang, Vegar Pedersen, Robert Westad, Roar Syversen, Trond Larsen,
 Jørn Tillnes, Rune Mindresunde, Jan Tore Sandvik and Jan Andersen

 Special thanks to Michaela Prüß for her major beta testing of v2.01 and
 for the nice glow icon :)
```

## 1.17 history

```
HISTORY
-------
2.17  - Added virus: Bastard Installer and Bastard Install Script
      - Improved hunk stripping while checking files...
      - Fixed some bugs in the bootblock data base load/save/merge
      - Fixed bug when bootblock checking text was to long.

2.16  - VE can now check for archives in archives in archives ...
      - Improved hunk checking when checking for Bobek virus.
      - Rewritten the whole file check routine.
      - Fixed bug if file time checking is more than 1 hour.
      - Fixed bug from v2.13 that "freeze" the machine while decrunching
        or extracting arhives... Should also take care of the mouse "freeze"
        while checking for memory.
      - Some small improvements.

2.15  - Added internal removal of the new Bobek link virus
      - Improved error output from xadmaster.library when checking
        archives.
      - Requiers xadmaster.library v9.0 instead of v10.0
```

```
2.14  - Fixed enforcer hit when adding files from SYS:WBStartup
      - When Enforcer or CyberGuard is running the MMU: text turns blue.
      - Using xadmaster.library for extracting archives.
      - Improved Bastard file checking a bit
      - Added memory checking and file checking for Bobek link virus
        Please wait for a new update of the xvs.library for removals of
        the Bastard and Bobek virus...
      - Shows only the diskdrives that you have.
      - Removed the requester 'VirusExecutor is allready running'
        When starting VE when VE is allready running the screen just come
        to front and get active.

2.13  - At last, fixed the font problem when running VirusExecutor from
        Workbench... Please let me know if there still are font problems.
      - Added some mem pointers for OXYRON Patcher v3.13 and CyberGuard
      - Fixed $VER: string.
      - When checking a lot of archives a file called T:VEpfh become quite
        big. Fixed.
      - Bug when pressing the 'Esc'-key more than one time during the file
        checking is fixed.
      - When pressing stop if a linked virus is found wouldn't stop. Fixed.
      - Fixed xvs.library and xfdmaster.library check at startup.
      - Starting VirusExecutor without the assign caused membugs. Fixed.
      - Fixed Enforcer hit when checking memory...

2.12  - Renamed the new TeamMOS TCP Trojan to Zakahackandpatch
        and fixed small bug in the decrypting code...
      - Added 'Bastard' link virus...
        Thanks to Zbigniew Trzcionkowski for the great analyzes of
        this virus... I'm using his code to disable it from memory...

2.11  - Forgot to remove 'TeamMOS HPA TCP Trojan' from memory...

2.10  - Saves the VirusExecutor.prefs fil to VirusExecutor:
        The old prefs fil in the S: dir will be deleted by VE...
      - Added BootControl v2.1 to memcheck
      - Added internal check for the new 'TeamMOS HPA TCP Trojan' Virus

2.09  - Added OS 3.9 ROM updates.
      - Added SystemPatch

2.08  - Added a save request after a file watch scan
      - You can now press the Esc key to abort the file watch checking
      - Added more text to the Aminet update if your screen height is
        bigger than 319 pixels
      - The guide should be a lot better now :)

2.07  - Fixed bug when reading readme file from Aminet
      - Rewritten a lot of the boot block analyze function.
        Just did it for fun. Who use disks anymore :)
      - Fixed some bugs in the 'File Watch' scan and adding...
      - Added: remove files from the file list

2.06  - Fixed faulty lib versions when starting VE if the 'Fast startup'
        flag was off.
        Thamks to Charlene Mcnulty for telling me about it :)
```

```
2.05  - VirusExecutor no longer crash when no screen mode is selected
        at first time run.... Thanks to Per M. Iversen who reported
        this bug.
      - Now you can check if there is new versions of VirusExecutor,
        VEPatchBrain, xvs.library and xfdmaster.library from Internet.
        If a new version is available you can download directly from VE.
        Right Amiga-U does the trick.
        Remember to be on the net :)

2.04b - Fixed bug when closing screen at the Workbench window
      - Added 'File watch' to the menu
      - Displays the release date of the xvs.library in the about window
      - Removed CPU speed... To many bugs... and not very important :)

2.03  - Fixed bug: The patch window didn't pop up at startup if there
        was unknown patches in memory
      - Added more OS 3.5 ROM Updates to the PatchBrain
      - Added a simple log file... See VirusExecutor.log
        Just logs if a virus is found. Please tell me what you want
        the log file to log! I will make some prefs options for this later
      - Fixed bug when a data virus was found
      - Added a 'Fast startup' flag to the prefs window.
        When checked, MHZ-check and the about-window are disabled at
        startup
      - If you have OS 3.5 a VirusExecutor glow icon is used.
        Thanks to Michaela Prüß for making this nice icon
      - Added 'Skip files older than ##### days' to the file checking prefs
      - Centered the prefs window...
      - Added an option to open VirusExecutor on the WorkBench screen
        Press F5... This will also be an option in the prefs window later :)
      - VirusExecutor also shows the version of the ROMUpdate if found
      - Fixed some minor bugs in KickTagPtr-checking:
        Miami Deluxe was found as Miami and ROMUpdate 44.1 was not recogized
      - Better guide... Don't say a thing! I'm still working on it :)
      - Added a BUG REPORT text file...

2.02  - Some virus is hidden deep inside linker-files. VE is now unlinking
        all links and not just one...
      - VE is now stripping hunk_name ($3e8).
      - MEMF_LARGEST is removed during file check. Little faster now :)
      - If you have the 'Overwrite crunched files'-flag selected, VE check
        if the drive is writeable... If not, the flag is turned off during
        file checking...
      - Updated some CPU speeds..
      - Added more patches to the PatchBrain
      - Fixed small bug when viewing patch memory
      - Added more devices and libraries to the patch checking
      - Added MMU check to the main window
      - Added 'ColdReboot' to the 'Project' menu
      - When a new patch is detected a <-- is displayed behind it.
        I hope :)
      - Fixed Miami-bug in PatchBrain. Should be SetPatch.
      - Added internal LVO-names... More to come...
      - From now on the latest 'xvs.library' is included in the archive

2.01  - Added more program to resident check
```

```
      - Fixed bug in GFX-chip checking (hopefully)
      - Added CPU speed in MHz. Just for fun :)
      - Some fonts have the same ID as zip-files... Fixed
      - Rewritten vector check routine... Should be much better now
        (hopefully) :)
      - Added more patches to PatchBrain
      - Fixed bug. VE was showing the wrong FPU sometimes...
      - VE now skips HARD- and SOFT links directories during file checking
      - Added VirusExecutor: assign
      - Sector checking can no be used on all 4 drives
      - When the 'Skip encrypted files'-flag was set, no crunched files
        was decrunched. Fixed...

2.00  - Locale support: Norsk, dansk, deutsch and français
      - Added 154 patch entries...
        Also added patches to gadtools.library, layers.library and
        icon.library
      - Fixed patch bug... ToolManager patch was screennotify.library
      - Major upgrade of the vector checking... Added reset resident
        programs to an internal database...
        Please let me know which program you use so I can make an update
        All resident programs that VE don't know, is mark *** UNKNOWN ***
      - VirusExecutor crashed when screen mode was not available. Fixed
      - Fixed 'empty-line' bug in the patch output window
      - Fix small bug in 'Convert IBN...' if tekstdata ended with a '\0'
      - Added devices to the patch checking
      - I think all this work is worth a 2.00 version! :)

1.84  - Changed VirusExecutor.patches again!
        I forgot to include the patch names within this file :)
      - 'Error 1200' was a typing mistake in v1.83c only. Fixed
      - From the prefs window you can now select an option to
        hide known patches.
        If this option is set and you choose 'Check Memory'
        from the menu, VirusExecutor will show all patches!
      - Added 'SmartCrash v1.1' to the patch brain
      - Added 'playsid.library' to Interrupt Vectors

1.83c - When starting VE, windows pop up only if there's a virus in
        memory or if an *** UNKNOWN VECTOR *** patch are detected
      - Added a meny function to view known patches
      - The "VirusExecutor.patches" file is now much smaller
      - Added patch: 68060.library, CyberPatcher, SnoopDos v3.0

1.83b - Improved and fixed some minor bug to the patch checking.
      - Added a few more patches. More to come...
      - Fix a bug when "*** UNKNOWN VECTOR ***" in CPU Interrupt checking.
      - Fixed FPU: 68040 when it was a 68060, again :)
      - Removed some internal viruses. Please get the xvs.library v33.19!

1.83a - Added "AMOS Joshua Clone Trojan"
      - 060FPU was showing as 040FPU. Fixed!
        Thanx to Jarle Eidet for telling me about that.

1.83  - Added "AMOS Joshua Trojan"
      - Major upgrade on vector and patch checking. This is just a preview.
        I had to release this version because of the new Joshua virus
```

```
1.82f - Added to prefs: Skip encrypted files
      - In encryped files, password was always wrong. Fixed
      - While typing password, no output is seen.
      - Improved Zakapior file checking
        VE is now encrypting the file...
      - Fixed an error msg that pops up as an CLI message when VE
        couldn't lock a directory
      - VirusExecutor is now listed in the task window

1.82e - Added sounds to VE :)
      - Added vector check for kickstart 40.70
      - Fixed small bug in List KickMemPtr output
      - Added a utility to save internal ROM to a file
      - Changed some text output
      - When clearing vectors, interrupt was not restored. Now fixed
      - Added DF0: sector checking

1.82d - Added kickstart 40.60/40.63/40.68 in vector check
      - When inserting a A1000 kickstart disk VE prints out
        the kickstart version. Anyone have kick 1.0 and 1.4 beta?

1.82c - VE now shows all tasks.. Sorry :)
      - BUG: The vector window pops up only if the vectors are changed
      - VE can now show entries using KickMemPtr

1.82b - Added a prefs window (BETA).
        VE goes directly to the prefs window when new preferences
        has been added.
      - Fixed the 'Error 12000' (I hope)
      - Added vector checking. Not very good, but I'm working on it.
      - VE can now display Tasks, libraries and devices...

1.82a - VE now sorts files when scanning disks for virus
      - Sorry, forgot to remove 'Zakapior' virus from memory, fixed!
      - Shows only filename of the infected file within an archive
        (Not the whole path)
      - Added more info while scanning files if you have big
        enough screen :)
      - Added zip arhcive, please use:
        UnZip 5.32 of 3 November 1997, by Info-ZIP. Maintained by Greg Roelofs.
        (found on Aminet)
      - Added memory scan during file checking


1.82  - Added a 'Select Screen Mode' requester (lots of requests)
      - Added auto remove link/file virus...
      - Cleaned up some code...
      - Rewritten file scan code... Much safer now.
      - Checks files in LHA/LZX archives (more to come)
      - Added "Zakapior Trojan" virus (internal, not xvs.library)

1.81c - VE can now unlink linked files... Thanks to Jan Andersen for
        sending me some linked files.
      - Removed stupid requester: "Seems like you own an old VirusExecutor".
      - And some other stuff that I don't remember :)
```

```
1.81b - VE is now using xfdmaster.library for crunched files.
      - After VE removes a link virus it now checks the file again
        for more viruses until the file is clean.

1.81a - Rewrite analyze function of encrypted bootblocks.
        Fix a small bug when the bootblock was a standard 1.3+.
      - Forgot to report the error message if a link virus couldn't be
        removed.
      - Also forgot to ask if you want to delete a data virus
      - Cleaned up some code and text output.

1.81  - First Aminet release.
```

## 1.18 jeo

Jan Erik Olausen
Email: virusexecutor@c2i.net
Norway

http://home4.inet.tele.dk/vht-dk/amiga/

## 1.19 locale

English is the build in language but VirusExecutor supports the locale.library. That means that you can easy translate from english to your language...

Just email me back the translated catalog file and I will include it in VirusExecutors archive...

Catalog writers:

| | |
|---|---|
| dansk | - Jan Andersen |
| deutsch | - Michaela Prüß |
| français | - Jean-Marc LEROUX |
| magyar | - Dósa Márton |
| italiano | - Andrea Zanellato |
| polski | - Michaî Sobieraj |
| português | - Alfredo Martins |
| norsk | - Jan Erik Olausen |
| slovak | - Juraj Mátel |
| svenska | - Börje |