

Safe

COLLABORATORS

	<i>TITLE :</i> Safe		
<i>ACTION</i>	<i>NAME</i>	<i>DATE</i>	<i>SIGNATURE</i>
WRITTEN BY		January 20, 2025	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

1	Safe	1
1.1	1
1.2	Contact with author	1
1.3	What is Safe	2
1.4	Requirements	3
1.5	How it works	3
1.6	What it gives me	4
1.7	Rest	4
1.8	To translators	5
1.9	Parameters	5
1.10	5
1.11	6
1.12	6
1.13	6
1.14	6

Chapter 1

Safe

1.1

English documentation to program

Safe version 13.3

written by

Zbigniew 'Zeeball' Trzcionkowski

Read all, please!

Safe is FREeware program

(c)1998-2000 by Zbigniew 'Zeeball' Trzcionkowski

What is Safe?
Shell parameters
Requirements
How it works?
What it gives to me?
Some words to translators
History
Contact with author

1.2 Contact with author

Zbigniew Trzcionkowski
Astrow 7

43 250 Pawlowice
Poland

Send me bug reports, ideas and infected files

100% answer to all disksenders

e-mail:

zeeball@interia.pl

or:

t_error@interia.pl SUBJECT: for zeeball
siumot@amiga.org.pl SUBJECT: for zeeball

You can download Safe from VHT-DK page:
www.vht-dk.dk

And You can download Safe from Polish page:
<http://amiga.org.pl/~siumot>

Look for newest versions in Aminet - util/virus!

To see results of testing Safe click here.

Special thanks to:

Jan Andersen of VH-DK for viruses

Tomasz 'Siumot' Bielinski for Fungus, testing TCP patch of Safe,
and several ideas/bug reports

Tomasz 'Error' Wiszkowski for all... ..bugreports... :)

1.3 What is Safe

Safe is small CLI command to detect link-viruses in Your system.
This program checks memory and itself only when running
and NOT resides anywhere in memory.
The only resident thing is TCP patch - see parameters
If You want resident memory guard use the one from new Fungicide archive
by DigitalCorruption.
The philosophy of Safe differs little bit because this tool
is designed also to discover new viruses.
All You have to do is to use my installer script
or put Safe icon to Your partition and run it when
You need.
Don't forget that Safe runned more times = safer system,
so You can add also Safe to buttons of Opus, Diskmaster etc.

Example of Safe with Diskmaster:

```
AddCmd Parent, 10, Parent ; StdIO "CON:0/12/640/100/Alert!/AUTO"; Extern Safe; ←  
StdIO CLOSE
```

Don't rename Safe file!
Don't try to crunch this file!
Put to Your LIBS: newest xvs.library you have
(To get version numbers of current xvs and Safe type 'safe VER' in Shell).
Safe can discover new viruses only when it's file is placed
in write-enabled device with some free space.
Standard RAM: cannot be used because it's always 100% full,
and lot of viruses can't infect files placed in RAM:

I added also small util to run Safe every 10 seconds.
It's doc is somewhere near this util.

If Safe works - you will not see anything.
If virus found you have to run big viruskiller like
VirusZ and remove it.
If new/unknown virus discovered send it to author of
your antivirus or to VHT-DK
You can send me file too.

1.4 Requirements

You need operating system 2.0 or newer

To recognition and memory removing of known viruses
You need xvs.library by Georg Hormann and Alex van Niel

To write report with REP parameter you need asl v38+
Same to write memory with SAVEMEM

To install TCP patch You need 'resident' command in C:

Other problems should be sent to:

zeeball@interia.pl

1.5 How it works

1.It checks memory for HNY99/IOZ, PolishPower, NeuroticDeath 1-2
and for viruses known by xvs.library...

2.It checks it's file for size, changed instructions,
known viruses

3.If something found You'll got messages in CLI.
Progam will try to recognize and remove problem
from memory via xvs.library or internal routines...

The file is written in special format for known link-viruses

to provoke infection.
I think that 90% of link-viruses will attack this file,
so will be detected.
Also TCP: trojans/viruses activity can be detected
with installed TCP patch.

1.6 What it gives me

Detects in Your system lot of link-viruses.
Discovers new link-viruses.
With TCP patch can also see activity of TCP trojans/viruses.

There is another tool similiar to Safe.
It's TheUltimateProtector by Andreas Falkenhahn. This one gives
to user possibility of checking some files every selected period
of time. So if You have fast HDD (Elbox's FastATA or SCSI)
You can use this program instead, but don't forget that You have
to choose many files, and better uncompressed, to provoke
infection (or use Safe file, but it detects infections itself).
People with slower HDD should use Safe added to
buttons of Opus, DiskMaster etc.
Dont't forget that Safe in selfcheck uses antistealth abilities,
so can detect 'invisible infections'!

1.7 Rest

Bugs: as always :-)

To do: lot of things

History:

size
v12.4 - 7000, improved VECS and SAVEMEM, optimized
v12.5 - 7000, added simply KickTag lister to VECS
v12.6 - 7000, fixed small bug, thanks for Tomasz Wiszkowski
for Muforce report
v12.7 - 7000, fixed small bugs, removed TurboVal from archive,
now it is available in util/boot
v12.8 - 7000, fixed another bug (thanx to Tomasz Wiszkowski
for trying to get any bug report until crash),
tested with more link-viruses (Thanx to Jan Andersen)
v12.9 - 7000, compatibilized with PatchControl (thanx to Tomasz Wiszkowski
for the show), fixed PolishPower checking
v13.0 - 7000, added to VECS possibility of remove any patches
from LoadSeg and NewLoadSeg
v13.1 - 7000, small fixes in Safe and docs,
Note to Roy Krister - I've checked RENRAM and it is OK...
v13.2 - 7000, tested with another virus,
added memory test for rexxfunc trojan (Thanks for Paul),
kit to detect unknown Vaginitis Clones (see AntiVag dir)
v13.3 - 7000, added new tool - QUICKTEST to remove rexxfifo and rexxfunc
trojans from HDD

1.8 To translators

If You want to make a translation just make it and send to Aminet.

The main executable file is only in english and still.

Translations of guide must be as separate file.

Translations of installer must be added to script and sent to me.

1.9 Parameters

Safe offers from CLI/Shell template:

REBOOT/S, RENRAM/S, TCPATCH/S, VER/S, REP/S, WBLOCK/S, VECS/S, OWNOUT/S, RUNVAL/S, SAVEMEM/S, NOPOLPOW/S

REBOOT - gives standard reboot without clearing reset vectors
 RENRAM - renames Ram disk: to RAM: This helps with some programs
 TCPATCH - installs patch to detect TCP: trojans/viruses
 VER - shows version of Safe and xvs.library
 REP - opens filerequester to save Safe's report to file
 WBLOCK - performs LockPubScreen(NULL) to prevent WB closing
 VECS - Shows some system vectors.
 Shows also special result of simple heuristic check.
 Most of tested viruses resulted Suspicion=50+,
 but don't forget that this is only suspecting,
 so the legal patches could cause big numbers too!
 Allows You to remove any patches from LoadSeg and NewLoadSeg!
 CLRVR - sets VBR to 0
 OWNOUT - forces use of new CON: window to talk with user
 RUNVAL - runs 'VAL' util. It have to be installed in C dir
 SAVEMEM - saves memory to file. You will be asked for start addy, end addy,
 and then choose filename from asl requester.
 At the moment size limit is 4096 bytes.
 NOPOLPOW - overjumps PolishPower test which saves 16/50 of second
 It is suggested to use it on startup because
 it is not needed to check for PolishPower which appears
 with delay.

1.10

hunk - in AmigaDos executable file means a part of it.

When You run program the system function LoadSeg will load different hunks of file to different places in memory.

The most popular hunks (called in assembler - sections) are:
 code - binary program for MC680x0 processor, small datas etc.
 data - datas of program (pictures, modules etc.),
 programs for Copper, etc.

bss - used to put big empty areas to programs without increasing their size on disk.
Contains only data about length of empty areas.

reloc- contains data about relations between other hunks which must be recalculated when hunks are loaded to memory

end - 4 bytes - only identifier. Used at the end of other hunks. System doesn't need it in some hunks, so code hunk added by FileShield is 4 bytes smaller.

1.11

linkvirus - means a real virus. Classic Amiga linkvirus adds it's code to executable files to be spreaded with them. When user runs successfully infected file the virus code is executed and the virus adds it's code to one of system functions (LoadSeg, Write, Open etc.) When the function is used the virus tries to infect another file.

On Amiga are two main ways of file infection:

1. first hunk increasing
2. hunk adding

1.12

first hunk increasing - adding virus code at the end of first hunk (if code hunk) and replacing one of MC680x0 instructions with jump to virus code.

Most popular instructions to be reinserted are: RTS, BSR, JSR, MOVE.L 4.W,A6

Safe from 11.0 can display some changed instructions.

1.13

hunk adding - adding to file hunk(s) with code of virus. This is NOT so easy to make good hunk adder, so there are more first hunk increasers.

The other comparable methods are adding new HunkHeader etc.

1.14

TCP viruses/trojans - normal viruses or trojans(faked libraries, programs)
that opens remote net door by making secret
shell in TCP: device.

Example of shell names

```
Fungus linkvirus           : TCP:1666
rexxkuang11.library 0.36  : TCP:2551
rexxkuang11.library 0.27  : TCP:2333
```

To detect this kind of elegal activity I have added to Safe
parameter 'TCPPATCH' which show message when something will try
to create shell in TCP:

TCP e-mail senders are not supported because I don't heave idea
how to recognize them.
