Safe

COLLABORATORS			
	TITLE : Safe		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		April 15, 2022	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

Safe

1.1

English documentation to program

Safe version 11.7

written by

Zbigniew ‘Zeeball‘ Trzcionkowski

Read all, please!

Safe is FREEWARE program

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

You can also contact me by Tomasz 'Siumot' Bieliïski.

His e-mail:
siumot@amiga.org.pl

And download Safe from his page:
http://amiga.org.pl/~siumot

Look for new versions in Aminet also - 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

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.

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

To write report with REP parameter you need asl v38+

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

1.5 How it works

```
                1.It checks memory for HNY99/IOZ and viruses known by xvs. ↩
                   library
2.It checks it's file
3.If something found You'll got messages in CLI.
  Progam will try to recognize and remove problem
  from memory via xvs.library.

The file is written in special format for known
             link-viruses
                to provocate 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 provocate
infection (or use Safe file, but it detects infections itself).
People with slower HDD should use Safe added to
buttons of OpusDiskMaster etc.
```

1.7 Rest

```
                Bugs: as always :-)

To do: lot of things

History:
         size
 v11.0 - 5000, crypted all code and texts to protect against
               modifications caused by lamers/funny people,
               added displayer of file length before and after,
               added messages about reinserted instructions
               (
             hunk increasing viruses
             ),
               fixed bug in TCP patch (code wasn't 100% PURE),
               added new parameter - REP/S. If You have asl v38+
               filerequester will appear to save Safe messages
               to file, now the texts from Safe will appear even
               from an icon (there was bug),
               added to docs informations about new Safe's site in net
               all 100% tested with Enforcer, Mungwall and Scratch
 v11.1 - 5000, added xfdmaster support to recognize name of cruncher
               when file is crunched and to check hunk structure,
 v11.2 - 5000, added WBLOCK/S parameter, removed XFD code because
               was quite useless, tested with some existing viruses
 v11.3 - 5000, optimized, tested with more viruses, begun adding new
               feature - built in vector analyzer (VECS/S in

             parameters
             )
 v11.4 - 5000, added auto-killer of CrM patch, added heuristic
               vector check in most popular dos.library functions,
               added antistealth abilities (for HitchHiker)
```

```
    v11.5 - 5000, added showing of pr_WaitPkt in strategic processes,
                  other additions in VECS/S
    v11.6 - 5000, added more antistealth abilities (for Beol96),
                  added waiting for validation of Safe's home device
    v11.7 - 5000, added reset of VBR by holding LMB
```

1.8 To translators

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

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.
```

1.9 Parameters

```
                Safe since version 10.6 offers from CLI/Shell template:

REBOOT/S,RENRAM/S,TCPPATCH/S,VER/S,REP/S,WBLOCK/S,VECS/S

REBOOT   - gives standard reboot without clearing reset vectors
RENRAM   - renames Ram disk: to RAM: This helps with some programs
TCPPATCH - 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     - at the moment shows some system vectors.
           Shows also special result of simple heuristic check.
           Most of tested viruses resulted Suspicity=50+,
           but don't forget that this is only suspecting,
           so the legal patches could cause big numbers too!
           Another important thing is pr_WaitPkt field
           in strategic processes - always should be 0!
```

1.10

```
hunk - in AmigaDos executable file means a part of it.
       When You run program the system function LoadSeg
       will load diffrent hunks of file to diffrent 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 datas 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
             FileShield fights with this kind of
             viruses.
             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 hunk adder, so there are more first hunk
increasers.
FileShield fights with this kind of virus via
using Reloc32Short unknown for very big part of them.
By the way - FileShield works like this kind of virus because
adds its own code hunk :-)
```

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 added to Safe (from v10.4)
   parameter `T` which show message when something will try
   to create shell in TCP:
```