results

COLLABORATORS			
	TITLE : results		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		January 20, 2025	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

results

1.1 main

```
Safe was tested with some viruses known by xvs.library.

Safe have also build in routines for recognition of HNY99/IOZ512.

Xvs don‘t have routines for NeuroticDeath viruses (they crashes on
all available configs).
Safe 12.1+ have build in memory removals for NeuroticDeath1&2.
Note that those viruses are very buggy, so the removals
will work 100% ok only on Amigas where the viruses work ok :-(
Address of NewLoadSeg is lost by virus (LoadSeg instead).
The truth is even worse -  on my config LoadSeg and NewLoadSeg
jump from virus contains strange numbers like $050314541. Only DoIO was ok.
BTW. This means that those viruses can‘t spread (they causes
GURU when You try to run something).
Note that from now You can remove any working patches from (New)LoadSeg
by typing ‘Safe VECS‘.

Xvs don‘t have routines to detect and remove from memory PolishPower.
Safe have internal routines to detect this one and disable in memory!
Safe will install patch on exec/Wait to detect and disable
PolishPower in memory for 16/50 of second (or forever if found)!
I‘ve not analyzed whole virus, so this is possible that there exists
better way to fix it. The virus was very strange to me,
and contains strange stuff like creating of invisible Process...
If any AV guy want this patch to use then just ask at:
error@alpha.net.pl with subject: ‘to zeeball‘ for this piece of code...
It costs only one greet for my humble person :-)

It also can detect infection of it‘s file by future viruses.

Name    - name of the virus
Detection - in memory and Safe‘s file


Results:
Name      Detection Changed instructions reported
          (if hunk increasing virus)
------------------------------------------------------------------------
```

Aram-Dol	OK	RTS, LastRTS
Beol	OK	-
Beol2	OK	-
Beol3	OK	-
Beol'96	OK	-
Commander	OK	jsr -x(Ay)
Crime92	OK	Last RTS; RTS
Ebola	OK	jsr -x(Ay)
Fungus/LSD	OK	Last RTS
HitchHiker1.10	OK	2*move.l 4.w,a6
HitchHiker2.01	OK	2*move.l 4.w,a6; Last RTS; RTS
HitchHiker3.00	OK	2*move.l 4.w,a6; Last RTS; RTS
HitchHiker4.11	OK	-
HitchHiker4.23	OK	-
HNY98	OK	Last RTS
HNY99/IOZ512	OK	Last RTS
NeuroticDeath1&2	ok (only memory, the virus crashes known systems)	
PolishPower	OK	
Polizygotronifikator	OK	2*move.l 4.w,a6

TCP new shell detecting patch was tested with net code ripped
from Fungus/LSD virus. The result was also OK!

For the LoadSeg viruses the heuristic vector analyzer gives
big numbers even for HNY99/IOZ512 (not included in xvs),
so it is good to analyze unknown patches!

Thanks to Jan Andersen for supporting me in viruses!