zeebsvs

COLLABORATORS

	TITLE : zeebsvs		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		July 31, 2024	

REVISION HISTORY

NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

zeebsvs

1.1 main

```
--------------------------------------------------------------------

Welcome to:

Zeeb'sVS v1.0

(c) 2001 by Zbigniew Trzcionkowski

Contact: zeeball@interia.pl

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

Zeeb'sVS IS MEMORY PATCH FOR XVS.LIBRARY!!!
JUST RUN THE FILE AND YOUR xvs based ANTIVIRUS BECOMES MUCH BETTER!

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

WHAT IT DOES?

1. It patches functions of xvs.library with my own additional routines.
2. It adds patch protection for SurveyMemory() which MUST be
   untouchable for viruses because this function must be able to
   heal the memory from the possible retro-viruses that might want to
   block entrance to that function!
3. It keeps the internal protections so SelfTest() still works for
   whole library authorization.

   *******************************************************
   *                                                     *
4. * RECOGNIZES ALL FILES INFECTED WITH HITCH-HIKER 5.00! *
   *                                                     *
   *******************************************************

5. It doesn't correct virus lists, but my favourite joke
   seems to be removed now.

--------------------------------------------------------------------
```

```
DISCLAIMER

I take no resposibility for my program and for results of it’s work.
All output from my patches is in [brackets], so You know
where to send thanks. What is more important this is beta version
I have done within days and many things will change or be added later.

To do:

1. Change patch protection to polymorphic timer.device based routine.
2. Add ND4 and ND5 removals. ND5 seems hard because it uses multilayered
   polyengine and stills one of the hardest viruses for Amiga ever.
3. Add closing of TCP: ports for other Vaginitis viruses
   (please send them to me)

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

WHY?

1. The most important thing was that I have been attacked
   with intelligent advices and ideas. The problem was why I am so
   passive and so on... THAT would make him/them rethink it before
   another attempt to annoy me.

2. I have noticed that I AM THE LAST ACTIVE ANTIVIRUS GUY who
   understands disassembled code.
   There already is much my code in xvs, so why loose possibility
   of quick updates of MY routines?

3. First Jan Erik’s HH 5.00 file detection almost broke me mentally,
   and even now it leaves about 20% of HH5 decoders undetected.

That’s in short why I didn’t sleep during last two weeks
and spent probably last sunny days in home.


AV greets for: Markus Schmall, Soenke Freitag, Dirk Stoecker,
               Jan Andersen and even Jan Erik Olausen who has
               lost my respect for months.

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

Improvement list:

  SurveyMemory()

        CheckFile() and RepairFile()
```

1.2 check

```
CheckFile() added virus/trojan file detections:
-----------------------------------------------------------------------

NeuroticDeath 1, 2, 3, 3d, 4 and 5
```

```
kills intended droppers of these viruses



CheckFile()/RepairFile() new linkviruses:
-----------------------------------------------------------------------

IOZ512

detects and cleans files infected with this virus
This is old and easy clone of HappyNewYear'96, but I have learnt much
from it since it was first hunk incresing virus I came into in late 1998.
It gave me motivation to develop Safe package and so on...
VirusZ died in that time, so it has never been added.
1998... just history... :-P


NeuroticDeath 1
NeuroticDeath 2
NeuroticDeath 3
NeuroticDeath 3 delta

detects and cleans files infected with these poymorphic viruses.



HitchHiker 5.00

detects all generations of this very polymorphic virus,
so if xvs didn't detect it my patch surely will. At the moment files
detected with my patch are delete only.
```

1.3 surv

```
SurveyMemory() added virus memory removals:
----------------------------------------------------------------------

IOZ512/HNY99

removes LoadSeg() patch


NeuroticDeath 1, 2, 3, 3d, 4 and 5

removes DoIO, LoadSeg, NewLoadSeg patches or interrupt server
if virus detected antivirus and hidden itself quickly


PolishPower

removes invisible interrupt with technique discovered by me,
that makes this task easy and extremally quick!
Previous memory removals were just a joke!
```

rexxfunc trojan

removes fake processes called ’SetPatch’ and closes TCP:2000 port
opened by that virus

SurveyMemory() fixed virus memory removals:

BOBEK 2

removes invisible interrupt with the my new technique used
for PolishPower too

Expl0de trojan

added closing of TCP:9876 port opened by that virus

Fungus

added closing of TCP:1666 port opened by that virus

Port 2421

added closing of TCP:2421 port opened by that virus