Heuristik

COLLABORATORS			
	TITLE : Heuristik		
ACTION	*NAME*	*DATE*	*SIGNATURE*
WRITTEN BY		March 2, 2022	

REVISION HISTORY			
NUMBER	DATE	DESCRIPTION	NAME

Contents

Chapter 1

Heuristik

1.1 Heuristik Module for VirusWorkshop - Written by Markus `Flake/TRSI` Schmall

Heuristik Scanner Module for VirusWorkshop 5.7 and coming ↩
versions

1.2 Author - Who am I ?

My name is Markus Schmall and I am since 5 years programming this lovely machince called AMIGA. I have started with some so called demonstrations, since I got first infected with the Lamer Exterminator Bootblockvirus. I started coding my my own viruskiller, better known as VirusWorkshop.

I am currently studying at the university in Hildesheim , located near Hannover/West Germany.

1.3 Contact adresses

If you want to contact me, then please try the following:

Snailmail:

Flake Productions
Markus Schmall
von Graevemeyerweg 25
30539 Hannover

Email:

flake@trsi.de

Voice:

+49/(0)177/2829402

(between 19.00 and 20.00 o'clock)

1.4 - Special comments and greetings -

Special thanks have to go to:

Vesselin Bontchev	for a couple of tips concerning the heuristic and the way it's done. Good luck at Frisk's place.
Sönke Freitag	for tips concerning the code-emulation and for all his AV work
Martin Berndt	for the keyfile protection and a lot of tips/hints
Olaf Barthel	for his help at operating system questions

1.5 Installation of the heuristik scanner module

How to install the heuristik module ?

In the now spread VirusWorkshop versions (5.x), the heuristik scanner will be a part of the mainprogramm. To ensure a better update possibility only for this module, I will implent a alone standing binary block, which has to be copied in the actual programmdirectory or in the "VW:" assign.

As said, this is just future.

1.6 What is it for a new option/module ?

This is just an additional tool for freaky users. It offers you the possibility to search for dangerous structures and stuff like that. It can cause a lot of FALSE positives, but it's (as said) a tool for the more advanced users.

1.7 What does heuristic exactly mean ?

Heuristic is a word, which is nowadays on the PC very popular and every better viruskiller offers you this possibility. Due to my contacts to some PC antivirus people and to the Virus Test Center in Hamburg, I came to the conclusion to implent such a scanner on AMIGA. Heuristic scanners search for dangerous filestructures and commands and give the user a warning. Such filestructures can e.g. appear in a lot of software

e.g. all packers look for special hunkstructures (ProPack etc.)
a lot of non crypted antivirus software can contain such commands