

# **Heuristik**

Markus Schmall

<b>COLLABORATORS</b>
----------------------

	<i>TITLE :</i> Heuristik		
<i>ACTION</i>	<i>NAME</i>	<i>DATE</i>	<i>SIGNATURE</i>
WRITTEN BY	Markus Schmall	July 20, 2024	

<b>REVISION HISTORY</b>
-------------------------

NUMBER	DATE	DESCRIPTION	NAME

# Contents

<b>1</b>	<b>Heuristik</b>	<b>1</b>
1.1	Heuristik Module for VirusWorkshop - Af Markus `Flake/TRST` Schmall . . . . .	1
1.2	Dansk Dokumentation - Copyright © 1995 - Virus Help Team Denmark . . . . .	1
1.3	Programmøren - Hvem er jeg ? . . . . .	2
1.4	Kontakt adresse . . . . .	2
1.5	- Lidt kommentare og tak - . . . . .	2
1.6	Installation af Heuristik scanner module . . . . .	3
1.7	Hvad er dette for en ny mulighed/module ? . . . . .	3
1.8	Hvad er heuristic for noget ? . . . . .	3
1.9	Heuristik Scanner historie . . . . .	4



Lars P. Kristensen  
Safirvej 25  
3650 Ølstykke  
Denmark  
Tlf. +45 4217 5233

Eller

Jan Andersen  
Veronikavej 33.1.tv  
2610 Rødovre  
Denmark  
Tlf. +45 3141 6867

### 1.3 Programmøren - Hvem er jeg ?

Mit navn er Markus Schmall og har i de sidste 5 år programmeret på denne dejlige maskine ved navn AMIGA. Jeg startede med at programmere demo'er, men efter at mit system blev inficeret med en Lamer Exterminator Boot virus, startede jeg på at programmere min egen virus killer, bedre kendt som VirusWorkshop.

Lige nu studere jeg på universitetet i Hildesheim, der ligger meget tæt på Hannover i Tyskland.

### 1.4 Kontakt adresse

Hvis du ønsker at kontakte mig, så prøv en af disse muligheder:

Alm. post:

-----

Flake Productions  
Markus Schmall  
von Graevemeyerweg 25  
30539 Hannover

Email:

-----

M.Schmall@LDB.han.de  
M.Schmall@Adebar.han.de (for overførsel af større data pakker)  
MSCH0091@rz.uni-hildesheim.de

Telefon nummer:

-----

+49/(0)511/514944  
(mellem klokken 19.00 og 20.00 )

Support BBS:

-----

Nirvana BBS Hannover  
Tlf: +49/(0)511/9524227  
V.Everything USR Modem

### 1.5 - Lidt kommentare og tak -

En speciel tak må gå til disse personer:

Vesselin Bontchev: For at par tips omkring heuristic og måden det er lavet på. Held og lykke på Frisk's place.

Sönke Freitag : For tips omkring kode-amulation og for al hans AV arbejde.

Martin Berndt : For keyfile beskyttelse og en masse tips.

Olaf Barthel : For din hjælp med operativ system spørgsmål.

Melanie : For ???? (an masse spildt tid)

## 1.6 Installation af Heuristik scanner module

Hvordan installeres Heuristic Module?

I den nu frigivede VirusWorkshop version 5.7, vil heuristik scanner være en del af selve programmet. For at sikre en bedre opdaterings mulighed kun for dette modul, vil jeg inkludere en enkelt binary blok, som skal være kopieret ind til det aktuelle program dir, eller til dit VW: assign.

Som sagt, dette er kun fremtid.

## 1.7 Hvad er dette for en ny mulighed/module ?

Dette er et specielt program for øvede brugere. Den tilbyder at kunne finde farlige strukturer og andre ting i stil med det. Den kan komme med mange FALSKE meldinger, men det (som før sagt) et program til øvede brugere.

## 1.8 Hvad er heuristic for noget ?

Heuristik er et ord, der nu om dage er meget kendt indenfor PC, det er meget populært og alle gode viruskillere tilbyder denne mulighed. Fordi jeg har en masse kontakter indenfor PC Antivirus kredsen og til Virus Test Center i Hamburg, bestemte jeg mig for at inkludere denne scanner til Amiga'en. Heuristik scanner leder efter farlige filstrukturer og kommandoer og giver brugeren en advarsel. Sådanne filstrukturer kan godt forekomme på f.eks. meget forskelligt software.

F.eks. alle pakkeprogrammer leder efter en speciel hunkstruktur (F.eks. ProPak.)

F.eks. en masse ikke beskyttede antivirus software kan indeholde disse kommandoer.

## 1.9 Heuristik Scanner historie

Ingenting her.. (Nothing here ?????)