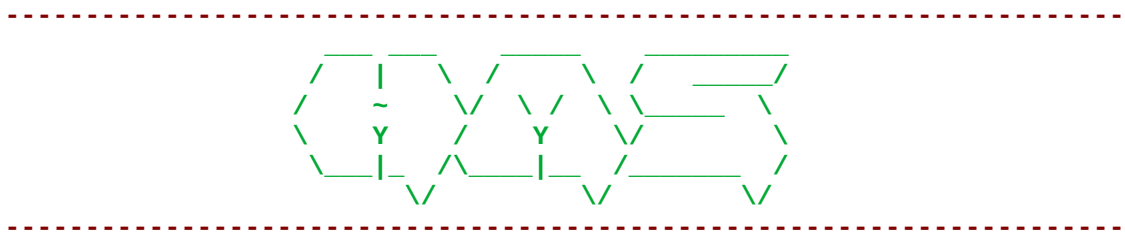
HMS - Heuristischer Memory Scanner für DOS - überprüft den PC auf DOS Viren
© by ROSE SWE, Dipl.-Ing. Ralph Roth



Virenscanner für das DOS Betriebssystem. Auch bedingt unter Windows einsetzbar (getestet mit Win95 bis Windows-**32bit** Version 10/11 und DosBox unter Linux).

Inhaltsverzeichnis

Funktion

HMS ist ein Programm zum Erkennen von bekannten und UNBEKANNTEN (neuen) Viren im DOS Arbeitsspeicher. Viele DOS Viren laden sich selbst in den Arbeitsspeicher und überwachen das Ausführen von Programmen durch DOS. Wird ein Programm ausgeführt, überprüft der Virus ob es schon infiziert ist oder infiziert es. Damit der Virus sich nicht laufend neu installiert, überprüft er, ob er schon 'speicherresident' ist. Diese Überprüfung führt HMS ebenfalls durch.

Normalerweise erhält HMS jedoch als Rückgabewert einen 'Fehler'. Falls kein Fehler zurückgegeben wird, könnte ein Virus diese Funktion belegen! Damit HMS keine Fehlalarme erzeugt, wurde HMS unter den verschiedensten Konfigurationen getestet und teilweise auch auf verschiedene Programme angepasst. So wurde HMS u. a. unter folgenden Betriebssystem/Konfigurationen getestet:

- Original MS-DOS 3.10, 3.21, 3.30, 3.31, 4.01, 5.00, 6.00, 6.20, 6.22
- PC-, Tulip- & Compac-DOS 3.31, 4.01, 5.00, 6.00
- DR-DOS 3.41, 5.00 & 6.00
- OS/2 1.x, 2.0, 2.1 (Achtung: Läuft nicht mit OS/2 Warp!)
- Windows 3.1x, Novell Netware, RTX-DOS, QEMM, IBM LAN Manager,
- 386 MAX, MS LAN Manager, SCROLLit 1.3,
- MS-DosShell, CEMM und verschiedenen residenten Antivirenprogrammen

- (VSAFE, TSAFE, SVS, DEFENDER, VDEFENDER, VIRSTOP u.a.)
- Novell DOS 7.0 - bis Patchlevel 13 (Englisch) und Patchlevel 15 (Dt)
- OpenDOS 7.01, 7.02, 7.03 (Caldera)
- Windows 95/95a-95c, 98SE, Windows NT 4.0 SP 1..SP 6a
- Win2K.RC3, Win2K SP1, SP2, WinME, Win-XP, Windows Vista, Windows 7
- FreeDOS Beta 8 und 1.00 mit FreeCOM (FAT16 und FAT32 Kernel)

Zusätzlich wurde HMS in Verbindung mit über 50 verschiedenen speicherresidenten Programmen ausführlich ausgetestet und teilweise angepasst!

Inkompatibilitäten

HMS funktioniert **nicht** mit folgenden Programmen bzw. Betriebssystemen:

- TSafe (die Uraltversion von 1990) - speichert nicht alle Register ab!
- XRAY - HMS erkennt ob XRAY (1.09) installiert wurde und bricht ab.
- RIO (Rock Input-Output)
- RelRes (aus CT'91 - 27.06.91) ist inkompatibel zu HMS, CHKPC & VSTOP.
- Novell DOS 7.0 (einige Funktionen werden deshalb nicht überprüft!)
- OS/2 alle Versionen!
- Spezielle, unsauber programmierte Festplattentreiber, z.B.: SCSI
- DosBox 0.72, 0.73, DosBox 0.74 = OK!
- DosBox 0.80, 0.81
- DosBox-X 0.85-3
- DosEMU 1.4
- vDOS 2020.03, vDOS Plus
- Windows 64bit (enthält keine DOS Emulation mehr)

Arbeitsspeicher scannen

Das Programm HMS überprüft den Arbeitsspeicher zusätzlich auf folgende bekannte Viren:

```
             ¦ Jerusalem Familie          >> 80 Varianten
             ¦ Vacsina + Yankee Doodle     - 48 Varianten
             ¦ Cascade Familie (1701/1704) - 14 Varianten
             ¦ Tequila                     -  3 Varianten
             ¦ Plastique (4.21/5.21/Cobol) - 11 Varianten
             ¦ Omicrone/Flip & Prism       -  6 Varianten
             ¦ Parity Boot, Tomalak etc.   -  3 Varianten
             ¦ EbbelWoi/King M.         mind. 3 Varianten
             ¦ Tremor (Tarnkappenvirus)    -  3 Varianten
             ¦ Natas (Tarnkappenvirus)  mind. 6 Varianten
             ¦ Hare Familie             mind. 3 Varianten
             ¦ Perfume (4711)              -  2 Varianten
             ¦ dBase, FSP Killer           je 1 Variante
             ¦ Neuroquila, Nighfall        je 2/3 Varianten
             ¦ MegaStealth                    1 Variante
             ¦ Spanska.4250                   1 Variante
             ¦ Implant                        3 Varianten
    und weitere...
```

Sollten Sie DR-DOS verwenden, bricht HMS nach dieser Prüfung ab (s. u.)!

Einsatz von HMS

Starten Sie Ihren Computer wie gewohnt. Führen Sie HMS aus. HMS sollte jetzt unter jeder überprüften Funktion ein "--- OK! ---" melden. Sollte dies nicht der Fall sein haben Sie wahrscheinlich ein Programm geladen, welches HMS antwortet. Sollte HMS jedoch beispielsweise folgendes melden:

```
          :
          :
       AX vor Aufruf FE01, AX nach Aufruf 01FE!
          :
          :
```

wäre (in diesem Fall) der Flip Virus aktiv. Lassen Sie sich jedoch nicht verunsichern, dieses Programm soll ja nur ein Werkzeug darstellen. Versuchen Sie in diesem Fall TSR's aus der AUTOEXEC.BAT und Devicetreiber aus der CONFIG.SYS zu deaktivieren. Bei MS-DOS 6.0 beim Booten die F5-Taste drücken und damit DOS 'nackt' booten. Meldet HMS nach der Deaktivierung keine Interruptüberschneidung mehr, liegt eine Inkompatibilität zu HMS vor! Bitte senden Sie mir das entsprechende Programm zu! Zum Überprüfen, welche Programme speicherresident geladen wurden, können Sie auch das Programm RESIDENT mit der Option '/a-' verwenden! Falls es Probleme mit irgendeinem Programm geben sollte, sollten Sie Ihrem Schreiben auf jedem Fall einen Ausdruck von ROSEDIAG beilegen. Einen Ausdruck erstellen Sie wie folgt:

```
                        rosediag > lpt1:
                             und
                          hms > lpt1:
                (anschließend eine Taste drücken)
```

Sollte HMS jedoch keine Interruptüberschneidung melden, können Sie HMS in die AUTOEXEC.BAT einbinden um einen größtmöglichen Schutz zu gewährleisten. Sollte sich nämlich jetzt ein Virus einnisten, könnte es zu eine Interruptüberschneidung führen, die eventuell beim Start von HMS angezeigt werden könnte!

HMS (und die anderen Antivirenprogramme) besitzen einen einzigartigen Selbstschutz, der teilweise aktive Tarnkappenviren erkennt und entsprechend den Virus deaktiviert! So erkennt HMS z. B. den Shiny-Virus und hält das Programm vorsichtshalber an!

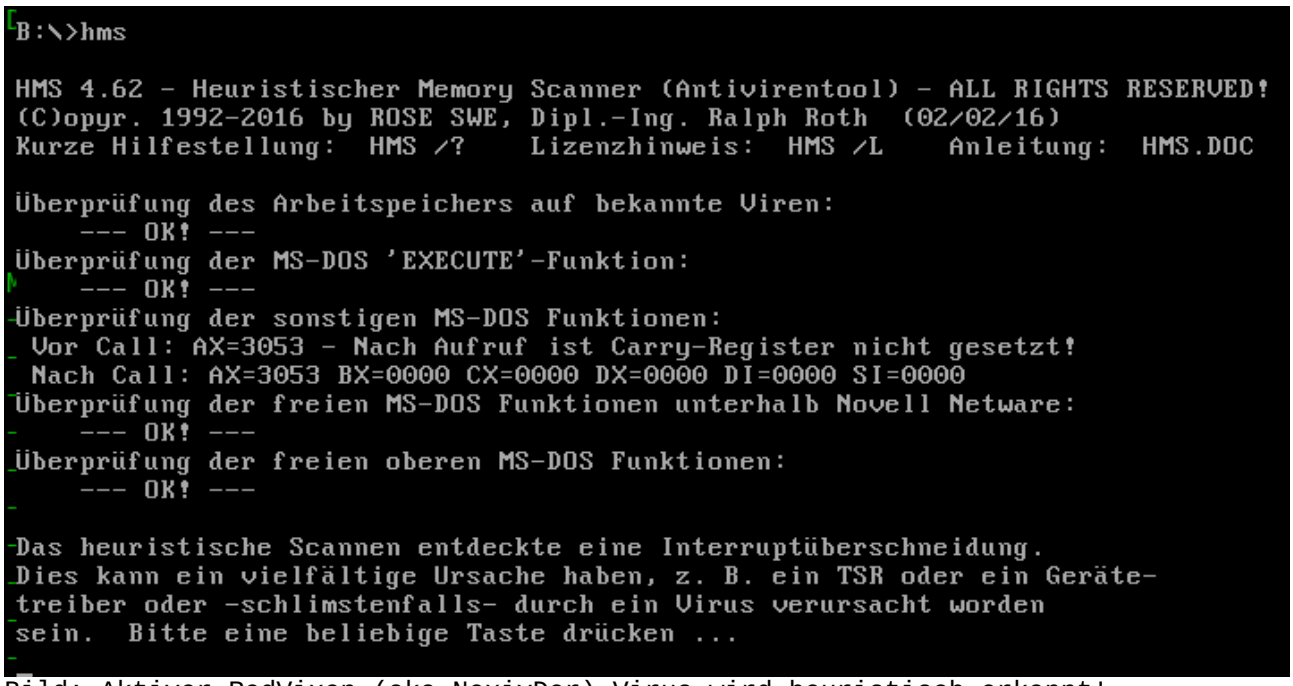


Bild: Aktiver RedVixen (aka NexivDer) Virus wird heuristisch erkannt!

Kommandozeilen Parameter

HMS kann mit verschiedenen Parameter an Ihre Bedürfnisse angepasst werden. Um eine Übersicht der aktuellen Parameter zu erhalten, starten Sie HMS mit dem Parameter '/?' (-> HMS /?).

Parameter /N+

Mit dem Parameter /N+ können Sie HMS anweisen, auch die Funktionen, die normalerweise Novell Netware bzw. andere Netzwerke belegen zu überprüfen. WARNUNG: Falls Sie diese Option in Verbindung mit einem Netzwerktreiber ausführen, kommt es zu einen Systemzusammenbruch Ihres Arbeitsrechners oder sogar des Netzwerkes! Aus diesem Grund muss diese Option explizit angeben werden. Falls von HMS ein Netzwerk gefunden wird, wird automatisch die Option /N+ gesperrt! Die Option /N+ ist nur für nicht vernetzte Rechner sinnvoll, oder bevor irgendein Netzwerktreiber geladen wird (z.B.: erstes Programm in der AUTOEXEC.BAT)!

Tipps für reine DOS Rechner

Wenn Sie einen größtmöglichen Schutz gegen eine Vireninfektion wünschen, binden Sie bitte wie folgt die Programme HMS, CHKPC und VSTOP in Ihre AUTOEXEC.BAT Datei ein (Reihenfolge beachten):

```
C:\VIRSCAN\TOOLS\QMS.EXE
C:\VIRSCAN\TOOLS\CHKPC.COM -p
C:\VIRSCAN\TOOLS\HMS.COM /n+
C:\VIRSCAN\TOOLS\VSTOP.COM -w
```

Falls Sie die Programme in ein anderes Verzeichnis installiert haben, müssen Sie die Pfade entsprechend anpassen. Fügen Sie die drei Zeilen gegen Ende der Datei ein, um einen größtmöglichen Schutz zu gewährleisten.

Hinweise

Eventuell nicht geeignet für vDOS, vDOS-Plus, DR-DOS, DOS-SCSI-Treiber und CD-ROM Treiber. HMS überprüft sich selbst auf Virenbefall oder Veränderungen und sollte deshalb in die AUTOEXEC.BAT (siehe oben) integriert werden! Durch einen integrierten Checksummentest kann das Programm nicht mehr geändert werden. HMS merkt hierdurch teilweise sogar eine Infektion durch Tarnkappenviren (Stealthviren)!

Lizenzvereinbarung

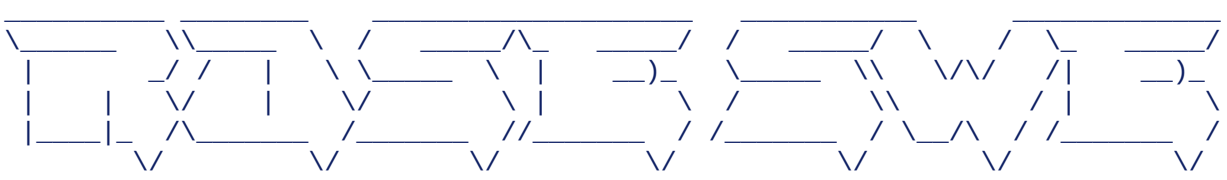
HMS ist BANNERWARE (darf **privat** umsonst benutzt werden)!
MODIFIZIEREN, VERÄNDERN, DIESE ANLEITUNG WEGLASSEN UNTERSAGT! JEDE KOMMERZIELLE WEITERGABE/NUTZUNG UNTERSAGT!
Weitere Nutzungslizenzbestimmungen: LIZENZ.DOC und FREEWARE.COM!
Jede kommerzielle Verwendung erfordert unser schriftliches Einverständnis (auch Bundling, Veröffentlichung in Zeitschriften u. ä.)!

Garantieausschlusserklärung

Das Programm HMS kann unter Umständen andere speicherresidente Software beeinflussen! Es wäre theoretisch möglich, dass es zu Seiteneffekten kommen könnte (solche Seiteneffekte wurden jedoch noch nicht festgestellt)!

Unter keinen Umständen ist der Programmautor Ralph Roth haftbar für jegliche Folgeschäden, einschließlich aller entgangenen Gewinne und Vermögensverluste, oder anderer mittelbarer und unmittelbarer Schäden, die durch den Gebrauch oder die Nichtverwendbarkeit dieser Software und ihrer begleitenden Dokumentationen entstehen. Dies gilt auch dann, wenn der Autor über die Möglichkeit solcher Schäden unterrichtet war oder ist!

(C)opyright by (ALL RIGHTS RESERVED!)



ROSE SWE
Dipl.-Ing. Ralph Roth
http://rose.rult.at
rose_swe@hotmail.com

See ROSEBBS.TXT for
full address, FAX and PGP keys.

/Ende/