

Caught in the act... DOS Viruses

The following screen shots shows you, how for example the programs QMS, VSP, BootVir and MemScan behave if a DOS or Multipartite (file and boot) virus is active.

ROSE AV EXE Shield

Small DOS programs like QMS are vaccinated with an Anti-Virus Shield (RecAV) to detect infection by standard DOS viruses.

```
B:\TOOLS>qms

----=[ ROSE SWE's EXE Integrity Checker: FAILED! ]-----
RecAV 4.83 (12/26/21)
! File has been MODIFIED or is INFECTED by malware!
! Please send us this file for further analysis (RalphRoth@gmx.de)!
! Visit: http://rose.rult.at
! Press a key to terminate the program!
```

Such infected programs are unusable and must be replaced by a clean copy. Please send us such files for further analysis!

ROSE AV COM Shield

Also DOS COM program from ROSE SWE are protected by an advanced self checking anti-virus shield (VSS) to detect infection by even advanced viruses.

```
B:\VIRUS>hms

USS, Viren Schutz Schild, (c) 1990-2003 by ROSE SWE, Ralph Roth

Datei: B:\VIRUS\HMS.COM

WARNUNG:
Das Programm wurde verändert und ist wahrscheinlich infiziert!
Wählen Sie eine der folgenden Möglichkeiten:

1 ... Selbstheilung (nicht bei komprimierten Dateien)
   und Programm abbrechen.
2 ... Selbstheilung, Programm ausführen.
3 ... Programm trotzdem ausführen!
4 ... Programm abbrechen.

Ihre Wahl (1-4): _
```

Such infected programs are normally unusable (you can try option 1.) or 2.) - *Selbstheilung*) and should be replaced by a clean copy. Please send us such files for further analysis!

Program: Quick Memory Scan (QMS)

QMS is a small program to detect active known and unknown DOS and Multipartite viruses.

```

--* QMS --* Quick Memory Scanner -- Version 12.47-1523 -- Fr 7. Okt. 2022 --
=====
(C)opyr. 1990-2022 by ROSE SWE, Dipl.-Ing. Ralph Roth - See ROSEBBS.TXT
Licensed to: Freeware, for non commercial use only!

--=[ Quick scan of the system and memory for viruses ]=--

Bootsector (512) ..... -- OK! --
MBR - HDD 0 (512) ..... -- OK! --
Interrupt 13h (DOS) ..... -- OK! --
Interrupt 13h (Orig) ..... -- OK! --
Interrupt 21h (DOS) ..... Cascade Virus
Interrupt 40h (DOS) ..... -- OK! --
Memory (Low-System) ..... -- OK! --
Memory (639 KB) ..... -- OK! --
Memory (HMA) ..... -- OK! --
HDD-IRQ 76h ..... -- OK! --
Path Companion Test ..... -- OK! --
Live Bait Test ..... Type: COM=1.701 Virus
Windows Trojans ..... -- OK! --

Please deactivate the virus through a cold boot from a system disc!
Press any key to continue...
```

Screenshot shows the standard Cascade.1701 virus active. As cascade only infects COM files, QMS.EXE remains uninfected. QMS detects Cascade on the hooked interrupt 21h as well as using the generic "Live Bait Test".

```

B:\>qms

--* QMS --* Quick Memory Scanner -- Version 12.47-1518 -- Fr 7. Okt. 2022 --
=====
(C)opyr. 1990-2022 by ROSE SWE, Dipl.-Ing. Ralph Roth - See ROSEBBS.TXT
Licensed to: Freeware, for non commercial use only!

--=[ Schnellüberprüfung des Systemes und Speichers auf Viren ]=--

Bootsector (512) ..... -- OK! --
MBR - HDD 0 (512) ..... -- OK! --
Interrupt 13h (DOS) ..... -- OK! --
Interrupt 13h (Orig) ..... -- OK! --
Interrupt 21h (DOS) ..... -- OK! --
Interrupt 40h (DOS) ..... -- OK! --
Memory (Low-System) ..... -- OK! --
Memory (636 KB) ..... Madjid Virus
Memory (HMA) ..... -- OK! --
HDD-IRQ 76h ..... -- OK! --
Path Companion Test ..... -- OK! --
Live Bait Test ..... -- OK! --
Windows Trojans ..... -- OK! --

Virus durch einen Kaltstart von einer virenfreien Systemdiskette deaktivieren!
Bitte eine beliebige Taste drücken...
```

Note here, that the Madjid virus had reduced the main memory by 4 KB from 640 KB. Madjid for example is a full stealth virus and can therefore bypass the RecAV Shield and the "Live Bait Test"

Program: MemScan

MemScan is a DOS program to detect active know and unknown DOS and Multipartite viruses. MemScan is additional protected against virus infection using advanced self checking technology and normally will refuse to run infected. Therefore we have started MemScan with the option /nocheckcrc for this screen shot

```
B:\>memscan /nocheckcrc
Virus Scanner, MemScan 17.8.6 - (c) 03.01.1991-2022 by ROSE SWE, Ralph Roth
MemScan: Heuristic virus scanner for memory resident boot and DOS file viruses

-----[ Quick scan of the system and memory for viruses ]-----

Bootsector (512) ..... -- OK! --
MBR - HDD 0 (512) ..... -- OK! --
Interrupt 13h (DOS) ..... -- OK! --
Interrupt 13h (Orig) ..... Majkl Virus
Interrupt 21h (DOS) ..... Majkl Virus
Interrupt 40h (DOS) ..... -- OK! --
Memory (Low-System) ..... -- OK! --
Memory (635 KB) ..... Majkl Virus
Memory (HMA) ..... -- OK! --
HDD-IRQ 76h ..... -- OK! --
Path Companion Test ..... -- OK! --
Live Bait Test ..... Type: COM=1.438/EXE=1.438 Virus
```

You can see here that the Majkl viruses is found on the hooked interrupts, as well as by the generic Live Bait Test revealing the virus has the size of approximately 1438 bytes and will infect both COM and EXE files.

```
B:\>memscan
Virus Scanner, MemScan 17.8.6 - (c) 03.01.1991-2022 by ROSE SWE, Ralph Roth
MemScan: Heuristic virus scanner for memory resident boot and DOS file viruses

-----[ Quick scan of the system and memory for viruses ]-----

Bootsector (512) ..... -- OK! --
MBR - HDD 0 (512) ..... -- OK! --
Interrupt 13h (DOS) ..... -- OK! --
Interrupt 13h (Orig) ..... Madjid Virus
Interrupt 21h (DOS) ..... Madjid Virus
Interrupt 40h (DOS) ..... -- OK! --
Memory (Low-System) ..... -- OK! --
Memory (636 KB) ..... Madjid Virus
Memory (HMA) ..... -- OK! --
HDD-IRQ 76h ..... -- OK! --
Path Companion Test ..... -- OK! --
Live Bait Test ..... -- OK! --
Windows Trojans ..... -- OK! --

Please deactivate the virus through a cold boot from a system disc!
Press any key to continue...
```

The Madjid virus is a full stealth virus and can bypass MemScan's self protection and Live Bait features, but not the Quick Memory Test.



Also MemScan finds the Madjid virus in the main screen. Please note that in this case MemScan must be started with the option "/NoMem" to bypass the Quick Memory and Live Bait tests, see picture above.

Program: VirScan Plus (VSP)

```
VirScan Plus 21.555 - (c) 20.10.1990-2022 by ROSE SWE, Ralph Roth
VirScan Plus - Virensuchprogramm gegen bekannte & unbekannte Computerviren
Tipp: Besuchen Sie unsere Home Page im Internet: http://rose.rult.at/
Seriennummer: VSP-#165.958 | Okt. 2022 | [Einzelplatzlizenz]
=[ Schnellüberprüfung des Systemes und Speichers auf Viren ]=

Bootsector (512) ..... -- OK! --
MBR - HDD 0 (512) ..... -- OK! --
Interrupt 13h (DOS) ..... -- OK! --
Interrupt 13h (Orig) ..... -- OK! --
Interrupt 21h (DOS) ..... -- OK! --
Interrupt 40h (DOS) ..... -- OK! --
Memory (Low-System) ..... -- OK! --
Memory (639 KB) ..... Clisti Virus
Memory (HMA) ..... -- OK! --
HDD-IRQ 76h ..... -- OK! --
Path Companion Test ..... -- OK! --
Live Bait Test ..... Type: COM=1.025 Virus
Windows Trojans ..... -- OK! --

Virus durch einen Kaltstart von einer virenfreien Systemdiskette deaktivieren!
Bitte eine beliebige Taste drücken..._
```

VirScan Plus uses the same Quick Memory Engine like QMS and MemScan and the above written explanations also apply. Starting with VirScan Plus Version 21.56 the Quick Memory Test can be bypassed with the command line options /NOMEM or /NOQMS

Program BootVir (German)

```
C:\LIVE>bootvir
BootVir: Überprüfen des Arbeitsspeicher auf bekannte DOS/Boot-Viren...

=[ Schnellüberprüfung des Systemes und Speichers auf Viren ]=

Bootsector (512) ..... -- OK! --
MBR - HDD 0 (512) ..... -- OK! --
Interrupt 13h (DOS) ..... -- OK! --
Interrupt 13h (Orig) ..... Junkie Virus
Interrupt 21h (DOS) ..... Junkie Virus
Interrupt 40h (DOS) ..... -- OK! --
Memory (Low-System) ..... -- OK! --
Memory (631 KB) ..... Junkie Virus
Memory (HMA) ..... -- OK! --
HDD-IRQ 76h ..... -- OK! --
Path Companion Test ..... -- OK! --
Live Bait Test ..... Type: COM=1.550 Virus
Windows Trojans ..... -- OK! --

Virus durch einen Kaltstart von einer virenfreien Systemdiskette deaktivieren!
Bitte eine beliebige Taste drücken..._
```

BootVir detects in this example the 1550 bytes variant of the Junkie virus. To continue the program you must start it with the option /NOMEM

New, unknown Bootvirus



BootVir had found a yet unknown MBR virus, that had changed the MBR.