

1 QUICK REFERENCE FOR VIRSCAN PLUS (VSP)

(C) 1989-2003 by ROSE SWE
http://come.to/rose_swe

1.1 Quick Reference

This is a short "**Quick Reference**" for English users that wish to evaluate the **VirScan Plus (VSP)** package.

1.2 Contents

| | | |
|----------|---|----------|
| 1 | 'QUICK REFERENCE' FOR VIRSCAN PLUS (VSP) | 1 |
| 1.1 | Quick Reference | 1 |
| 1.2 | Contents | 1 |
| 1.3 | Synopsis | 1 |
| 1.4 | Requirements | 2 |
| 1.5 | Command line Options | 2 |
| 1.6 | Short Description of the Options | 2 |
| 1.7 | Environment Variable | 3 |
| 1.8 | Examples | 4 |
| 2 | Cleaning of Viruses | 4 |
| 3 | Testing the Scanner? | 4 |
| 3.1 | Suggested Options for Testing | 5 |
| 3.1.1 | File viruses | 5 |
| 3.1.2 | Boot viruses (on disks) | 5 |
| 3.1.3 | Limits | 5 |
| 3.2 | Bugs? | 5 |
| 4 | Difference between the shareware- and the registered version | 5 |
| 5 | Integrated virus self checking | 6 |
| 6 | Questions? | 6 |
| 7 | License | 6 |

1.3 Synopsis

VirScan Plus is both a very fast signature scanner and a so-called heuristic scanner. Beside its blazing speed it has many configuration options. It can detect mutants of viruses; it can by-pass stealth type viruses as well as it will scan for Trojans, jokes, scripts viruses (VBS, HTML etc.), IRC worms, mal-

ware and dropper programs. VirScan Plus is able to disassemble and decrypt files using many advanced approaches and a software emulator. This makes VirScan Plus possible to detect suspicious instruction sequences and to detect yet unknown viruses!

1.4 Requirements

An Intel AT (80486 CPU or better), 540 KB of free memory and DOS 4.0+ is enough!

1.5 Command line Options

```
VIRSCAN
DRIVE:\ [DRIVE:\]] [DIRECTORY] [/?] [/ALL] [/AUTO] [/BOOT]
[/BATCH] [/CDROM] [/COLLECT] [/CONT] [/DEL] [/Directory]
[/EXTR] [/Ffile.ext] [/HEUR] [/HILFE] [/IVT] [/JN]
[/KILL] [/LAPTOP] [/LESEN] [/LOG[=]] [/MEMHI] [/MORE]
[/MULTI] [/MEHR] [/MEM] [/MUTANT] [/NOMEM] [/NOPART]
[/NOSIG] [/NOSCRIP] [/NOTROJ] [/PRT] [/PROZ]
[/Q] [/REG] [/REP]
[/SHOWLOG] [/SICHER] [/SPEICHER] [/TURBOAUS] [/ULTRA]
[/UNB] [/VL] [/WIN] [/ZEIT] [Search Mask]
```

Customers familiar with the American or UNIX parameter syntax (minus sign) instead of the slash (' / ') can also use the minus sign (' - ') to start an option.. Example: -lvt is equivalent to /lvt

Note: There must be at least one blank between the individual arguments! The arguments are not case sensitive. Options can be set using the environment variable VIRSCAN (set VIRSCAN=...). To unset an option set by setting VIRSCAN=... you can use the "-" at the end of the option (for example: set VIRSCAN=/auto -> VirScan a: -auto-).

1.6 Short Description of the Options

| Option | Short Description |
|----------|---|
| ----- | ----- |
| /? | Shows a short German help. |
| /ALL | Scan recursively ALL files (*.*). This option must be used with caution, it will trigger false positives! |
| /ANALYZE | Tries to determine the type of virus (COM/EXE/TSR) |
| /AUTO | Autopilot. Scans all drives, except disc drives and CD-ROMs. |
| /BATCH | Batch mode, do not wait for a key press. |
| /BOOT | Scan files for boot viruses too. (Droppers) |
| /CDROM | The autopilot feature shall scan CD-ROM's too! |
| /COLL | Creates a report format suitable to generate a virus collection (see also vspzoo.bat etc.). |
| /CONT | Continues scanning of specified drives. Ideal for permanent background scans under Win or OS/2 |
| /D. | Scan current directory. /D.. the parent dir. |

```

/Dxx          Scan directory xx.
/DEL          Delete infected files. Unrecoverable!
/EXTR         Generates a virus search string (only in
              registered version)
/H /HILFE     Load a quick reference in German language.
/HEUR         Use second level of the heuristic code analyzer.
              Only recommended for virus experts (only in
              registered version available)! Key files for
              AV people doing testing are available.
/KILL         Kill virus if possible (see VIRSCAN.TXT for a
              list of removable viruses).
/LAPTOP       Use B/W color.
/LESEN        Shows the file VIRSCAN.DOC.
/LOG          Log infected files to VIRSCAN.LOG
/LOG=path\file Save report into specified file. /LOG:file
              is also correct.
/MULTI /MORE /MEHR Scan multiple disc drives.
/MEM          Scan main memory (0-640 KB).
/MEMHI        Scan high memory too (640 - 1024 KB + A20).
/MUTANT        Relaxed scanning for mutated virus strains.
              Warning: Many false positive alarms will occur!
/NOMEM        Skip 'Quick Memory Scan' features.
/NOPART        Skip checking of Partition and MBR
/NOSCRIPT      Skip checking for script viruses and IRC/VBS worms.
/NOSIG         Do not use signatures. Use only AVR modules
              and the code analyzer.
/NOTROJ        Skip scanning for Trojans and droppers.
/PR /PRT /PRN Print report.
/PROZ         Show processor/co-processor type and CPU speed
/Q /QUIET      Quiet mode (no sound).
/REP /REPORT   Log EVERY scanned file to VIRSCAN.LOG
/ULTRA         Faster scanning (approx. 70% detection).
/SHOWLOG       Shows the file VIRSCAN.LOG.
/SHOWKEY       Shows the registration information of your
              key file ROSE.KEY.
/UNB          Scan for unknown generic viruses.
              Better use option /HEUR
/VL           Make a virus list.
/VTC          Special predefined switch for anti virus testing.
/WIN          If you have problems using VSP under windows...
/ZEIT         don't report suspicious time/date (62 sec, year
              2095, month: 15 or day: 0/32)

C:            Scan drive C:\ (recursively)
D:\XX         Scan directory D:\XX (recursively)
. (dot)        Scan all files in the CURRENT directory.
c:\dos\command.com scans a single file.

```

If some of the signature files (VIRSCAN.TRJ or VIRSCAN.VBS) are missing, then the options /NOTRJ and /NOSCRIPT are set by the program automatically!

1.7 Environment Variable

```

e.g.:         set VIRSCAN=/auto /MEMHI /IVT -unb
or:           SET VIRSCAN=/Option /Option /Option ...

```

1.8 Examples

Maximum security:

```
VirScan -auto -IVT -unb /boot
```

Scan multiple discs in drive A: and print the results:

```
VirScan a: /MEHR /PRN
```

2 Cleaning of Viruses

VirScan cleaning abilities are limited. VSP can remove most of the viruses found in Germany as well as almost all Boot/MBR viruses. If you have encountered a virus VSP can not remove please send me this virus for programming a cleaner. With the VSP package you will find in the TOOLS subdirectory the following generic cleaners:

- n RVK - ROSE VIRUS KILLER, generic cleaner for, even polymorph encrypted viruses infecting COM files.
- n MBR-Kill, generic cleaner and immunisier for boot viruses infecting your MBR.
- n BootKill, generic cleaner for boot viruses infecting your discs. For system discs use the program SYS supplied with DOS! Please read the .DOC files first, before using the cleaners! Special cleaners are available, request the file RVIRKILL

3 Testing the Scanner?

Testing a virus scanner is not an easy task and should be only done by experts on a large virus collection!

VirScan Plus doesn't scan for boot viruses in files nor does it use its boot virus heuristic on files. If you want to test VirScan Plus against boot viruses you must use the option /BOOT to scan boot viruses too. Use also the option /ALL if your boot virus images have no standard extension (.BIN, .IMG, .BOO). Please remember that this option slows down the scanning speed. If you want to test the boot virus heuristic then you have to scan infected discs! You can use then the option /HEUR to enable extra heuristic on boot sector viruses, which will catch all unencrypted boot viruses I have encountered!

Files with the extension .DOS, .IMG, .BIN and .BOO, as well as all scripts (e.g. .HTML or .VBS etc.) and IRC scripts (.INI etc) are scanned too. Use the option /HEUR to test the heuristic abilities on file and boot viruses.

3.1 Suggested Options for Testing

3.1.1 File viruses

```
VirScan <directory> /log=c:\tmp\vtc.log /batch /boot /all /q /zeit /nomem /unb /mutant
```

You can also use the option /VTC that sets all the major switches for a test environment (sets /BATCH, /BOOT, /ALL /Q, /ZEIT, /MUTANT & /NOMEM). If you want you can also add the option /heur to maximize the hitting rate!

```
VirScan <directory> /log=vtc.log /vtc
```

3.1.2 Boot viruses (on disks)

```
VirScan <drive:> /log=c:\tmp\vtc.log /q /nomem /unb /multi
```

or

```
VirScan <drive:> /log=vtc.log /vtc /multi
```

3.1.3 Limits

VirScan Plus is currently not able to scan inside archives (ARJ, ZIP and LHA etc.) as well as macros viruses!

3.2 Bugs?

This program can only handle filenames with at least 79 (67+12) char length (including paths) - this is a limitation of the DOS box! If you have longer filenames (Win 95/Win-NT supports 252 chars) you have to map your paths. Detection has been added for LAN-Manager, NetWare based networks and Microsoft compatible networks (e.g.: Gateway for Novell NetWare etc.) Under Novell NetWare this is an easy job, just take a look at MAP.EXE

VSP has problems with displaying the proper size of drives larger than 2 GB - this is a limitation from the old MS-DOS interrupts, that can only handle drives up to 2 GB (Int 21h, AH=36h - $2^{32} * 512$ bytes). Scanning is NOT affected from this MS-DOS limitation!

4 Difference between the shareware- and the registered version

The difference between the shareware version and the registered version of VSP is: VSP registered has the options /HEUR and /EXTR enabled. The registered version doesn't have the shareware beg screens!

When registering you will get the newest version on disk with additionally tools and documentations (approx 2 MB unpacked), as well as the newest version of VSP. Beside that you are entitled to support (FAX; Email, Voice) and obtaining new releases for the half price.

5 Integrated virus self checking

The program contains an integrated checksum tester to alert the user on a possible virus infection. The checksum for the program can be found in the file with the extension „.XXX“. The checksum in the file as well as the main program must not be changed nor modified in any case! Otherwise, the main program regards itself being possibly infected by a virus (a virus still unknown to the program)!

The following features of the EXE-file are monitored and checked for modifications every time the program is executed:

- n Checksum (CRC32) - If only one bit of the program is changed by a virus, the checksum will no longer match (own secure routine, according to ANSI X3.66 - CRC-Poly is: 0xDEBB20E3).
- n File size - If a program becomes one or two KB longer, it is infected!
- n Overlay size - If the program uses overlays („.OVR“).

I strongly recommend not making any changes to the EXE & XXX-file since the program will not run any more! The file with the extension „.XXX“ also contains the creation date and the standard MD5 checksum that can be checked with other tools like md5dir from ROSE SWE. Verifying the CRC32 checksum takes approx. 1 seconds (depending on computer type and hard disk drive). In to my opinion a passable effort! If the checksum is OK, the program is being executed. Otherwise a detailed error report with indications of possible error reasons will be displayed.

6 Questions?

Any suggestions, improvements, bugs or undetected viruses you found? Please write to the address found in the file ROSEBBS.TXT (contains full address, Email, PGP-key, FAX-number etc.) or visit our home page.

7 License

NOTICE TO USER:

You should read the following terms and conditions carefully before using this software. Your use of this software indicates your full acceptance of this license agreement and warranty. BY INSTALLING THIS SOFTWARE YOU ACCEPT ALL THE TERMS AND CONDITIONS OF THIS AGREEMENT.

The SOFTWARE is owned and copyrighted by ROSE SWE. Your license confers no title or ownership in the SOFTWARE and should not be construed as a sale of any right in the SOFTWARE.

No Warranty. The Software is being delivered to you AS IS and ROSE SWE makes no warranty as to its use or performance. ROSE SWE AND ITS SUPPLIERS DO NOT AND CANNOT WARRANT THE PERFORMANCE OR RESULTS YOU MAY OBTAIN BY USING THE SOFTWARE OR DOCUMENTATION. ROSE SWE AND ITS SUPPLIERS MAKE NO WARRANTIES, EXPRESS OR IMPLIED, AS TO NONINFRINGEMENT OF THIRD PARTY RIGHTS, MERCHANTABILITY, OR FITNESS FOR ANY PARTICULAR PURPOSE. IN NO EVENT WILL ROSE SWE OR ITS SUPPLIERS BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR SPECIAL DAMAGES, INCLUDING ANY LOST PROFITS OR LOST SAVINGS, EVEN IF AN ROSE SWE REPRESENTATIVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY THIRD PARTY.

In short: This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. If you do NOT agree simply do NOT install this software!

/* the end */