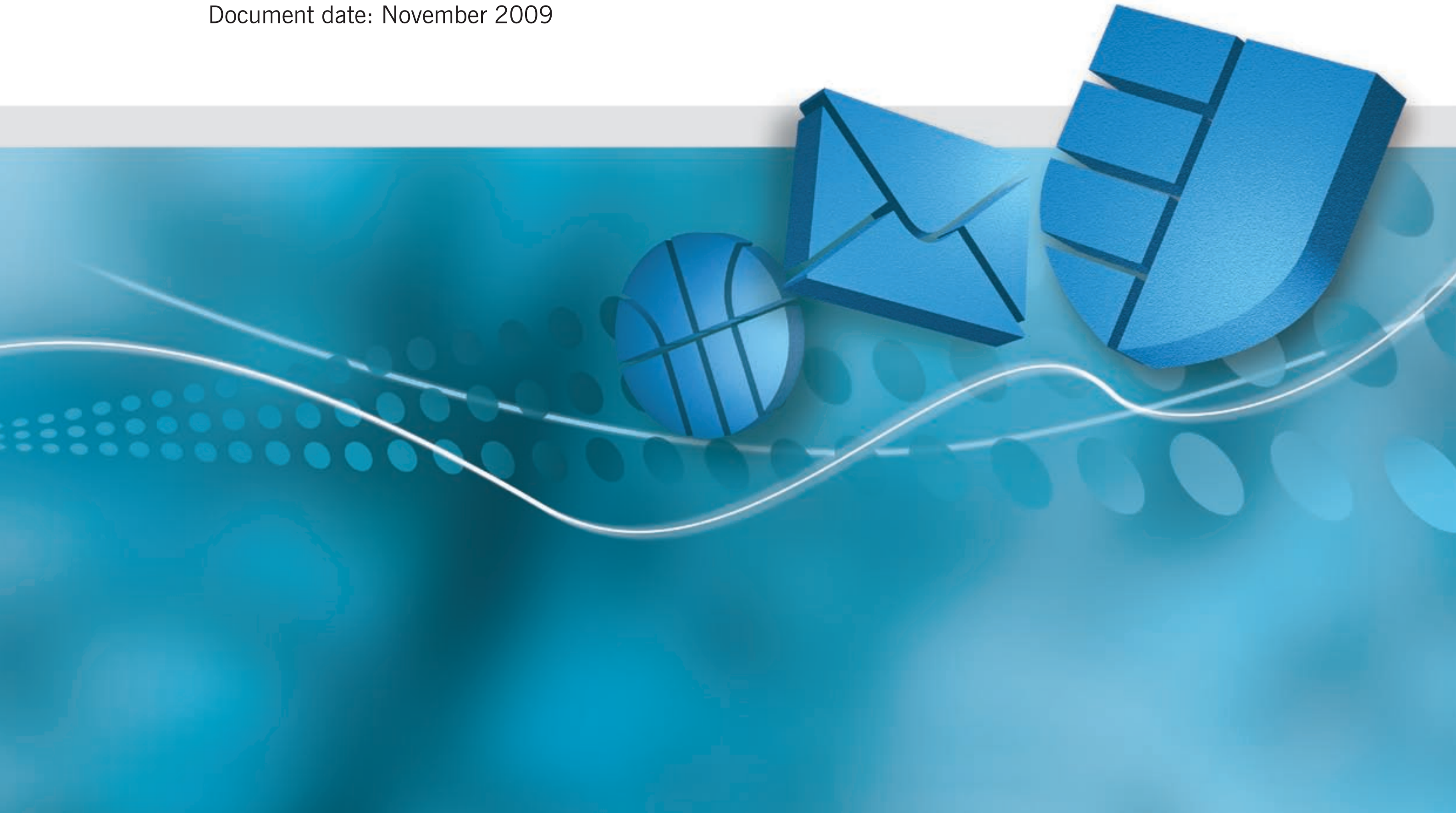
SOPHOS

Sophos Anti-Virus for OpenVMS

user manual

Document date: November 2009



About this manual

This user manual describes Sophos Anti-Virus for OpenVMS. It explains how to

- install Sophos Anti-Virus
- use Sophos Anti-Virus
- configure Sophos Anti-Virus
- disinfect files from viruses
- update Sophos Anti-Virus.

Sophos documentation is published at www.sophos.com/support/docs/.

Contents

Installation

Using and configuring Sophos Anti-Virus

Updates

Glossary and index

About Sophos Anti-Virus for OpenVMS

This section contains information about installing and updating Sophos Anti-Virus on OpenVMS.

If you have workstations connected to the OpenVMS server, contact Sophos technical support for advice on installing Sophos Anti-Virus on the network.

What is Sophos Anti-Virus?

Sophos Anti-Virus is software that can

- detect viruses
- report virus finds to specified locations
- disinfect viruses.

Sophos Anti-Virus can run on single computers or entire networks.

Why is it needed on OpenVMS systems?

At the time of writing, there are no known viruses that infect OpenVMS systems. However, it is useful for an OpenVMS system to scan files for viruses that infect other operating systems, for example, when an OpenVMS system is used

- as a file server for Windows workstations and Macintoshes (e.g. PATHWORKS/Advanced Server)
- to provide an ALL-IN-1 file cabinet
- for processing email with attachments (e.g. PMDF).

The Digital product PATHWORKS allows VAX and Alpha AXP computers to provide powerful network drive facilities for Windows workstations. This means an OpenVMS system can contain Windows executable files and documents that include macros, which can be infected by viruses.

How is Sophos Anti-Virus installed and updated?

You install Sophos Anti-Virus directly on an OpenVMS server or cluster from the Sophos Anti-Virus Supplementary CD (section 1).

Sophos Anti-Virus can only detect and disinfect viruses known to Sophos at the time it was released. This means you must update your software regularly to ensure it is capable of recognising the latest viruses. You should update it at the following times:

Every month (section 4.1)

Every month, Sophos releases a new version of Sophos Anti-Virus on CD and on the website. New versions contain new functionality, as well as the capability to detect the latest viruses. Update any computer on which you installed Sophos Anti-Virus as soon as you receive the Sophos Anti-Virus Supplementary CD.

When there is a new virus that poses a threat to your system (section 4.2)

When Sophos identifies a new virus, it issues a virus identity file (IDE), a type of file that enables Sophos Anti-Virus to detect that virus. Download IDEs from the Sophos website (www.sophos.com/downloads/ide/) and save them to the location specified in section 4.2.

To receive email alerts about new viruses, register at www.sophos.com/security/notifications/.

What if Sophos Anti-Virus finds a virus?

If a virus is found, find out its name and check its virus analysis on the Sophos website (www.sophos.com/security/analyses/viruses-and-spyware/). The analysis should provide disinfection advice. For help with disinfection, contact Sophos technical support.

See also section 3 for general information about disinfection.

Recommended precautions

The book ‘a to z of computer security threats’ describes many common types of virus and what you can do to avoid being infected by them. If you do not have a copy, a PDF version is available from the Sophos website (www.sophos.com/security/best-practice/).

You should also:

- Investigate potential loopholes such as unpatched servers, which may allow viruses into your organisation. Install all relevant software patches as soon as they become available.
- Advise your users not to run executables they receive as email attachments (or configure your gateway anti-virus software to remove this type of attachment).
- Encourage your users to send Microsoft Office documents in formats that cannot contain macros (and therefore cannot be infected with macro viruses), such as .RTF instead of .DOC, and .CSV instead of .XLS.
- Check your email and internet security settings.
- Always use passwords and never disclose them to anyone.
- Keep sound backups of your operating systems, programs and files. Even if you are able to disinfect programs, you must subsequently replace them from backups. Clean boot disks are also sometimes necessary to help with disinfection.
- Keep Sophos Anti-Virus up to date at all times.

Installation

Installing Sophos Anti-Virus on OpenVMS

1 Installing Sophos Anti-Virus on OpenVMS

To install Sophos Anti-Virus on OpenVMS, you must carry out the following steps, which are described in the following sections:

- Install VSWEEP on the OpenVMS server (section 1.1).
- Make LIBSAVI available for use (section 1.2).
- Make VSWEEP a DCL foreign command (section 1.3).

If you want to install Sophos Anti-Virus on workstations connected to an OpenVMS server, contact Sophos technical support for advice.

1.1 Install VSWEEP on the server

VSWEEP is supplied on the Sophos Anti-Virus Supplementary CD and on the Sophos website. The installation files comprise:

- VSWEEP.BCK (CD only)
  Save set of VSWEEP update files.
- VSWREST.CMD (CD only)
  Command procedure to restore the VSWEEP update files from the save set.
- READVMS.TXT (CD and website)
  Release notes.
- INSTVMS.TXT (CD and website)
  Installation notes.
- VSWEEP.ZIP (CD) or AVSW.ZIP (website)
  Zip file with the same contents as VSWEEP.BCK, provided as an alternative way of installing VSWEEP.

The save set and the Zip file each contain the following files:

virus engine shareable image files	LIBSAVI_AXP.EXE LIBSAVI_VAX.EXE LIBSAVI_I64.EXE
command-line interface image files	VSWEEP_AXP.EXE VSWEEP_VAX.EXE VSWEEP_I64.EXE
virus definition files	VDL.DAT *.VDB

Each image filename indicates the target platform as follows:

AXP	Alpha
VAX	VAX
I64	Itanium

The files VDL.DAT and *.VDB are usually kept in the same directory as VSWEEP_AXP.EXE, VSWEEP_VAX.EXE and VSWEEP_I64.EXE. To use a directory other than this directory, define the system executive-mode logical name VSWEEP_MAIN_VDATA_DIR to refer to this directory, for example

```
$ DEFINE/SYS/EXEC VSWEEP_MAIN_VDATA_DIR
MYDEV:[VSWEEP.VIRDATA]
```

If you specify an alternative directory in this way, ensure that the definition of the logical name is included in the site-specific startup procedure to ensure that the logical name is defined after a reboot.

There are three ways to install VSWEEP:

- using the save set on the CD and copying the files to the server from a Pathworks-connected workstation (section 1.1.1)
- using the save set on the CD and copying the files directly from the CD to the server (section 1.1.2)
- using the Zip file on the CD or the website (section 1.1.3).

1.1.1 Installing from a Pathworks-connected PC

At a Pathworks client, copy the contents of the /OpenVMS folder from the Sophos Anti-Virus Supplementary CD to the directory on the OpenVMS server where VSWEEP is to be installed.

Within VMS, run VSWREST.CMD, for example

```
$ @VSWREST.CMD
```

to extract the VSWEEP update files from VSWEEP.BCK.

If VSWREST is run ***with no parameters***, the save set VSWEEP.BCK must be in the current VMS default directory. The VSWEEP update files are then extracted to the current default directory.

If VSWREST.CMD is run with the -M parameter, the user is prompted for the directory to which the VSWEEP update files are to be extracted and for the location of VSWEEP.BCK.

The settings entered are saved in a configuration file, VSWREST.CFG. To use these values in future updates use the parameter -A.

You have installed VSWEEP. Now make LIBSAVI available for use (section 1.2).

1.1.2 Installing directly from the Sophos Anti-Virus Supplementary CD

To install directly from the Sophos Anti-Virus Supplementary CD, the VMS system must be capable of reading ISO 9660 format CDs.

Load the CD into the disk drive and mount the CD using the command:

```
$ MOUNT /MEDIA=CD /OVER=IDENT /UNDEFINED=(STREAM:132)
device_name
```

where `device_name` is the CD-ROM device name (e.g. DKA400:).

Ensure the current default directory is either the directory to which VSWEEP should be installed, or the directory containing VSWREST.CFG (if VSWREST is run with -A).

Run the installation command procedure VSWREST.CMD, for example

```
$ @DKA400:[OPENVMS]VSWREST.CMD
```

to install to the current directory.

or

```
$ @DKA400:[OPENVMS]VSWREST.CMD -M
```

to customise installation settings

or

```
$ @DKA400:[OPENVMS]VSWREST.CMD -A
```

to install customised settings.

Do not SET DEFAULT to the CD-ROM device before running VSWREST.CMD.

You have installed VSWEEP. Now make LIBSAVI available for use (section 1.2).

1.1.3 Installing using the Zip file

The Zip file is on the Sophos Anti-Virus Supplementary CD in the /OpenVMS folder as VSWEEP.ZIP, and on the Sophos website (www.sophos.com/support/updates/sophos-anti-virus-non-windows.html) as AVSW.ZIP.

It can be unzipped from the Sophos Anti-Virus Supplementary CD after the CD has been mounted on the OpenVMS system, or it can be unzipped after it has been copied from a PC via Pathworks/Advanced Server. Unzip it into the directory you want to use, replacing any files there. Sophos recommends that it is unzipped on an OpenVMS system. An OpenVMS unzip utility is available from Info-ZIP (www.info-zip.org).

You have installed VSWEEP. Now make LIBSAVI available for use (section 1.2).

1.2 Make LIBSAVI available for use

When the update files have been copied to the OpenVMS system, the LIBSAVI shareable image must be made available for use by the VSWEEP image. To do this, either

- copy the LIBSAVI image to SYS$COMMON:[SYSLIB] (section 1.2.1), or
- refer to the LIBSAVI image by logical name (section 1.2.2).

1.2.1 Copy LIBSAVI image to SYS$COMMON:[SYSLIB]

You must have SYSTEM privileges to use this method.

Copy LIBSAVI_AXP.EXE, LIBSAVI_VAX.EXE or LIBSAVI_I64.EXE (as appropriate) to the directory SYS$COMMON:[SYSLIB] (which is referenced by the logical name SYS$SHARE). If there is an earlier version of this file in the directory already, replace it. Ensure that the file protection for the file is set to (S:RWED, O:RWED, G:RWED, W:RE), and the owner is set to SYSTEM.

This step can be performed automatically if VSWREST.CMD is run with the qualifier -M to set the option, and -A for subsequent updates.

You have made LIBSAVI available for use. Now make VSWEEP a DCL foreign command (section 1.3).

1.2.2 Reference LIBSAVI image by logical name

Define a system logical name that refers to the device, directory and filename of the LIBSAVI image in the installation directory. This logical name must translate to the full specification of the LIBSAVI image. For example:

```
$ DEFINE/SYS LIBSAVI_AXP
MYDEV:[MYEXES.VSWEEP]LIBSAVI_AXP.EXE
```

or

```
$ DEFINE/SYS LIBSAVI_VAX
MYDEV:[MYEXES.VSWEEP]LIBSAVI_VAX.EXE
```

or

```
$ DEFINE/SYS LIBSAVI_I64
MYDEV:[MYEXES.VSWEEP]LIBSAVI_I64.EXE
```

If you use this method, ensure that the command above is included in the site-specific startup procedure to ensure that the logical name is defined after a reboot.

Alternatively, if VSWEEP is to be run only from within a command procedure, the logical name may be defined within that procedure, for example where the foreign symbol VSWEEP is defined.

If the logical name is not defined, or defined incorrectly, the following error message is generated:

```
%DCL-W-ACTIMAGE, error activating image LIBSAVI_AXP

-CLI-E-IMAGEFNF, image file not found
  AXP1$DKA0:[SYS0.SYSCOMMON.][SYSLIB]LIBSAVI_AXP.EXE;
```

You have made LIBSAVI available for use. Now make VSWEEP a DCL foreign command (section 1.3).

1.3 Make VSWEEP a DCL foreign command

If this has not yet been done, make VSWEEP a DCL foreign command using a statement such as

```
$ VSWEEP:==$D0:[MYEXES]VSWEEP_VAX.EXE
```

or

```
$ VSWEEP:==$D0:[MYEXES]VSWEEP_AXP.EXE
```

or

```
$ VSWEEP:==$D0:[MYEXES]VSWEEP_I64.EXE
```

where the device name (here D0) is preceded by a $.

This definition of VSWEEP should normally be placed in the LOGIN.COM file.

Take care to invoke the executable that is appropriate for the platform. An AXP executable run under VAX/VMS or OpenVMS VAX may lead to unspecified system behaviour. Other incorrect combinations normally result in a graceful OpenVMS error message.

Access rights for VSWEEP

VSWEEP requires read access to all files and directories in the area being scanned. No other access modes or privileges are required.

Installation is complete.

Using and configuring Sophos Anti-Virus

Using and configuring VSWEEP

Disinfection

2 Using and configuring VSWEEP

In this section 'VSWEEP' is a term used to describe the on-demand scanning functionality of Sophos Anti-Virus.

This section contains the following information:

- How to run VSWEEP from DCL (section 2.1).
- Information about running VSWEEP from a command procedure (section 2.2).
- How to check subdirectory levels (section 2.3).
- A list of VSWEEP command line qualifiers (section 2.4).
- A list of VSWEEP status return codes (section 2.5).

2.1 Running VSWEEP from DCL

Having made VSWEEP a command as described in section 1.3, run VSWEEP from the DCL prompt as

```
$ VSWEEP filespec[,...]
```

2.1.1 Specifying which files are scanned

The command parameter 'filespec' specifies to VSWEEP, in part or in full, the OpenVMS file or files to be searched for viruses.

A single command line can include more than one file specification, separated by commas. The filespec defaults to *.*;* with the result that

```
$ VSWEEP []
```

is the same as

```
$ VSWEEP []*.*;*
```

A typical invocation of VSWEEP will often specify more than one file to be scanned, e.g.

```
$ VSWEEP MYDEV:[PCSAV40...]*.EXE,*.DLL
```

Normal DCL defaulting rules apply, so that here the search of *.EXE and *.DLL would all be on MYDEV in the specified directories.

2.1.2 Scanning subdirectories

It is important to direct VSWEEP to examine the subdirectories as well as the main directory. In the above example, the ellipsis '...' at the end of the directory specification tells VSWEEP to search all subdirectories as well. Remember that:

- ***Under Pathworks File Services*** the DOS directory tree is emulated by an equivalent VMS directory tree, from the File Services directory downwards. See section 2.3.
- ***Under Pathworks Disk Services*** there may be many DOS files and directories within a single VMS container file. See the description of the /DS qualifier in section 2.4.

2.1.3 VSWEEP's File Service and Disk Service modes

When run from the DCL prompt or in a batch file, VSWEEP has two modes of operation:

In File Service mode (the default) VSWEEP treats VMS files as images of DOS files.

In Disk Service mode , which is selected by using the /DS qualifier, VSWEEP will automatically determine if a file is a Disk Service (FAT container file). If it is, VSWEEP will scan the files contained within each Disk Service file. If not, VSWEEP scans the file as in File Service Mode.

2.2 Running VSWEEP from a command procedure

There are extensive facilities under VMS for running sequences of DCL commands, either from a terminal or as a batch job. Because of VSWEEP's command line qualifiers, process return code and the return value in SWEEP$_STATUS, it can be successfuly integrated into such procedures.

The DCL command SUBMIT can be used to set a command procedure going as a background process. The process can be stopped using the DELETE/ENTRY command. The priority of the process can be controlled using the SUBMIT/PRIORITY command.

You can tailor the simple example procedures below to do much more, such as scanning several different areas within one job or handling the error conditions more comprehensively. Further information can be found in Digital's OpenVMS documentation, in the section entitled 'Guide to Using Command Procedures'.

Example 1: send mail on finding a virus

A typical requirement is for VSWEEP to run repeatedly in the background and raise the alarm if a problem is found. The following is a simple command procedure to achieve this, using SWEEP$_STATUS to test VSWEEP's results:

```
$ GOTO DO_IT

$ DO_IT_AGAIN:

$ WAIT 02:00

$ DO_IT:

$ VSWEEP filespec/FO/OUTPUT=VS.LIS

$ PURGE VS.LIS

$ IF SWEEP$_STATUS .NES. "SWEEP$_VIRUS" -

THEN GOTO DO_IT_AGAIN

$ MAIL/SUBJ="VSWEEP alert" VS.LIS SYSTEM

$ EXIT
```

where `filespec` should be replaced with the appropriate specification.

The batch job will go round and round the loop, creating a file called VS.LIS each time it runs VSWEEP, containing VSWEEP's output. If VSWEEP has reported a virus, it sends the output file as a mail message to SYSTEM and then stops. If VSWEEP reports informational messages or warnings, it simply waits two hours and then starts again.

However, if VSWEEP reports errors, this batch job aborts due to there being no appropriate handling of the VSWEEP process return code. You can avoid this by using a statement of the form ON ERROR THEN ..., instructing VSWEEP to take appropriate action on finding an error.

The mail message includes the virus alert string '>>>', which can cause problems for some users. The user can change the string by creating the logical name VSWEEP_ALERT_STRING with the new string as its value. For example

```
$ DEF/SYS/EXEC VSWEEP_ALERT_STRING ***
```

Example 2: delete infected files

The following DCL command procedure uses the /VF qualifier to write the names of the infected VMS files to SWEEP.VIR, so that it can then delete them, and tests the VSWEEP process return code:

```
$ VSWEEP filespec /VF

$ IF ($STATUS .AND. %X10) .EQ. 0 -THEN EXIT

$ OPEN/READ INFILE SWEEP.VIR

$ START_LOOP:

$ READ/END_OF_FILE=END_LOOP INFILE RECORD

$ DELETE/ERASE 'RECORD'

$ GOTO START_LOOP

$ END_LOOP:

$ CLOSE INFILE

$ EXIT
```

where `filespec` should be replaced with the appropriate specification.

2.3 Checking subdirectory levels

One general problem with Pathworks File Services when viewed from VMS is that of legal file specifications. A VMS file specification can only include eight explicit directory levels, including the root directory, for example

```
[000000.L1.L2.L3.L4.L5.L6.L7]MYFILE.EXT
```

A DOS file specification (as seen from a workstation) can however include a greater number of levels, for example

```
D:\L1\L2\L3\L4\L5\L6\L7\L8\L9\MYFILE.EXT
```

Since Pathworks File Services emulate the DOS directory structure using VMS files and directories, DOS files in directories at the ends of long chains may not be instantly reachable under VMS. This can have implications both for virus detection and for backup purposes.

To test whether any unreachable directories exist, begin by defining a suitable concealed logical name for the Pathworks File Services area, for example

```
$ DEFINE/TRANS=CONC TEMP $DISK1:[PCSAV40.]
```

and then see whether this has any unreachable directories, i.e.

```
$ DIR TEMP:[000000.*.*.*.*.*.*.*]*.DIR
```

If this returns ‘File not Found’ ($STATUS = ‘%X10018290’), or ‘No such Directory’ ($STATUS = ‘%X1001C04A’) then no unreachable directories exist. Otherwise, create one or more suitable concealed logical names for each of the problem areas in turn and repeat the process, for example.

```
$ DEF/TRAN=CONC TEMP1 TEMP:[L1.L2.L3.L4.]
```

```
$ DIR TEMP1:[000000.*.*.*.*.*.*.*]*.DIR
```

If a search for directories results in ‘File not Found’, that area can safely be scanned using

```
$ VSWEEP TEMP1:[000000...]
```

Note that the same considerations apply to the use of BACKUP, which may also miss certain files.

2.4 Command line qualifiers

There are two kinds of command line qualifiers:

- **Global qualifiers**, such as /OUTPUT and /VF, have the same effect wherever they appear in the command line. They affect the entire VSWEEP run.
- **Positional qualifiers**, such as /DS, apply only to the preceding file specification. All qualifiers are positional unless stated otherwise. If a positional qualifier appears before any of the file specifications, it applies to all of them as if it were a global qualifier. All VSWEEP's positional qualifiers can be negated by prefixing NO. For example, the negative of /DS is /NODS. This can be useful for countermanding an effect temporarily:

  ```
  $ VSWEEP /DS *.EXE/NODS, *.DSK, [.TEST]
  ```

  Here VSWEEP will search []*.DSK and [.TEST]*.DSK in Disk Service mode, but will search []*.EXE in File Service mode.

/AD Autodefault mode

This global qualifier will make VSWEEP run in autodefault mode. In this mode, provided primarily for compatibility with earlier versions of VSWEEP, any filename, extension or version in the file specification will be ignored. VSWEEP will instead take the specified device and directory (which may include the ellipsis [...] to specify subdirectories), and search there for files with certain extensions.

Run VSWEEP with the qualifier /VV to see the current list of extensions VSWEEP searches for.

In Disk Service mode (see the /DS qualifier), VSWEEP will search for the above files and for files matching *.DSK.

If any of the archive scanning options are enabled, the corresponding file extensions will be added to the list. Run VSWEEP with the qualifier /VV to see the current list of archive types that VSWEEP can scan inside.

See also the /AL and /DA qualifiers.

/AL Scan files with any extension

The /AL qualifier is permitted only in autodefault mode (see the /AD qualifier). It directs VSWEEP to scan all OpenVMS files, regardless of their extension, instead of the usual subset (listed under the /AD qualifier).

In Disk Service mode (see the /DS qualifier), VSWEEP will search for the above files and files matching *.DSK.

Use of the /AL qualifier is normally unnecessary, but it can be useful if, following a virus attack, infected files have been renamed to prevent inadvertent execution.

/ARCH Scan inside archives

The /ARCH qualifier causes VSWEEP to scan inside archives. The archive types scanned include ARJ, CMZ, GZIP, RAR, TAR, UUE, ZIP. Zipmail files are also scanned when /ARCH is enabled.

When /ARCH is specified self-extracting files in ARJ, LZH, RAR and ZIP formats will be scanned. /ARCH will also enable scanning of MacBinary and Binhex files if /MACV is specified.

If /ARCH is not set, you can specify scanning of particular types of archive individually, using /ARJ, /CAB, /CMZ, /GZIP, /RAR, /TAR, /UUE or /ZIP.

Use /VV to display the full list of archive types.

If this qualifier is used in conjunction with /NS, the files within each archive will be listed.

/ARJ Scan inside ARJ archives

See also /ARCH.

/CAB Scan inside CAB archives

This option is off by default and is not enabled when /ARCH is enabled.

/CDR Scan CD boot image

To scan the boot image of a CD that is bootable on Intel platforms, specify the device name of the mounted CD drive containing the CD to be scanned using the /CDR qualifier. For example

```
VSWEEP /CDR DKA400:
```

scans the boot image (if any) of the CD in device DKA400. If VSWEEP finds a boot image, it scans the boot sector of that image for boot sector viruses, and scans all executables in the boot image for file viruses.

You must have PHYIO privilege to use this qualifier.

To list the files in the boot image as they are scanned, use the /NS qualifier.

On computers that support ISO9660 CDs, you can mount the CD drive as a file-structured device. Otherwise, you must mount it /FOREIGN. If the CD drive is mounted as a file-structured device, the scanning of the boot image can be included as part of the scanning of the files on the disk. For example

```
VSWEEP /CDR DKA400:[000000...]
```

scans the boot image as well as the visible files on the disk.

/CMZ Scan inside CMZ archives

See also /ARCH.

/DA Search all files in Disk Service

The /DA qualifier is applicable only to Disk Service mode (see the /DS qualifier), and then only in default mode. It directs VSWEEP to scan all DOS files within the virtual disk, rather than the usual subset (listed under the /AD qualifier). As with the /AL qualifier, this is not normally necessary.

/DI Disinfect files containing viruses

The /DI qualifier enables VSWEEP to disinfect files containing portable executable (PE) and macro viruses automatically. The disinfection of executables may be disabled by specifying /NODIPE.

/DL List searched files in Disk Service

The /DL qualifier is applicable only in Disk Service mode (see the /DS qualifier). It lists all DOS files being scanned within the virtual disk. /DL does an implicit /NS (see below).

/DS[=(f1,f2...)] Disk Service mode

The /DS qualifier causes VSWEEP to scan inside Disk Service files, i.e. FAT container file images of entire DOS disks.

In Disk Service mode VSWEEP searches not only the files contained within the virtual disk, but also its boot sector. /DS can optionally be invoked with a list of DOS file specifications f1, f2, etc. enclosed in brackets. If f1 consists of just filename and extension, with no path, then the file or files will be scanned regardless of the directory in which they appear within the virtual disk. If f1 includes a path specification, only the files in the specified directory will be scanned. A path specification must start with a backslash (\). DOS drive letters may not be used. DOS wildcards (* and ?) may be used in the filename or extension, but not in the path. For example,

```
$ VSWEEP /DS=(MYFILE.*,\PROGS\*.EXE) *.DSK
```

would search for viruses in DOS files matching MYFILE.* (anywhere in the DOS directory structure) and \PROGS*.EXE, within each of the *.DSK container files in the OpenVMS default directory.

Using just /DS is the same as using /DS=(*.*), i.e. all files will be searched in all directories in the virtual disk.

/DXO95 Scan password-protected Office files

This option allows VSWEEP to scan inside most password-protected Office 95 Word and Excel files. This option is on by default.

/EEC Extended error codes

This option directs VSWEEP to use an alternative set of error codes. For details, see section 2.5.

/ELF Scan ELF files

The option is on by default.

/FF Include ‘FIX’ format files

The normal record format for OpenVMS files created by Pathworks File Services is ‘Stream’. In File Service mode VSWEEP by default treats files with any other record format as being unexpected. However, Pathworks does have an option allowing the files to be created in ‘Sequential’ format, with fixed-length records. In File Service mode the /FF qualifier can be used to include fixed-length record files in VSWEEP’s concept of ‘expected’ formats. The /FF qualifier thus interacts with both the /FI and /FO qualifiers.

The /FF qualifier is not applicable in Disk Service mode, as the only expected record format for virtual disks is currently fixed-length sequential.

/FI Ignore record format

This directs VSWEEP not to output informational messages when it encounters files with record formats not expected under Pathworks. Likewise, it prevents VSWEEP from returning INFO status as a result of encountering such files. /FI applies both in Disk Service and in File Service mode. It is useful when scanning directories containing mixed DOS and OpenVMS files. See also the /FF and /FO qualifiers.

When used in conjunction with the /RW qualifier, for example in order to scan mounted read/write Disk Services, /FI also suppresses messages resulting from apparent corruption or incompleteness.

/FO Standard format files only

This directs VSWEEP to avoid scanning files with record formats not expected under Pathworks.

In File Service mode /FO used without /FF therefore makes VSWEEP search only those files with the normal ‘Stream’ format and ‘Sequential’ organisation used by Pathworks File Services. Using /FO and /FF makes VSWEEP search sequential files with fixed-length records as well. Note that this will include normal VMS program files as well, if they are present in the directories being scanned. The /FO qualifier is useful when scanning directories containing mixed DOS and OpenVMS files. See also the /FF and /FI qualifiers.

In Disk Service mode the /FO qualifier directs VSWEEP to search only those files with fixed-length sequential record format.

/GZIP Scan GZIP archives

See also /ARCH.

/HTML Scan HTML files

This option is on by default.

/IDEDIR

This qualifier allows the default directory used for IDE files to be overridden to the specified directory, for example:

```
/IDEDIR=MYDEV:[MYIDES]
```

This qualifier takes precedence over the logical name VSWEEP_AUX_DIR which may also be used to specify an alternative IDE directory.

/IL Ignore locked files

If VSWEEP tries to open a file locked by another process and that file does not become unlocked within 10 seconds, VSWEEP normally returns a warning. The /IL qualifier can be used to direct VSWEEP to ignore any locked files it encounters. In this case no ‘locked file’ errors are signalled, and VSWEEP proceeds straight to the next file.

/MACENC Scan Macintosh encoded files

This option enables VSWEEP to scan two types of Macintosh encoded file, MacBinary format and Binhex format.

/MACV Detect Macintosh viruses

This option allows VSWEEP to detect Macintosh executable viruses stored in Pathworks for Macintosh file shares.

/MIME Scan MIME files

This option is off by default.

/NC Non-concealed device names

This directs VSWEEP to list OpenVMS files using their physical device names rather than any concealed or logical device name which might have been used in the command line. This can be useful if there is any confusion over the physical location of an infected file.

/NODIPE Do not disinfect PE files

Directs VSWEEP not to disinfect portable executable (PE) files. It is used in conjunction with /DI.

/NOSSA Scan files that VSWEEP incorrectly identifies as “zip bombs”

By default, VSWEEP stops scanning “zip bombs” when they are detected.

“Zip bombs” are malicious files that are designed to disrupt the action of anti-virus scanners. These files usually take the form of innocent looking archives that, when unpacked in order to be scanned, require enormous amounts of time, disk space, or memory.

When a “zip bomb” is detected, a message such as

```
WARNING: Aborted checking DEV:[TEMP]BOMB.ZIP;1 -
appears to be a zip bomb.
```

is displayed. Occasionally, VSWEEP incorrectly identifies files that have complex and/or multiple levels of archiving as “zip bombs”, and stops scanning them. To scan such files, rescan them using the qualifier /NOSSA. For example

```
$ VSWEEP MYDEV:[FILES]PACKAGE.ZIP /NOSSA
```

directs VSWEEP to scan PACKAGE.ZIP, even if it identifies it as a “zip bomb”.

! Use this qualifier only if absolutely necessary. If a genuine “zip bomb” is accessed with this qualifier, VSWEEP continues to scan it.

/NS Non-silent mode

The qualifier /NS directs VSWEEP to list all OpenVMS filenames as the files are scanned. Otherwise the names are suppressed. To list the contents of archives as well, use the /RNS qualifier instead. To list the names of DOS files within a virtual disk, use the /DL qualifier.

/OE Scan Outlook Express mailboxes

This qualifier enables VSWEEP to scan Outlook Express mailboxes when it does a scan. By default, it is ***not*** enabled to scan Outlook Express mailboxes. You must also use the /MIME qualifier with this qualifier.

/OUTPUT=filename Send output to file

By default, VSWEEP sends its output to SYS$OUTPUT. The /OUTPUT qualifier can be used to send the output to a different destination. /NOOUTPUT can be used to suppress all VSWEEP output except for totals of viruses found, and certain error messages. /OUTPUT and /NOOUTPUT are global qualifiers.

/QU Quick Scan

By default, VSWEEP scans in ‘full mode’, i.e. it searches files intelligently for viruses, and then makes a byte-by-byte search for virus fragments. The /QU qualifier can be used to select the ‘quick mode’. This increases VSWEEP’s speed by restricting it to searching for viruses (virus identities) only. This will still find all normal infections, but in the case of multiple infections of a single file it will report only the ‘outermost’ virus.

/RAR Scan inside RAR archives

See also /ARCH.

/REMOVEF Delete infected files

If this option is used, VSWEEP will delete infected files. Note that this option does not prompt for confirmation before deleting a file and should be used carefully.

/RNS Recursive non-silent mode

The qualifier /RNS directs VSWEEP to list all OpenVMS filenames as the files are scanned, including the contents of archives. Otherwise the names are suppressed. To omit listing the contents of archives, use the /NS qualifier instead.

/RTF Scan RTF files

This option is switched on by default.

/RW Read files already opened for writing

VSWEEP normally tries to search only files to which it can gain clean read-only access. This includes non-mounted virtual disks and those which have been mounted as read-only services, but excludes mounted read/write services. If the /RW qualifier is used, virtual disks which have been mounted as read/write services can be searched as well.

Note that a read/write mounted disk service may be in an incomplete state due to unflushed buffers or unfinished writing. Normally, VSWEEP will give up scanning a disk which it finds incomplete. The /RW qualifier causes VSWEEP to make a best attempt to read such a virtual disk.

Warnings resulting from problems encountered while searching mounted read/write services can be suppressed using the /FI qualifier.

Files which have been opened for exclusive use by another process will not normally be readable, even using /RW.

/SINCE=time Scan files revised since specified time

The /SINCE qualifier can be used to select files to be scanned based on each file’s revision date. The specified value may be VMS date/time string or the keywords YESTERDAY, TODAY, e.g.

```
$ VSWEEP */SINCE=28-AUG-1998:10:30:00
```

or

```
$ VSWEEP */SINCE=28-AUG-1998
```

(equivalent to 28-AUG-1998 00:00:00)

or

```
$ VSWEEP */SINCE=TODAY
```

If no time is specified, the default is TODAY.

It is also possible to use delta times, i.e. to specify scanning of all files modified within a particular period of time. Thus

```
$ VSWEEP */SINCE=-1-00
```

scans files with revision dates less than one day old.

/TAR Scan inside TAR archives

Controls the scanning of TAR archives. See also /ARCH.

/TNEF Scan TNEF files

This option enables VSWEEP to detect viruses in TNEF (Transport-Neutral Encapsulation Format) files. This file format is typically used for mail attachments and formatting information when sent from Microsoft Outlook using Rich Text Format.

This option is off by default and is mainly of benefit to users of VSWEEP in conjunction with PMDF to scan mail attachments.

This option cannot be used to disinfect viruses in TNEF files.

/UUE Scan UUEncoded archives

See also /ARCH.

/VARIABLE Scan OpenVMS variable-length text files

This qualifier enables VSWEEP to scan files that are in OpenVMS variable-length text format. This option is disabled by default. Note that if you use this qualifier, there is a scan-time overhead, and that ***disinfection*** is not supported for variable-length text files.

/VER Display information about virus data

This qualifier can be used to display information about loaded IDEs and the virus data used by VSWEEP. Unlike other options, /VER can be used on its own without running a scan.

/VF[=filename] Write filenames to file

When a virus is detected, it is useful to be able to take action on the infected files. This could include renaming them, deleting them, moving them, dismounting them or changing their protection. To help automate this, without restricting the choice of possible action, the global qualifier /VF=filename lets VSWEEP create a file containing just the names of the infected OpenVMS files, one name per line. A suitable DCL command procedure can then read the filenames one by one from this file, and take appropriate action.

If the qualifier is used just as /VF, without specifying a filename, the file will be called SWEEP.VIR, in the current OpenVMS default directory. If the /NC qualifier is used, any concealed or logical device names will be replaced with physical device names.

Details of the infected file's owner and the name of the virus can also be written to the SWEEP.VIR file. See the /VREPORT qualifier.

/VREPORT Write filenames, virus names, owner names to file

This qualifier allows VSWEEP to create a file containing not only the names of infected files (see the /VF qualifier above) but also details of the owners of infected files and the names of the viruses discovered.

The default name of the report file is SWEEP.VIR, but it can be specified using /VF .

/VREPORT takes one or more keywords, which specify what should appear in any line of SWEEP.VIR. When a virus is found, a new line will be added containing the information specified, in the same order as the keywords were given, formatted to the number of characters specified (or the default width for that keyword if no width is specified).

Keyword	**Meaning**
FILENAME	Full name of the VMS file in which the virus was found
DOSFILENAME	(if applicable) name of the DOS file within the FAT Container file
VIRUSNAME	Name of the virus reported by VSWEEP
UIC	Owner of FILENAME in format [123,456]
GROUPNAME	Groupname, if it exists
USERNAME	'Username' field from UAF record for UIC

OWNER	'Owner' field from UAF record for UIC
ACCOUNT	'Account' field from UAF record for UIC

The order and width of each field can be specified, and keywords can be abbreviated, e.g.

```
VSWEEP * /VREP=(OWNER=20,VIRUS,FILE=50)
```

```
VSWEEP * /VR=(FILE=50,VIRUS=20,OWNER=20)
```

```
VSWEEP * /VREPORT=(OWNER,VIRUS,FILE,ACC)/VF=VIR.TXT
```

/VV Display information and list of default extensions

Use this qualifier to display information about loaded IDEs and the virus data used by VSWEEP. It also lists the default extensions used in autodefault mode and the full list of archive types scanned.

/VV can be used on its own without running a scan.

/ZIP Scan inside ZIP archives

See also /ARCH.

2.5 VSWEEP status and return codes

VSWEEP's results can be tested either through its normal process return code, or through a DCL string symbol. These values can be tested by a DCL command procedure, which can take appropriate action such as broadcasting a warning, alerting the security manager or isolating the infected files.

2.5.1 Process return code

The process return code for VSWEEP takes the form %X18008yyz, where yyz are three hexadecimal digits:

yy

- 00 no viruses found
- 01 virus(es) found

z

- 0 completed with warning(s)
- 1 completed OK

- 2 error(s) encountered
- 3 completed with informational message(s)
- 4 did not complete

Extended error codes

If the qualifier /EEC is specified, the set of values for yy becomes (in order of increasing precedence):

hex	decimal	
00	0	No errors
0C	12	Compressed files found
08	8	Survivable errors (unspecifed) found
10	16	Password-protected files found. (They are not scanned.)
20	32	VSWEEP failed integrity check
24	36	Unsurvivable errors found
14	20	Virus(es) found and all disinfected
18	24	Virus(es) found and one or more not disinfected

The behaviour of z is unchanged.

Testing the process return code is the recommended method of ascertaining VSWEEP's results.

2.5.2 DCL string symbol

VSWEEP also creates a local DCL symbol called SWEEP$_STATUS, in which it returns one of the following string values (in order of increasing precedence):

SWEEP$_CLEAN	Search OK, no virus found
SWEEP$_INFO	Informational message(s) reported
SWEEP$_WARNING	Warning(s) reported
SWEEP$_ERROR	Error(s) reported
SWEEP$_VIRUS	Virus(es) found

3 Disinfection

This section gives advice on how to deal with a virus or virus fragment once it has been discovered.

3.1 Dealing with viruses

The method used to deal with a virus depends on where that virus is found, what type of virus it is, and how it affects the computer/s it infects.

You must find out the name of the virus and check its virus analysis at www.sophos.com/security/analyses/viruses-and-spyware/. Each virus analysis provides information about how the virus spreads and how to disinfect it. For more help with disinfection, contact Sophos technical support.

3.2 Eliminating viruses on the OpenVMS server

If VSWEEP reports a virus, first prevent further use of the infected item, and then disinfect or replace it. The /VF qualifier can be used to list the names of infected files, and these can then be automatically dismounted, moved, renamed or deleted by VSWEEP, if desired. See section 2.4.

The action taken against viruses on the file server depends on the type of item infected:

Files with macro viruses

Files infected with macro viruses can usually be disinfected by running VSWEEP from DCL using the command line qualifier /DI.

Infected executables

By default, VSWEEP will attempt to disinfect PE executables if the /DI qualifier is used.

However, it is impossible to ensure that executables are properly restored after disinfection. Restored files may be unstable, putting valuable data at risk. After disinfection use the DCL command DELETE/ERASE to delete the files, and restore them from the originals or from sound backups.

Infected disks

On OpenVMS servers, hard disks cannot currently be infected, and floppy disks are generally not used.

3.3 Dealing with virus fragments

If a virus fragment is reported, contact Sophos technical support for advice.

The report of a virus fragment indicates that part of a file matches part of a virus. There are three possible causes:

Variant of a known virus

Many new viruses are based on existing ones, so that code fragments typical of a known virus may appear in files infected with a new one. If a virus fragment is reported, it is possible that VSWEEP has detected a new virus, which could become active.

Corrupted virus

Many viruses contain bugs in their replication routines that cause them to infect target files incorrectly. An inactive portion of the virus (possibly a substantial part) may appear within the host file, and this is detected by VSWEEP. A corrupted virus cannot spread.

Database containing a virus

When running a full scan, VSWEEP may report that there is a virus fragment in a database file.

Updates

Updating Sophos Anti-Virus

4 Updating Sophos Anti-Virus

This section describes

- how to update Sophos Anti-Virus every month (section 4.1)
- how to update Sophos Anti-Virus between monthly updates when there is a significant new virus threat (section 4.2).

You must remember to update Sophos Anti-Virus on workstations. See the installation guide or update guide for the workstation platforms for instructions.

4.1 Updating Sophos Anti-Virus every month

Install the new executables from CD or from the Sophos website, as described in section 1.

Old versions of the Sophos Anti-Virus executables may be purged, to prevent them accumulating.

4.2 Updating Sophos Anti-Virus between monthly updates

Between monthly updates, it may be necessary to update Sophos Anti-Virus with new virus identity files (IDEs), in order to enable it to detect new viruses.

You should download new IDEs from www.sophos.com/downloads/ide/. Either download the IDE for the virus against which you want to be protected, or download all the latest IDEs in the IDE Zip.

Copy the IDEs into the directory containing the VSWEEP executable when VSWEEP loads. VSWEEP will load the new IDEs when restarted. To use a directory other than this directory, define the system logical name VSWEEP_AUX_DIR to refer to this directory, for example

```
$ DEFINE/SYS/EXEC VSWEEP_AUX_DIR MYDEV:[VSWEEP.IDES]
```

VSWEEP will then read IDEs from the specified directory.

Note that VSWEEP generates the following message if IDEs have been read:

```
INFO: Using additional viruses from n IDE files
```

where n is the number of IDEs found.

Appendix

Installing an InterCheck Server on a cluster

Appendix 1 Installing an InterCheck Server on a cluster

This appendix documents ways to run an InterCheck Server on a cluster.

The rule to observe when running Sophos Anti-Virus on a cluster is that only one CPU can run an InterCheck process serving any specific communications directory (designated by the logical name INTERCHECK_COMMS_DIR in that CPU's system logical name table).

The InterCheck Server can be run:

- On one CPU only. This is the recommended option.
- On more than one CPU.

Appendix 1.1 Running the InterCheck server on one CPU only

The preferred way to run VSWEEP as the InterCheck Server in a cluster is to run it on one CPU only. To maintain the InterCheck service in the event of one node going down, a background task may be run on one or more other nodes, which periodically checks whether it can take over as the InterCheck Server. The simplest logic for this is to look in the communications directory:

```
IF
  ((IC.STA doesn't exist) OR (IC.STA can be deleted))
THEN
  @IC_START.COM
ENDIF
```

Note that any executive-mode system logical names used to configure the InterCheck Server process (INTERCHECK_*) will need to exist in the system logical name table(s) of the failover CPU(s) as well as in that of the primary CPU, so that settings are maintained through the switch from one CPU to another.

Appendix 1.2 Running the InterCheck server on more than one CPU

An InterCheck Server can run on more than one of the CPUs. Note that this approach does not allow one node to take over from another, and is therefore not recommended.

1. Create a separate, non-conflicting INTERCHECK_COMMS_DIR logical name for each CPU.
2. Create a separate Pathworks File Service for each CPU to use, with the correct subdirectories [.COMMS] and [.LISTS]. The file services might for example be called 'INTRCHK1', 'INTRCHK2', 'INTRCHK3', etc.
3. Decide which of your PC clients are going to be served by which of these file services, and connect appropriately, for example using

```
[NET]USE Q:\\vmsclusteralias\INTRCHK2
```

Glossary and index

Glossary

ASCII

American Standard Code for Information Interchange; the standard system for representing letters and symbols. Each letter or symbol is assigned a unique number between 0 and 127.

Backup

A copy of computer data that is used to recreate data that has been lost, mislaid, corrupted or erased.

BAT

The extension given to the names of batch files in MS-DOS. A batch file contains a series of MS-DOS commands, which can be executed by using the name of the file as a command. AUTOEXEC.BAT is a special batch file which is executed whenever a computer is switched on, and can be used to configure the computer to a user’s requirements.

Booting

A process carried out when a computer is first switched on or reset, where the operating system software is loaded from disk.

Boot Protection

Method used to prevent bypassing security measures installed on a hard disk by booting a microcomputer from a floppy disk.

Boot Sector

The first part of the operating system to be read into memory when a computer is switched on (booted). The program stored in the boot sector is then executed, which loads the rest of the operating system from the system files on disk.

Boot Sector Virus

A type of computer virus which subverts the initial stages of the booting-up process. A boot sector virus attacks either the master boot sector or the DOS boot sector.

Checksum

A value calculated from item(s) of data which can be used by a recipient of the data to verify that the received data has not been altered.

COM

The extension given to a type of executable file in MS-DOS. A COM file is similar to an EXE file, but can only contain up to 64K of code and data. In operating systems other than DOS, the extension COM can have a different significance.

Companion Virus

A virus which ‘infects’ EXE files by creating a COM file with the same name which contains the virus code. It exploits the DOS property that if two programs with the same name exist, the operating system will execute a COM file in preference to an EXE file.

DOS

Disk Operating System.

DOS Boot Sector

The boot sector which loads the BIOS and DOS into PC RAM and starts their execution. Common point of attack by boot sector viruses.

EXE

The extension given to executable files in MS-DOS. These are similar to COM files, but can contain more than 64K of code and data.

FAT

File Allocation Table; a term used by the MS-DOS operating system (and others) to describe the part of a disk which contains information describing the physical location on the disk of the chains of clusters forming the files stored on that disk.

IDE

A type of file that contains the data Sophos Anti-Virus needs to enable it to detect a specific virus. IDEs are issued in between monthly updates to keep Sophos Anti-Virus up to date with the very latest viruses.

Link Virus

A virus which subverts directory entries to point to the virus code.

Macro Virus

A type of virus which uses macros in a data file to become active in memory and attach itself to other data files. Unlike other types of virus, macro viruses can attain a degree of platform independence.

Master Boot Sector

The first physical sector on the hard disk (sector 1, head 0, track 0) which is loaded and executed when the computer is booted. It contains the partition table as well as the code to load and execute the boot sector of the active partition. Common point of attack by boot sector viruses.

Memory-resident Virus

A virus which stays in memory after it has been executed and infects other objects when certain conditions are fulfilled. Non-memory-resident viruses are active only while an infected application is running.

Multipartite Virus

A virus which infects both boot sectors and executable files, thus exhibiting the characteristics of both boot sector viruses and parasitic viruses.

Parasitic Virus

A computer virus which attaches itself to another computer program, and is activated when that program is executed. A parasitic virus can attach itself to either the beginning or the end of a program, or it can overwrite part of the program.

Polymorphic Virus

Self-modifying encrypting virus.

Stealth Virus

A virus which hides its presence from the user and anti-virus programs, usually by trapping interrupt services.

Trojan Horse

A computer program which carries out hidden and harmful functions. Generally trojans trick the user into running them by claiming to have legitimate functionality. Backdoor trojans enable other users to take control of your computer over the internet.

TSR

Terminate and Stay Resident; a term used to describe an MS-DOS program which remains in memory after being executed. A TSR can be re-activated either by a specific sequence of keystrokes, or at some specific time, or by some specific signal from an I/O port.

UNC

Universal Naming Convention; a standard system for naming network drives, e.g. the UNC directory \\MAIN\USERS\ would refer to the USERS directory on the server called MAIN.

VDL

Virus Description Language; a proprietary Sophos language used to describe virus characteristics algorithmically.

Virus

A computer program that can spread across computers and networks by attaching itself to a program (such as a macro or boot sector) and making copies of itself.

Index

Technical support

For technical support, visit

www.sophos.com/support/

If you contact technical support, provide as much information as possible, including Sophos software version number(s), operating system(s) and patch level(s), and the exact text of any error messages.