About Sophos Plc.

SOPHOS

Sophos Plc was founded in 1980, moved into data security in 1985, and is now a world leader in the development of software for data security and computer virus detection. At the centre of this success is a reputation for innovative and sophisticated products backed by quality support. Sophos currently exports to 27 countries through a network of international distributors.

All Sophos products are designed, manufactured and supported at our base near Oxford in England. These products include:

- "SWEEP" virus detection utility.
- "D-FENCE" disk authorisation software.
- "VACCINE" checksumming virus detection system.
- "EDS" file encryption package for DOS and Windows.

For more information on Sophos products, please contact:

Sophos Plc.
21 The Quadrant
Abingdon Science Park
Abingdon
OX14 3YS
England

Tel	+44 1235 559933
Fax	+44 1235 559935
BBS	+44 1235 559936
Email	enquiries@sophos.com
FTP	ftp.sophos.com
WWW	http://www.sophos.com/

What is a computer virus?

A computer virus ‘infects’ programs and disks by attaching copies of itself to them:

- A boot-sector virus will infect the boot sector of disks.
- Parasitic, companion and link viruses infect files.
- Multi-partite viruses can infect both files and boot sectors.

A PC or disk is said to be infected if it contains an infected boot sector and/or one or more infected files. A PC’s memory is said to be infected if it contains some form of memory resident virus.

There are two ways in which a PC and a PC’s memory can become infected:

- The PC is bootstrapped from a disk infected with a boot-sector or multi-partite virus.
- An infected file is executed.

See Sophos’ *Data Security Reference Guide* for more information on viruses.

Viruses and Windows 95

Although almost all viruses are written for DOS, most still function under Windows 95. Windows 95 allows you to run DOS programs, and so a virus attached to a DOS program can also run. Even though the ability of many DOS based parasitic viruses to infect other programs, especially Windows 95 specific programs, is restricted, the side effects are still likely to function. In addition, most boot sector viruses are PC viruses, rather than DOS viruses, and as such will be able to infect PCs irrespective of the operating system they are running.

As information on writing Windows 95 programs becomes more readily available and its use more widespread, the number of viruses specific to it is sure to increase. By installing SWEEP for Windows 95 you are recognising the need to be prepared, as well as protecting yourself against the continuing threat from existing viruses.

How SWEEP can help

Computer viruses often include side-effects, which can range from the relatively harmless to the decidedly malicious. Viruses can spread widely before these side-effects are seen, so it is vital to detect and eliminate them as soon as possible. This is SWEEP’s main purpose.

SWEEP for Windows 95:

- Checks local hard disks, floppy disks and networks for the presence of all viruses known to Sophos at the time of SWEEP’s release.
- Looks for both virus patterns (small fixed parts of the virus which can be used to recognise it) and virus identities (a set of known characteristics of a virus) which allows reliable detection of polymorphic viruses.
- Is updated twelve times a year with the latest virus patterns and identities.
- Provides automatic updating for networked PCs.
- Offers two levels of security, allowing a ‘quick sweep’ which looks for virus identities in parts of executables likely to contain a virus, and a ‘full sweep’ which looks for virus patterns in every part of every executable.
- Features an ‘immediate mode’ which allows checking on demand, along with a ‘scheduled mode’ which allows multiple scheduled jobs to be configured for automatic operation.
- Can notify network managers automatically, via Microsoft Exchange, if a virus is found.
- Includes an extensive on-line virus information database.
- Is a 32-bit application and is fully Windows 95 compliant.

SWEEP is also available for DOS/Windows, Windows NT (i386 & Alpha AXP), Novell NetWare, OpenVMS (VAX & Alpha AXP) and OS/2.

Updating SWEEP

Updating SWEEP

Registered users of SWEEP are sent an updated SWEEP disk in the first week of every month. SWEEP for Windows 95's 'auto-upgrade' facility makes installing these upgrades simple.

Urgent SWEEP updates

Viruses are detected using Sophos' proprietary Virus Description Language (VDL). These descriptions are encoded as a string of ASCII characters, which facilitates their distribution by means such as fax or email.

Using SWEEP

Overview of the SWEEP display

The menu and toolbar

The icons in the toolbar provide short-cuts to commonly used menu options.

The immediate and scheduled mode tabbed pages.

The immediate mode page is displayed on start-up. This contains the file list along with the progress indicator for immediate operation.

The immediate mode file list shows the drives, paths and files that can be swept on demand. An ‘active’ light indicates currently selected entries. The selection status of an entry can be toggled by clicking the selection indicator to the left of its icon.

The progress bar indicates the state of an active sweep. The scheduled mode progess bar also shows the name and time of the next scheduled job.

On-screen log

After a job is started for the first time, the SWEEP display will expand to incorporate the on-screen log. This provides a record of activity in the current session, and reflects the information that is appended to the continuous log file.

Immediate mode

Starting an immediate sweep

To sweep all the selected drives, paths and files, select *Sweep* from the *File* menu or click the associated 'GO' icon.

Any individual item in the immediate mode display can be swept by double-clicking on its icon in the file list.

Default immediate mode file list

All local drives are displayed on the immediate mode page and all local hard drives are marked as selected.

Adding new items for immediate sweep

To add new items for immediate sweep, press *Add* on the immediate mode page. This will display the new item details dialog.

- path name
- file types
- subfolders

Removing items from immediate sweep

Highlight the name of the path to be removed and click *Remove*. An entry in the file list is highlighted by clicking on the path name.

Editing an item for immediate sweep

To edit an entry in the file list, highlight the name of the path to be edited and click *Edit*. This will display the item selection dialog, as described in the 'Adding new items for immediate sweep' section above.

Scheduled mode

To view or edit scheduled options, click on the ‘scheduled’ tab.

Default scheduled mode job list

By default, a job named ‘Default’ is created. This will sweep the system at 21.00 every day, unless it is deselected or removed from the job list.

Adding a new scheduled job

To add a new scheduled job, press *Add* on the scheduled mode page. You will be prompted for a job name, and will then be presented with the scheduled mode configuration page as described in Configuring SWEEP.

Removing a scheduled job

Highlight the name of the job to be removed on the scheduled mode page and click *Remove*.

Editing a scheduled job

Highlight the name of the job to be edited and click *Edit*. This will display the scheduled mode configuration page as described in Configuring SWEEP.

Configuring SWEEP

About configuring SWEEP

Select *Configuration* from the *Options* menu or click the associated icon to call up the configuration page for the mode whose tabbed page is currently displayed.

Immediate and scheduled modes are configured independently.

Sweeping mode

- sweeping level
- priority
- compressed files

Action on virus detection

- disinfect boot sectors
- infected files

Notification on virus detection

When SWEEP detects one or more viruses, it can send a notification message through Microsoft Exchange. If Microsoft Exchange is not installed, this option will not be available (see Mail profile).

- notify timing
- notification list

Reporting results

The report file contains information about individual immediate or scheduled jobs. It is generated in addition to the continuous log file.

- report mode
- report file

File list (scheduled mode only)

The scheduled mode file list is similar to the immediate mode file list, but specifies the files to be swept in a scheduled job.

Time (scheduled mode only)

SWEEP can be configured to run at particular times on specific days of the week, for example, once a day on weekdays and twice a day at weekends.

The virus library

Starting the virus library

Select *Virus Library* from the *View* menu or click the associated icon to start the on-line virus library.

Information on a particular virus

Information about the highlighted virus can be displayed by clicking *Info* or by double-clicking its name. This information includes advice on disinfection.

Searching for a particular virus

The virus library can be searched for viruses with certain characteristics. Click the *Find* button to enter search criteria.

- infected objects
- memory resident
- disinfectable by SWEEP
- trigger conditions
- text in description

After a search, *Find Prev* and *Find Next* will find the previous (or the next) entry in the database which matches the search criteria.

SWEEP options

Auto-start

Starting SWEEP for Windows 95 from a command line in the following way

```
    SWEEP -I
```

will force SWEEP to perform an immediate sweep as soon as it is loaded.

SWEEP can also be set to start as soon as Windows 95 starts, by placing a shortcut to it in the Windows 95 startup folder.

Sweep memory

SWEEP will check memory automatically for memory resident viruses when it is first started. Memory can also be swept at other times by clicking *Sweep Memory* from the *File* menu.

Log file

SWEEP maintains a continuous log of all of its activity. This log file contains administrative messages along with the messages described in On-screen log messages. The location of this log can be specified by the *Set Log Folder* option from the *File* menu.

Set log folder

By default the log file will be saved in the root folder of the first local hard drive, but this can be changed by clicking *Set Log Folder* from the *File* menu.

Executables

The list of file extensions to be treated as executables by SWEEP can be edited with this option. This list is only used if SWEEP is set to check ‘executable’ rather than ‘all’ file types.

Exclusion list

The exclusion list contains the specific files and subfolders to be excluded from all SWEEP operations. If you have set SWEEP to copy infected files to a particular folder, you might want to exclude that folder.

Restore defaults

This option will set all SWEEP settings back to their defaults, after requesting confirmation. This will destroy all scheduled jobs as well as resetting other options.

Clear log

The on-screen log provides a record of activity in the current session, and reflects the information that is appended to the continuous log file. This option clears the on-screen log, but does not affect the continuous log file on disk.

Mail profile

This option is only available if Microsoft Exchange is installed.

To send notification messages SWEEP must be able to log on to Microsoft Exchange without supplying a password. If your default profile requires a password to be entered, create a new profile with a preset password and use this option to select it.

Progress bar

In order to display the progress bar, SWEEP has to count all the items to be swept before starting the virus check. On large network drives this can take a significant length of time, which can be saved by disabling this option. This option will not affect any SWEEP jobs that are already running at the time the option is selected.

Treating viral infection

Establishing a clean environment for disinfection

A virus can be eliminated from the memory of an infected PC by switching the PC off and booting from an uninfected (and preferably write-protected) system disk. This is called performing a secure bootstrap or a clean boot, and is essential to providing a safe environment from which the disinfection process can begin.

Assuming the computer’s memory is free from viruses, it is safe to move or copy infected files.

Treating infected floppy disks

If a virus is discovered on a floppy disk that has just been received, then it is relatively easy to deal with.

Infected files can be automatically renamed, deleted, shredded, moved or copied if SWEEP has been configured to do so.

Floppy disks infected with boot sector viruses can normally be disinfected automatically by SWEEP. However, if SWEEP does not disinfect the boot sector, data can be safely copied off the disk and the disk reformatted. Formatting a floppy disk destroys all the data that is stored on it, including any viruses.

The source of the infected disk should then be established to locate any other infected disks.

Important! If just one infected floppy escapes disinfection other disks and PCs could be reinfected.

Note: It is advisable to preserve a clearly marked infected floppy for analysis and evidence.

Treating infected hard disks

If SWEEP discovers a virus on a hard disk, it is likely that the infection is widespread and considerably more work may be required to recover from the virus attack. The first step is to identify all infected PCs and disks.

The next step involves stopping the virus from spreading. Infected PCs should be disconnected from the network and all disk interchange between PCs suspended.

After the virus outbreak has been contained, the recovery process can begin. The virus has to be eliminated from all the infected floppy disks, as described above, as well as from infected hard disks.

If the hard disk only contains infected files, then these can be dealt with as described above.

However, if the boot sector of the hard disk is infected, then SWEEP for Windows 95 will not disinfect it. You should use the DOS version of SWEEP after a clean boot. See the DOS SWEEP user manual for more details, or contact Sophos' technical support.

After disinfection

There are a few other things worth bearing in mind after a virus attack:

- Uncover and close the loopholes which allowed the virus to enter the organisation.
- Inform any possible recipients of infected disks outside the organisation that they may be affected by the virus.
- In the UK, inform the *Computer Crime Unit* of *New Scotland Yard* in London about the attack (Tel 0171 230 1177, Fax 0171 230 1275).

Troubleshooting

SWEEP runs slowly

Full sweep

By default, SWEEP is set to perform a ‘quick sweep’ which checks only the parts of files which are likely to contain a virus. However, if ‘full sweep’ is set SWEEP will be much slower. The speed difference between ‘full sweep’ and ‘quick sweep’ depends on the configuration of your machine, but typically the ‘quick’ level is 5 to 10 times faster than the ‘full’.

Checking all files

By default, SWEEP will only check files defined as executables. If SWEEP is checking all files, it will take longer than if only executable files are being checked.

Network drives selected

Some network drives will be much larger than a local hard disk, and so will take significantly longer to check. Most network interfaces provide much slower access than a local hard disk, which can reduce the speed further still.

Progress bar selected

If the progress bar is selected, then SWEEP will have to count all the items that are to be swept. This can take several minutes on large network drives.

False positives

When SWEEP reports a virus pattern or identity match, it has almost certainly discovered a virus. However, there is a small chance that the contents of a virus-free program may be identified as a virus. This is due to the fact that polymorphic viruses (which change their appearance on every infection) are deliberately written to look like normal programs.

If you are ever in doubt, contact Sophos’ technical support for advice.

Options and actions which increase the chance of false positives are:

- sweeping all files
- sweeping memory

False negatives

A false negative is the opposite of a false positive, i.e. the event in which SWEEP fails to report a virus in an infected file.

Unknown viruses

Any virus-specific software will discover only those viruses which were known to the manufacturer at the time of software release. If you suspect you have discovered a virus unknown to SWEEP, please send Sophos a sample as soon as possible. There is a good chance that the virus is ‘in the wild’ and the sooner that it gets incorporated into SWEEP, the better.

You can also upload the infected sample onto our secure bulletin board (+44 1235 559936) or our ftp site (ftp.sophos.com). When the virus has been analysed (which may take from 10 minutes to a few days), we will fax or email you the IDE file which can be used to update SWEEP.

On-screen log messages

On-screen log messages

```
Virus:  'virus name' found in location
        No action taken

Virus:  'virus name' found in location
        File deleted

Virus:  'virus name' found in location
        File renamed to filename

Virus:  'virus name' found in location
        File shredded

Virus:  'virus name' found in location
        File moved to new location

Virus:  'virus name' found in location
        File copied to new location

Virus:  'virus name' found in location
        Error action

Virus:  'virus name' found in location
        Has been disinfected

Virus:  'virus name' found in location
        Error:  Disinfection failed

Error:  Could not open filename

Error:  Could not read filename

Error:  Sector size of drive drive is too large

Error:  Could not notify user

Error:  Could not initialize mail system

Error:  Could not login to mail system

Error:  Could not allocate memory for filename/directory
```

On-screen log pop-up messages

This is the ‘virus found’ message. Double-clicking on the ‘virus found’ message will display more information about that virus. The ‘virus found’ message will be followed by information about the action taken. This action will depend on the settings on the Action tab of the Configuration page.

The *location* will be one of either:

filename
Drive *drive name*: Sector *sector number*
Disk *disk* Cylinder *cylinder* Head *head* Sector *sector*
Memory
Memory block at address *8 digit hexadecimal address*

No action will be taken if SWEEP has been configured not to disinfect boot sectors, and not to rename, delete, shred, move or copy any infected files.

The file in which the virus was found has been deleted.

The *filename* will be the old name with the file extender changed to a number. For example, if a virus was named VIRUS.EXE it would be renamed to VIRUS.000, or VIRUS.001 if there was already a file called VIRUS.000.

The infected file has been deleted and cannot be recovered.

The *new location* is the location specified in the Action tab of the Configuration option.

The *new location* is the location specified in the Action tab of the Configuration option.

The file could not be deleted/renamed/shredded/moved/ copied. If the infected file was found on a floppy disk, check that the disk is not write protected.

The *action* will be one of either:

```
deleting file
renaming to filename
shredding file
moving to location
copying to location
```

Important! The infected file will remain unchanged and may be able to infect other disks and files.

SWEEP for Windows 95 can automatically disinfect, or remove, certain boot-sector viruses on floppy disks if the ‘disinfect boot sector’ option has been selected. SWEEP for DOS will be required to disinfect a hard disk boot sector.

SWEEP was unable to disinfect the boot-sector. See the ‘Treating viral infection’ chapter for advice on disinfecting a boot sector.

Important! The infected disk will remain unchanged and may be able to infect other disks and files.

The file called *filename* was on the list of files to be swept, but could not be opened for examination. Check that the file is not in use or already open.

The file called *filename* was on the list of files to be swept, but could not be read. This might indicate that the file or the disk is corrupt.

SWEEP will only currently sweep disk sectors of 2k or less. It is highly unlikely that it will ever encounter larger sectors.

The *user* was on the notification list but could not be notified. This could be because the *user* is no longer on the list of recognised Microsoft Exchange users, or because a profile requiring user entry of a password was used.

SWEEP checks to see if Microsoft Exchange is installed before allowing access to the notification options. However, there might be some situations in which SWEEP allows access even though Microsoft Mail is not setup correctly. For example, the MAPI mail interface might not be installed correctly.

If SWEEP cannot login to the mail system, then the profile name may be invalid.

SWEEP needs to allocate memory for the report if it is to send it to the users on the notification list. If the report is too big then SWEEP will not be able to load it into memory to send it. The report file can become very large if it is configured to list every file that it examines (see the ‘Report mode’ section of the ‘Configuration’ chapter).

Pop-ups

Specifies the drive, folder or filename to be swept. Both mapped and UNC path names can be entered. Wildcards can also be included. *Browse* can be used to select items.

Only those files defined as executables will be swept, unless the all file types option is selected.

Subfolders will be swept if this option is selected.

The ‘quick’ sweeping level only checks the parts of files likely to contain viruses, while the ‘full’ level examines the complete contents of each file. The ‘full’ level is more secure because it can discover viruses ‘buried’ underneath other code appended to a file, as well as minor virus mutations and corruptions. However, ‘full’ sweeping level is much slower, and for normal operation ‘quick’ sweeping is sufficient.

To minimise SWEEP’s impact on system performance it can be set to run at ‘low’ priority. This will increase the time taken to sweep the system.

SWEEP is capable of looking for viruses inside files compressed with PKLite, LZEXE and Diet.
There are currently no viruses that can infect the inside of a compressed file, but a file might have been infected before it was compressed. If a compressed file does contain an infected item, the virus can only be released if the file is decompressed and executed.

SWEEP can disinfect most boot sector viruses from floppy disks. Confirmation will be requested before a floppy disk is disinfected. Normally this option should only be used in immediate mode, because scheduled jobs will be suspended until confirmation is granted or refused by the user.

If an infected file is found, there are several actions that can be taken to make that file safe. Renaming or moving an executable file should prevent it from being run, but deleting or shredding the file will ensure that it cannot be accidentally executed. Shredding is a more secure type of file deletion that overwrites the contents of the file.

The notification message can be the full report file sent at the end of each job, and/or a brief message for every infected file found.

The notification list defines the users who will be notified. Clicking *Add* will connect to Microsoft Exchange, and the list of possible users will be displayed.

Setting list filenames will cause SWEEP to record in the report file the names of every item examined. Otherwise only infected items will be recorded.

The report file will be saved to disk.

Viruses can attach themselves to COM and EXE files; they can infect the master boot sector or the DOS boot sector; companion viruses place the virus code in a COM file with the same name as the EXE file; link viruses subvert directory entries to point to the virus code; and Windows viruses affect Windows executables. Trojan horses are not viruses, but are programs which provide unanticipated and undesired side effects when executed.

Memory resident viruses stay in memory after they are executed and infect other objects when certain conditions are fulfilled.

A tick in these boxes will include in the search viruses which can be removed from floppy and hard disks.

Many viruses require specific conditions, such as a certain time or date, in order to exhibit side-effects.

The ‘text description’ option will search for a string which appears in the information about that virus.