Virus Scanning Compressed Files and Disks

Dr. Jan Hruska, Sophos Plc, Oxford, England

Part # tr000037/950601

1. Introduction

An increasing amount of software is supplied in compressed form. Compression changes the contents of the files in such a way that virus scanners cannot diagnose an infection correctly. MS-DOS 6® is supplied with dynamic compression of complete disks *(Drivespace®)* which has caused concerns with regard to the ability to bootstrap a system from a clean floppy disk. This has also been the case with similar products such as *Stacker®* by *Stac Electronics* and *Superstor®* by *Addstor*.

2. File compression

Files can be compressed either **statically** (*PKZIP®*, *ARC®* etc) or **dynamically** (*PKLITE®*, *LZEXE®* etc).

Statically compressed files can be decompressed onto disk and scanned in the normal way before being executed.

Dynamically compressed files exist in a decompressed form only in memory; when a compressed file is run, the decompression routine is executed first, which loads the compressed file into memory while performing the decompression. A file can be infected either before of after being compressed.

If the infection happens **before** compression, it will not be picked up (Fig. 1). If the infection happens **after** compression, it will be picked up by a scanner in the normal way (Fig. 2). The former would happen if the program manufacturer compressed an already infected program (**which is not very likely**), while the latter could happen at any stage after the program has left the manufacturer (much more likely).

3. Checking compressed files using SWEEP

3.1 Checking statically compressed files

Statically compressed files should be decompressed on an isolated PC and scanned.

3.2 Checking dynamically compressed files

SWEEP can perform dynamic decompression of files compressed with a range of compression tools (-SC command line qualifier). It can also warn you if you are trying to check files compressed with a much wider variety of tools (-WC command line qualifier). It is recommended that both qualifiers are used with discretion, due to the resulting decrease in scanning speed.

Scanning inside the files

Use the -SC command line qualifier. For example:

```
SWEEP A: -SC
```

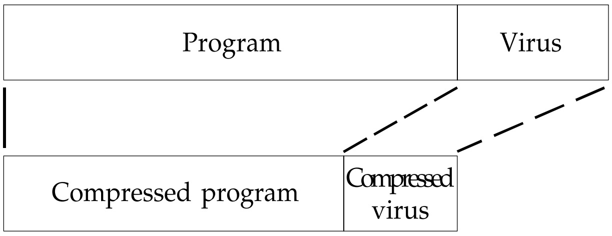


Fig. 1 - Program infected <u>before</u> dynamic compression: compressed virus not discovered

® All trademarks acknowledged

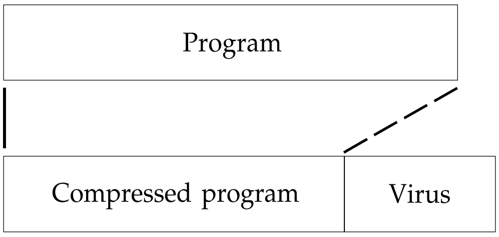


Fig. 2 - Program infected after dynamic compression: compressed virus discovered normally

SWEEP can dynamically decompress files compressed with *PKLite*, *LZEXE* and *Diet*.

Warning about compressed files

Use the -WC command line qualifier. For example:

```
SWEEP A: -WC
```

SWEEP will report files compressed with *ARC, ARJ, BOO, LZH, PAK, ZIP, ZOO, PKLite, ARJ self extract, LX 0.9X, LHarc, TopSpeed CRUNCH, PKARCK, BSA, LARC, LH, LZEXE, Diet* and *Cruncher,* but will not decompress them.

3.3. Dynamically compressed disks

Utilities such as *Drivespace* (delivered with MS-DOS 6), *Stacker* and *Superstor* allow transparent dynamic compression of whole drives. Compressed drives are not accessible if the bootstrapping is performed from a standard system floppy disk.

MS-DOS 6

To create a bootable floppy disk use the

```
FORMAT A: /S
```

while *Drivespace* compression is active. In addition to the two hidden system files (`IBMBIO.SYS` and `IBMSYS.SYS` or similar), the operating system automatically creates a third file `DBLSPACE.BIN` which contains the compression code.

After bootstrapping from such a system disk, the compressed drive can be accessed and Swept as normal.

Stacker

The creation of a bootable floppy for Stacker is somewhat more complex than for MS-DOS 6. Stacker uses a device driver which is loaded through `CONFIG.SYS`. Proceed as follows:

1. Format a bootable DOS system disk using the command

   ```
   FORMAT A: /S
   ```

2. Copy the file C:\STACKER\STACKER.COM to the floppy disk
3. Copy the file C:\STACKER\SSWAP.COM to the floppy disk
4. The file CONFIG.SYS on the hard disk should have the two lines which refer to STACKER and look like:

```
DEVICE=C:\STACKER\STACKER.COM C:\STACKVOL.DSK
DEVICE=C:\STACKER\SSWAP.COM C:\STACKVOL.DSK /SYNC
```

These lines should be copied into CONFIG.SYS on the floppy disk, but the references to C:\STACKER should be replaced with A:\. The above file would read:

```
DEVICE=A:\STACKER.COM C:\STACKVOL.DSK
DEVICE=A:\SSWAP.COM C:\STACKVOL.DSK /SYNC
```

It is important that no other parts of those lines are changed.

After bootstrapping from such a system disk, the compressed drive can be accessed and Swept as normal.

Superstor

1. Create a bootable floppy disk using the command

   ```
   FORMAT A: /S
   ```

2. The files SSTORDRV.SYS and DEVSWAP.COM should be copied to the floppy. The CONFIG.SYS file on the floppy should contain

```
DEVICE=A:\SSTORDRV.SYS
DEVICE=A:\DEVSWAP.COM
FILES=20
BUFFERS=20
```

After bootstrapping from such a system disk, the compressed drive can be accessed and Swept as normal.

4. Checking compressed files automatically using InterCheck and a server based SWEEP

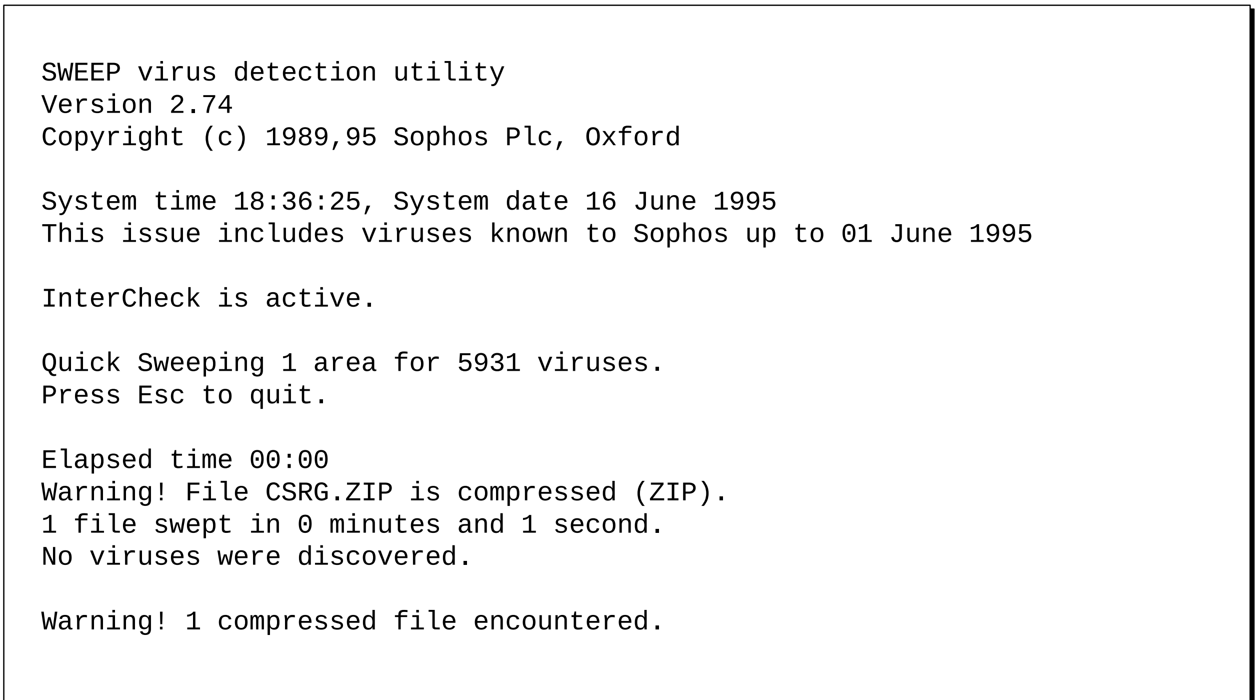
If you are using InterCheck on client workstations and a server-based SWEEP, both dynamically and statically compressed files can be checked automatically.

4.1 Checking statically compressed files

InterCheck will trap the closing of files as they are decompressed (with PKZip, ARC etc) and send them to the server automatically for checking.

4.2 Checking dynamically compressed files

If you wish to check dynamically compressed files both inside and outside, you must enable your server-based scanner to scan compressed files. These will then be checked automatically.



```
SWEEP virus detection utility
Version 2.74
Copyright (c) 1989,95 Sophos Plc, Oxford

System time 18:36:25, System date 16 June 1995
This issue includes viruses known to Sophos up to 01 June 1995

InterCheck is active.

Quick Sweeping 1 area for 5931 viruses.
Press Esc to quit.

Elapsed time 00:00
Warning! File CSRG.ZIP is compressed (ZIP).
1 file swept in 0 minutes and 1 second.
No viruses were discovered.

Warning! 1 compressed file encountered.
```

Fig. 3 - Sweep discovering compressed files if -WC command line qualifier is used