FAT32
New Problems for Anti-Virus, or Viruses?

Martin Overton

Email: Martin@arachnophiliac.com

Tel: +44 (0) 1403 241376

51 Cook Road,
Horsham, West Sussex,
RH12 5GJ, United Kingdom.

Abstract:

The sudden appearance of FAT32 in service pack 2 for Windows '95 has brought some new complications for both viruses and anti-virus software. What's worse is the update is only available to OEMs to ship on new PCs. It's been dubbed Windows '96-and-a-half, as it is just a short stop from Windows '97 (*now finally called Windows '98*).

What are the implications of Microsoft's latest addition to the file system format jungle?

Can the existing anti-virus software handle FAT32?

Can the existing boot and partition sector viruses infect FAT32 successfully, and without making the system unbootable or unusable?

Will file-infecting viruses be affected?

This paper aims to deflate the myths, clarify the differences and report the results of testing the above scenarios.

This paper was written for, and presented at the 1997 Virus Bulletin conference at San Francisco, USA on October 2nd-3rd 1997.

I would welcome any suggestions for improvement, comments on this paper and it's content.

This paper will be updated from time to time.

(Martin Overton 8th October 1997)

Introduction

Although this is intended as a technical paper, where possible full and detailed explanations will be given so that any laypersons that may be reading this (*hopefully*) won't be too confused. Anyone with a reasonably technical or support background will find the main content of this paper understandable and maybe a little too basic. The virus specific information and test results will be explained as clearly as possible within limited technical parameters of virus nomenclature and related jargon.

As I began to research this paper I was astonished by the lack of testing of Windows 95 with live viruses running under 95. There are plenty of papers and reviews testing Windows 95 scanners against a test set of viruses, but not when active in memory, only as dormant, inanimate images. Only two other papers were found that tested Windows 95 with viruses allowed to go resident and infect the system, and these used a very small set of viruses for testing.

Before jumping straight into the technical results, lets set the scene as you may not know about the service releases of Windows '95 and what these bring to the table. So here goes, a potted history...

What is 95B and OSR 2.x?

Whenever a new operating system is released, inevitably some user somewhere finds a problem, which needs to be fixed. Rather than release a complete new version of the operating system, software providers fix errors through *'service releases'* also known as *'service packs*'.

Service pack 1, released in January 1996 brought Windows 95 (*4.00.950*) up to version 95A (*4.00.950a*). Service pack 2 brings Windows 95 up to 95B (*4.00.1111*), released to OEMs in August '96, this is not being made generally available. It cannot (*legally*) be used to upgrade existing machines, it can however be purchased with a new Hard Drive or Motherboard. It is mostly only being pre-installed on new PCs, although some parts of OSR2 can be downloaded from Microsoft's web site for free. (*http://www.microsoft.com*)

Toshiba, Dell, Compaq and IBM are already pre-installing 95B on new PCs, many other manufacturers and resellers are planning to ship 95B on forthcoming models.

Windows 95 OSR2 is a service release (*service release 2*) of Windows 95. It includes all of Service Pack 1, and all of the later patches and fixes currently available on the Microsoft Web site, as well as Internet Explorer 3 and Personal Web Server. It also includes several components currently not available for download, including a new file system, FAT32. Other bugs, which were present in earlier releases of Windows 95, are fixed in OSR2. Though some users complain that other things were broken, c'est la vie!

What is FAT32?

Versions of Windows 95 older than OSR2 (*95 and 95A*), as well as many DOS versions, use a file system called FAT16[1] (*or FAT12 with DOS 3.30 or earlier versions*). The existence of large hard drives has led to large partition sizes, which mean large cluster sizes and wasted space.

To clarify this: Imagine a file that is 600 bytes (*characters*) in size. On a 1GB FAT16 partition this file would take up not 600 bytes but *16KB (16,384 characters, 1KB =1,024 Characters or 'Bytes'*), wasting over 15KB. On a 1GB FAT32 drive the same file would take up 4KB of space, wasting a lot less space. Below is a table that shows the cluster size used by different sized drives under FAT16 & FAT32.

[1] File Allocation Table: Holds information about which parts of a disk are used, unused, and can't be used either because they are reserved or faulty.

Partition Size (FAT16)	Cluster Size	Partition Size (FAT32)	Cluster Size
Up to 128Mb	2Kb	Less than 260MB	512 Bytes
Up to 256Mb	4Kb	260MB to 2GB	4Kb
Up to 512Mb	8Kb	8-16GB	8Kb
Up to 1Gb	16Kb	16-32GB	16Kb
Up to 2Gb	32Kb	Greater than 32Gb	32Kb

Although by default, FAT32 will be used on drives over 512MB, it can be forced, though this is not recommended by Microsoft, to work on drives of any size less than 512MB.

To do this you can use *FDISK* with the */FPRMT* switch to enable large disk support (*FAT32*) on drives smaller than 512MB. Not for non-expert users and don't expect Microsoft to bail you out it you experience problems. There is also a way to specify the cluster size when the drive is formatted, (*FORMAT /z:n*) *n* 512 bytes=cluster size*, e.g. *FORMAT C: /z:2* would format the C: drive with 1KB clusters. Be warned though, Microsoft will not support cluster sizes of less than 4KB.

FAT32 supports large drives and partitions (*up to 2TB (Terabytes)*) whereas FAT16 only supports up to 2GB (*Gigabytes*). Unfortunately FAT32 formatted drives cannot currently be read or written to by NT, DOS or OS/2 and therefore this is seen as a major headache by support staff. Some major PC manufacturers have taken the stance that installing FAT32 on their system would invalidate the warranty.

If you use FAT32 then you can no longer boot to the previous version of DOS as you could with 95A. You can use third-party boot managers, such as: OS/2 boot manager, NT boot manager, etc. As long as you don't use FAT32 you will still be able to read and write to the Windows 95B drive from other operating systems.

Other file system improvements include: FAT mirroring, backup of critical areas (*such as the DBR*), relocatable root directory and dynamic resizing of FAT32 partitions.

How Do I Tell If I've Got 95B (OSR2.x)?

Typing '*VER*' at a DOS prompt inside Windows 95 produces the following version number information:

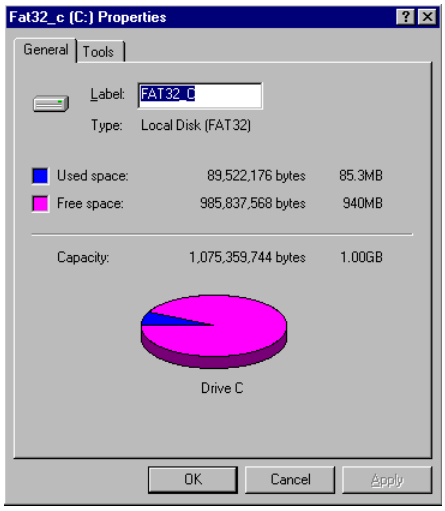
95 release version: `Windows 95. [Version 4.00.950]`
DOS Version: `MS-DOS 7.0`

95A (OSR1): `Windows 95. [Version 4.00.950]`
DOS Version: `MS-DOS 7.0`

95B (OSR2): `Windows 95. [Version 4.00.1111]`
DOS Version: `MS-DOS 7.1`

How Do I Tell If I'm Running FAT32 On My Drive(s)?

Simply double-click on the 'My Computer' icon on the desktop, and then right-click on the relevant drive icon and selecting 'Properties' will show the following dialogue box



The Type entry clearly shows that this local disk is FAT32, not FAT16 or FAT12.

If you use FDISK to create a partition of greater than 512MB and you enable large disk support, then the drive will be set to FAT32 by default.

Drives smaller than 512MB or disabling 'large disk support' will ensure that FAT16 is used instead.

Running FDISK on a drive larger than 512MB will display the following message if you have OSR2.x installed.

```
Your computer has a disk larger than 512 MB. This version of Windows
includes improved support for large disks, resulting in more efficient
use of disk space on large drives, and allowing disks over 2 GB to be
formatted as a single drive.

IMPORTANT: If you enable large disk support and create any new drives on this
disk, you will not be able to access the new drive(s) using other operating
systems, including some versions of Windows 95 and Windows NT, as well as
earlier versions of Windows and MS-DOS. In addition, disk utilites that
were not designed explicitly for the FAT32 file system will not be able
to work with this disk. If you need to access this disk with other operating
systems or older disk utilities, do not enable large drive support.

Do you wish to enable large disk support (Y/N).....? [N]
```

FDISK can also be used to check to see if your current drive(s) are formatted as FAT12, FAT16 or FAT32. Selecting option 4 from the menu when FDISK is run shows the following:

```
                     Display Partition Information

Current fixed disk drive: 1

Partition  Status   Type    Volume Label  Mbytes   System   Usage
 C: 1          A    PRI DOS   FAT32_C2      1028   FAT32      50%
    2              EXT DOS                 1020              50%


Total disk space is  2047 Mbytes (1 Mbyte = 1048576 bytes)


The Extended DOS Partition contains Logical DOS Drives.
Do you want to display the logical drive information (Y/N).....?[Y]




Press Esc to return to FDISK Options
```

Why all this fuss?

It seems that Microsoft have once again caused a large amount of confusion regarding it's new file system. We only have to look back at the confusion of the average user when HPFS[2] and NTFS[3] were released. Even now many users believe that viruses cannot infect under these file systems. As stated in the 1996 Virus Bulletin conference "*Although Windows NT was designed as a secure operating system, this security does not include viruses*"[Jones]. This shows that with NT and NTFS that many viruses work fine, others such as macro viruses are hardly inconvenienced unless they try to use API's or OS specific functions.

Regular lurkers in the Alt.Comp.Virus newsgroup will remember the flurry of posts and threads regarding a certain anti-virus program being criticised for not supporting FAT32. Many came to their defence, such as Vesselin Bontchev, Jimmy Kuo and the incumbent Virus Bulletin editor, Nick Fitzgerald (*though at the time he was the Comp.Virus & Virus-L moderator and FAQ maintainer*).

Later in this paper I will cover the 'myths' some of which were being offered as fact by well-intentioned participants of this newsgroup.

Myth #1?

Windows 95 is so different that viruses cannot infect it.

Of course in reality, very few people now believe this, though this appears to have been one of the common 'urban myths' about Windows 95 and it's near magical protection[Whalley]. The reason for the myth is understandable as Microsoft's own marketroids, insisted that Windows 95 was '*All New'*.

It is perfectly clear that although Windows 95 brings some new challenges to the virus writer, many DOS viruses (*including MBR and DBR viruses*) work adequately under Windows 95 and FAT32. In fact macro viruses are the group of viruses least troubled and inconvenienced by FAT32. Only those that use API's and other operating system specific calls are likely to fail.

Microsoft's claim that Windows 95 was '*All New'* was to say the least misleading. Bearing in mind that Microsoft tried extremely hard to support the vast majority of legacy Windows 3.x and DOS applications, and to be fair to a great extent they succeeded, but at what cost?

Windows 95 still runs on DOS, it's DOS 7.0, but it's still DOS with many of its legacy faults that the virus writers can use to their benefit and to your detriment.

Effects on Anti-Virus software?

Anti-virus product	DBR infector removal	MBR infector removal	Comments
Mcafee 3.0.3	Y	Y	FAT32 Support Ghost positive when trying to remove MBR infector!
Dr. Solomons 7.72	Y	Y	The Magic Bullet natively supports Fat32.
F-Prot 2.27	N	Y	Error reading DBR message on infected FAT32 DBR.
Thunderbyte 8.02	N	N	Access denied when accessing infected FAT32 DBR or MBR.
Symantec anti-virus (NAV 3.0)	Y	Y	Invalid media type reading drive C Abort, Retry, Fail. Only continues and remove DBR infector if FAIL selected. Ghost positive when trying to remove MBR infector! FAT32 Support.
AVP 3.0	N	Y	DBR detected but not removed.
Sophos Sweep 3.00	N	N	Bad Logical Sector C:|0 message when trying to remove DBR infector. Detected MBR infector but would not disinfect.
VET 9.44	Y	Y	Native FAT32 Support. No problems encountered.

[2] IBM and Microsoft with OS/2.
[3] Microsoft with Windows NT.

Effects of Boot Sector [DBR] viruses?

Putting the Boot in

Boot sector [DBR] viruses infect the computer when an infected floppy diskette is attempted to be booted from (*assuming that the CMOS boot sequence is the standard A: then C:. If it's set to C: then A: then standard DBR (and MBR) viruses (excluding droppers) don't stand a chance*[Overton]). The virus in the infected diskette boot sector will try to go resident and infect the DBR of the hard disk. If successful, and the virus can operate correctly on the host operating system then the virus will try to infect any diskette that is not write protected accessed in the floppy drives of the system.

FAT16 DBR Viruses vs. FAT32

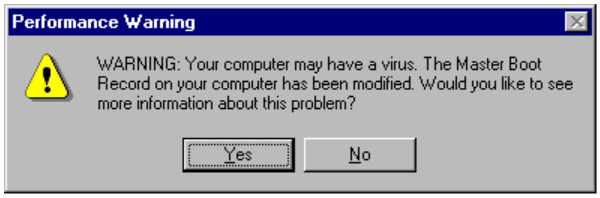
It is not surprising that this group of viruses has the most profound impact on FAT32 partitions, as the Dos Boot Record has been radically changed. "*The boot record on FAT32 drives is greater than 1 sector. In addition, there is a sector in the reserved area on FAT32 drives that contains values for the count of free clusters and the cluster number of the most recently allocated cluster*"[MS].

To date (July 97) no FAT32 specific DBR infectors exist. This is not to say that they won't be created, as virus writers seem to fight to be the first to infect new operating systems or to use new techniques. I predict that we will see a FAT32 specific or FAT16/FAT32 DBR infector before the end of this year, if not sooner. It is only a matter of time after that happens before the first multi-partile virus that can infect the FAT32 DBR will be released.

Infected DBR or MBR? Confused? You Will Be!

When Windows 95 is infected by a DBR or MBR infector[4], and is first booted, in most cases the following dialogue box is displayed.

Fig 1



Bear in mind that this is only displayed the *first* time after the original infection. This dialogue box is a step in the right direction for Microsoft, as it actually mentions the word '*Virus*'. This may encourage an infected user to actually use some anti-virus software to check their system for viruses, or maybe not.

The confusing part of this story is that if the DBR is infected this message is also displayed. I would have expected Microsoft to know the difference between a DBR and an MBR, obviously this is not the case!

Many users would simply ignore this message and carry on regardless.

If you select the Yes button on this dialogue box you will see the following detailed dialogue box.

As you can clearly see this informs you that your system is using the MS-DOS compatibility mode for both the File System and Virtual Memory.

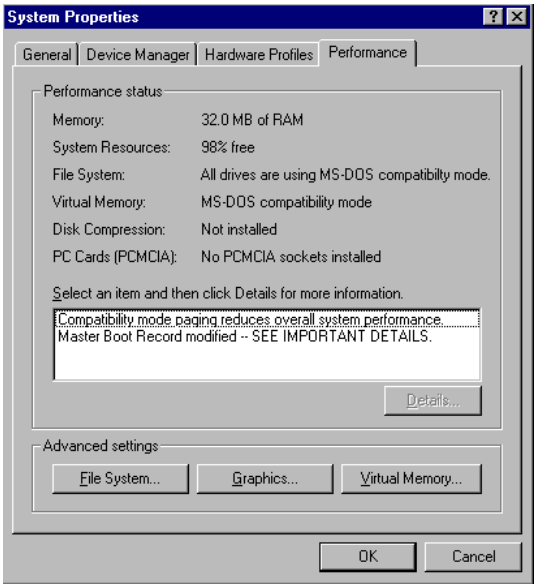


Fig 2

[4] Although this could be caused by a faulty driver or badly written security product.

It also offers the following information, which the user should be more than a little curious to read, especially as it states:

'Compatibility mode paging reduces overall system performance'

and

'Master Boot Record modified --SEE IMPORTANT DETAILS.'

On most systems that are properly configured and not infected by one of the many MBR or DBR viruses, the following dialogue box would be shown instead.

This dialogue box clearly shows that 32-bit access to Virtual Memory and the File System is being used.

It has been said many times that Microsoft looks toward functionality first, security has always been the poor relation and it seems that it is almost an after thought, some of you may feel that I am understating this point.

Microsoft has been of recently talking to many of the anti-virus industries largest players to form a working party on Macro virus issues with Microsoft products. I look forward to the outcome from this undertaking. Unfortunately (for the end user) I predict any expectations will fall short, and the anti-virus industry will be required to charge to the rescue again to thwart the virus foe.

Fig 3

Myth #2?

DBR viruses cannot be removed from FAT32 partitions by non-FAT32 compatible anti-virus software.

Currently there are no FAT32 specific viruses, not to say that they will not be created in the future. Non-FAT32 compatible scanners appear to be unable to successfully remove the current FAT16 DBR viruses.

My findings with the DBR infectors and scanners tested for this paper appear to validate this supposed myth!. Disconcertingly, my results with genuine infections appear to be the completely opposite to some postings by notable researchers on the Alt.Comp.Virus newsgroup[5].

Is the truth out there?

[5] See the newsgroup postings reprinted in the appendices of this paper.

Test Results

Swiss-Boot.A resisted all attempts to remove it by anti-virus software. It had to be manually removed using *SYS C:* after booting from a clean boot disk and locking the C: drive with the *LOCK C:* command.

FORM.A was also resistant to removal, only being successfully removed using Dr. Solomon's Magic bullet, McAfee 3.0.3 and Vet 9.44, which are all FAT32 aware.

Although some researchers insist that DBR infectors can be removed from FAT32 drives by FAT16 compatible scanners, my tests seem to indicate the opposite. This obviously needs more investigation.

Virus [3]	Infected OK?	Detected by '95?	Clean Boot?	Removal?	Comments
Boot-437	Y	Asks for COMMAND.COM	Y	Y	Only removed by Dr. Solomon's Magic Bullet, which is FAT32 compatible. Still infected other floppies.
Form.A	Y	Asks for COMMAND.COM	Y Invalid Media	Y	Only removed by Dr. Solomon's Magic Bullet, which is FAT32 compatible. Still infected other floppies.
Swiss-Boot.A	Y	While initializing VBACKUP could not load VFD.VXD Hang	Y	Y	Any attempt to SYS or remove this virus after a clean boot resulted in a message indicating that the drive was locked. Clean booting and using the LOCK C: command and then running SYS C: cleared the virus correctly. Dr. Solomon's Magic Bullet, reported that the drive was write protected.

Effects of Partition Sector [MBR] viruses?

Myth #3

MBR viruses cannot be removed from FAT32 partitions by non-FAT32 compatible anti-virus software.

This, you might think after *Myth#2*, and you'd be excused for thinking this, would be correct. Luckily for most MBR infectors this is not the case. In testing all the MBR viruses were successfully removed, without incident. Why is this the case, when DBR viruses refused to give up without a struggle?

The simple answer is that the MBR under FAT32 is practically the same as under DOS 6.0. Therefore, currently non-FAT32 compatible scanners can (*in almost all cases*) safely remove MBR viruses from FAT32 drives.

Test Results

This was an interesting group of viruses, especially as all of them were unable to infect floppy disks from within the Windows 95 GUI or DOS boxes run within it. (W*hile I was completing this paper, a new MBR infector was reported that could infect from within the Windows 95 GUI, the virus is known as Dodgy or Ravage*[Dr. Sol]). The greatest surprise was how badly some of the MBR viruses fared when trying to infect in '*MS-DOS Compatibility Mode*' and/or the '*Command Prompt Only*' boot option mode.

STOP PRESS: *Dodgy* has been tested and the results added to the table below. This MBR infector can infect floppy disks in all the test modes. It does this by deleting the *HSFLOP.PDR*[6] file from the *WINDOWS\SYSTEM\IOSUBSYS* directory. This simply removes the 32-bit floppy driver support, so that next time Windows '95 starts, the floppy drive is accessed using standard *DOS BIOS* routines instead. This type of attack is not new; the *Hare* family of viruses used this method too. Although in the tests carried out for this paper all *Hare* samples tested failed to go resident and infect the MBR or any files[7].

One thing to bear in mind, just because an MBR infector can't spread does not mean it is not a threat.

[6] This is the 32-bit floppy driver.
[7] As it is a multipartile virus.

Take *Kampana* as an example, even though it failed to replicate in testing, confirmed by at least one third party[Emm] , it's payload will almost certainly still trigger (*after 400 reboots, it overwrites the hard disk with garbage, then displays its message*). Others that refused to spread include*: AntiCMOS.A, Jumper.A, Stoned.Standard.A and V-Sign.A*.

Some of the test group offered '*General Failure Reading Drive A:*' messages, these were: *Michelangelo, ExeBug.C and Stoned.16*.

Quox refused to allow Windows 95 to boot, and would only infect floppy disks entered during the '*Diskette Read Failure*' message, which could not be bypassed.

Those that performed best[8], infecting on both 3 & 4[9], were: *AntiEXE.A, Leandro, ParityBoot.B, Ripper, Sampo, Stoned.Azuza, Stoned.Angelina, W-Boot.A and Welcomb*.

There were a number of MBR infectors that would only infect under condition 4, these include: *Monkey.B, NYB, and Stealth_Boot.C.*

All of those that successfully infected the MBR and went resident, apart from *Jumper.A* caused Windows 95 to report that the MBR had been changed (*Fig 1*), which dropped Windows 95 file and memory system mode from 32-bit (*Fig 3*) into MS-DOS Compatibility mode (*Fig 2*). Interestingly, even though the hard drive is in MS-DOS mode, the floppy driver is still running in 32 Bit mode[CN] *(that is why the floppy disks are not infected within the GUI by the viruses tested even though they infected the hard drives MBR and are resident*).

Why did all of the viruses that infected the MBR and went resident except *Jumper.A* have Windows 95 detect the change? The answer isn't all that mystical, simply all other tested MBR infectors hook Int 13h and Windows 95 actually monitors the Int 13h[10] vector code for modifications (*not the actual MBR or DBR*) as this will affect its ability to drive the hardware directly. Not surprisingly most MBR infectors will do just that. *Jumper.A* on the other hand hooks not Int 13h but Int 21h[11] instead, this means that Windows 95 can't see the change and therefore the warning messages are not shown.

Filler.A ,*Chinese-Fish* and both *Hare* samples refused to even go resident, let alone infect the test systems MBR.

On a clean boot all was fine except as expected for *Monkey.B* (*as it encrypts the MBR*), and *ExeBug.C* (*Invalid media when reading drive C:*). Even given these errors, the viruses were still correctly and easily removed, even with non-FAT32 specific scanners.

A number of the test set hung after infecting the hard drive, instead of giving the more usual '*Invalid system disk Replace the disk, and press any key*' or '*Non-system disk or disk error Replace and strike any key when ready*'messages. This simply needed the system to be rebooted for Windows 95 to load as normal, except for the warning messages (*Fig1 and Fig3*). The viruse exhibiting this phenomenen were: *AntiCMOS.A, Leandro, Parity_Boot.B and Stoned.16*.

The really interesting results are when these test results are compared to tests conducted by *Ian Whalley[Whalley]*. All the MBR and DBR viruses he tested replicated under FAT16 [4.00.950]. The viruses he tested were: *AntiCMOS, AntiEXE, Monkey.B, Form, Jumper.B, NYB, ParityBoot.B, Quandry, Sampo, Stoned.Angelina and V-Sign*.

Yet in another test conducted [VB2], *Jumper* failed to infect other floppies as found in the tests carried out for this paper. On the other hand *Kampana* and *V-Sign* apparently did replicate in the same test conducted by Virus Bulletin, but failed to when tested for this paper!

But if we look closer these tests[VB2] were done on a pre-release version of Windows 95 [4.00.347] and

---

[8] Apart from Dodgy which was tested as this paper was being completed.
[9]Test Types, (1) = From Explorer (My Computer A:) (2) = DOS BOX Within 95 (3) = Restart in MS-DOS Compatibility Mode (4) = Restart, F8 and Command Prompt Only.
[10] ROM BIOS Disk Interrupt
[11] DOS Function Calls

this may go some way to explain the anomolies found in this and other tests by Ian Whalley [4.00.950][Whalley] and David Emm [4.00.950][Emm] when comapred with later versions of Windows 95 tested for this paper [4.00.1111].

As you can see the results are somewhat different. Are the different results due to FAT32 and or other changes in OSR 2.x, or something else? I feel that more testing is required to get the diffinitive answer, and unfortunately this is beyond the scope of this paper.

Virus [31]	Infected OK?	Detected by '95?	Clean Boot?	Removal?	Comments
AntiCMOS.A	Y Hang	Y	Y	Y	Won't infect another floppy at all
AntiEXE.A	Y	Y	Y	Y	Infects on 3 & 4
Chinese Fish	N				Hang
Dodgy (Ravage)	Y	Y	Y	Y	1 & 2 Only on next restart, deletes HSFLOP.PDR, 3 & 4 straight after infection.
ExeBug.C	Y	Y	Y Invalid drive specification when accessing drive C:		Removed A: drive entry from CMOS. Infects on 3 only, General failure reading drive A on 4
Filler.A	N				Won't infect MBR or go resident.
Hare.7610	N				Won't infect MBR or go resident.
Hare.7786	N Hang				Won't infect MBR or go resident.
Jumper.A	Y	N	Y	Y	Won't infect another floppy at all
Kampana.A	Y	Y	Y	Y	Won't infect another floppy at all
Leandro	Y Hang	Y	Y	Y	Infects on 3 & 4
Michelangelo	Y	Y	Y	Y	General failure reading drive A on 3 & 4, but floppy still infected.
Monkey.B	Y	Y	Y Invalid Media	Y	Infects only on 4.
NYB	Y	Y	Y	Y	Infects only on 4.
PartityBoot.B	Y Hang	Y	Y	Y	Infects on 3 & 4
Quox	Y				Diskette Read Failure. On boot infects other diskettes.
Ripper	Y	Y	Y	Y	Infects on 3 & 4
Russian Flag	Y	N Hang & Reboot	Y	Y	Infects on 4 only. Hang & Reboot cycles until Safe Mode chosen, then when restarted in normal mode Exception OE Occurs
Sampo	Y	Y	Y	Y	Infects on 3 & 4
SheHas	Y	Y	Y	Y	Infects on 3 only. Appears to disinfect itself on 4, virus no longer found after that.
Stealthboot.C	Y	Y	Y	Y	Infects on 4 only.
Stoned.16	Y Hang	Y	Y	Y	General failure reading drive A on 3 & 4, but floppy still infected
Stoned.Angelina	Y	Y	Y	Y	Infects on 3 & 4 only.
Stoned.Azuza	Y	Y	Y	Y	Infects on 3 & 4 only.
Stoned.June4th.A	Y	Y	Y	Y	General failure reading drive A on 3 & 4, but floppy still infected
Stoned.Noint.A	Y	Y	Y	Y	Infects on 3 & 4 only, some directory entries corrupted.
Stoned.Standard.A	Y	Y	Y	Y	Won't infect another floppy at all
Swedish Disaster.A	Y	Y	Y	Y	Won't infect another floppy at all
V-Sign.A	Y	Y	Y	Y	Won't infect another floppy at all
Wboot.A	Y	Y	Y	Y	Infects on 3 & 4 only.
Welcomb	Y	Y	Y	Y	Infects on 3 & 4 only.

1 = *From Explorer (My Computer A:)*
2 = *DOS BOX Within 95*
3 = *Restart in MS-DOS Compatibility Mode*
4 = *Restart, F8 and Command Prompt Only*

Effects of File Infecting viruses?

Myth #4

You can't boot clean from an OSR2 boot disk, the virus is still found in memory.

This rumour has been impossible to verify first hand. I contacted Virus Bulletin and spoke to Nick Fitzgerald (*the editor*) and he confirmed that this rumour was passed to him via trusted third parties[12].

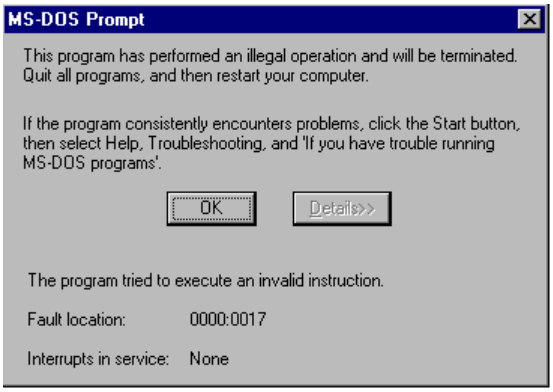
The situation, in which this problem appears to occur, is where small drives or small partitions are used. It is possible that after booting from the Windows 95 rescue disk and running your anti-virus software that it may report that the virus is still in memory (*even though it really isn't (this is known as a false positive or ghost positive*)). To resolve this issue simply add a **`CONFIG.SYS`** file with the following entry: **`BUFFERS=5,`** or **`8`**.

It is further suggested to address this problem that you use a DOS 6.x boot disk to clean boot from before trying to remove an MBR infector.

STOP PRESS: After further research I managed to confirm this myth when either *McAfee* or *Norton Anti-Virus* was used after a clean boot. The tips suggested were tried and appeared not to alleviate the false alarm problem with these products. All the other scanners tested did not suffer from this false alarm problem.

Test Results

Fig 4



This set of viruses gave the widest range of results, not surprising really when you consider the number of different types of file infecting viruses there are.

A number of viruses that went resident completely refused to infect any files whatsoever. These include old and new viruses, such as*: Tequila, Cawber, Die_Hard, both Hare samples and Ginger.*

Others just produced the '*illegal operation*' dialogue box (*Fig 4*), and refused to do anything more. These included: *Goldbug, Dark Avenger.1800 and 2100, Neuroquilla and MacGyver.*

A further subset produced the more drastic '*Fatal Exception xx*' message that invariably ended up with the system either becoming extremely unstable or having to be restarted. These included: *ByWay, Green Caterpillar, Tremor and Frodo.*

There were a reasonable number of viruses that could survive and replicate successfully within a single DOS box. These included: *Anticad.4096.Mozart, Avispa and even old favourites such as Cascade and all of the tested Jerusalem variants*.

A few viruses could survive and replicate in all DOS boxes, these were: *Barrotes.1303 and Three_Tunes.1784.* Both these viruses infected *COMMAND.COM,* so this may explain why this was possible, although other viruses infected *COMMAND.COM* but were not viable outside the single DOS box they went resident in, these were: *Barrotes.1310.A, CPW.1527, Fairz, Kaos4 and Npox.963.A*.

Only one that could infect not only all target files, in all DOS boxes but also could infect DOS files executed from Explorer! This was: *No_Frills.Dudley*.
Comparing these results with other papers that have tested earlier versions of Windows 95 shows

[12] Dr. Solomons also sent out a Press Release on this very subject.

similar results. David Emm's paper [Emm] confirms the findings here with regard to *Cascade* and *Yankee.Doodle* and *Frodo*, but not *Tequila*. The difference with *Tequila* may be explained by the use of FAT32 partitions in this paper compared to FAT16 in his tests. The test carried out by Ian Whalley [Whalley], confirms the behaviour observed with *ByWay*, *Jerusalem, Kaos4 and Taipan.438*.

It appears that the tests carried out for this paper use the largest set of viruses of the known papers written to date. In many ways I can understand why as this level of testing is rather time consuming.

Virus [82]	Infected OK?	Detected by '95?	Clean Boot?	Removal?	Comments
Anticad.4096.Mozart	Y	N	Y	Y	Infected *.COM files in same DOS box.
Avispa	Y	N	Y	Y	Infected *.EXE files in same DOS box.
Bad_Sectors.3428	N Resident				No files infected.
Barrotes.1303	Y	N	Y	Y	Infected *.COM & *.EXE files in ALL DOS boxes. Infected COMMAND.COM Won't infect files from Explorer.
Barrotes.1310.A	Y	N	Y	Y	Infected *.COM files in same DOS box. Infected COMMAND.COM
Bootexe.451 [MP]	Y Hang	N	Y	Y	Invalid Media Type reading type C: Missing COMMAND.COM Infected COMMAND.COM & MBR.
ByWay	N	Y	N	N	Fatal Exception 0D at 0DDC:000078C6
Cascade.1701.A	Y	N	Y	Y	Infected *.COM files in same DOS box.
Cascade.1704.A	Y	N	Y	Y	Infected *.COM files in same DOS box.
Cawber	N Went Resident				No files infected.
ChangSha.MP.3072	Y	N	Y	Y	Infected *.COM & *.EXE files in same DOS box.
Chaos.1241	Y	N	Y	Y	Infected *.COM & *.EXE files in same DOS box. Message: "Cannot Execute <filename>" when resident.
Cordobes	N				No files infected.
CPW.1527	Y	N	Y	Y	Infected *.COM & *.EXE files in same DOS box. COMMAND.COM also infected.
Dark.Avenger.1800.A	Y				Illegal Op Dialogue
Dark.Avenger.2100	N				Illegal Op Dialogue Fault location: 0DDC:10000
Demon.1759	Y				Illegal Op Dialogue
Desperado	N Resident				TOM reduced by 4KB No files infected.
Die-Hard	N				Nothing infected.
Dir-II	N				Illegal Instruction, Program Terminated. Nothing infected.
Fairz	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box. Infected COMMAND.COM
Fichv.2-1	Y	N	Y	Y	Infected *.COM files in same DOS box.
Flip.2153.A	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Flip.2343	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Freddy_Krueger	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Frodo	N				Fatal Exception Error 06 at 9EA0:00000431.
Ginger.2774	Y Resident				No files infected.
Goldbug	Y	Y	Y	Y	Illegal Op Dialogue. No files infected.
GreenCaterpillar.1575	Y				Fatal Exception 06 at 032E:00000467 On reboot COMMAND.COM found to be infected.
Hare.7750	N				Divide Overflow Error. No files infected.
Hare.7786	N				Illegal Op Dialogue (4BF3:FFFF). No files infected.
Helloween.1376.A	Y	N	Y	Y	Infected *.EXE in same DOS box.
Hi.460	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
HLLC.Even_Beeper.B	N				No files infected.
Jerusalem.1244	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Jerusalem.1808.Standard	Y	N	Y	Y	Infected *.COM files in same DOS box.
Jerusalem.Mummy.1364.A	Y	N	Y	Y	Infected *.EXE in same DOS box.
Virus [82]	**Infected OK?**	**Detected by '95?**	**Clean Boot?**	**Removal?**	**Comments**
Jerusalem.Sunday.A	Y	N	Y	Y	Infected *.COM *.EXE in same DOS

					box.
Jerusalem.Zero-Time_Australian	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Junkie	Y	Y	Y	Y	Infected WIN.COM & MBR No files infected in DOS Box.
Kaos4	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box. Infected COMMAND.COM & WIN.COM
Keypress.1232.A	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Lemming.2160	Y	N	Y	Y	Infected *.COM & *.EXE in same DOS box.
Liberty	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Little_Red.1465	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
MacGyver.2803	N	Y	N	N	Illegal Op Dialogue. No files infected.
Maltese_Amoeba	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Manzon	N				No files infected.
Markt.1533	N				No files infected.
Mirea.1788	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Natas.4744	N From DOS Box Y In DOS Mode	Y	Y	Y	In DOS Mode: Infected MBR, MEM.EXE, WIN.COM, DBLBUFF.SYS, COMMAND.COM and SETVER.EXE
Necros	Y	N	Y	Y	Infected *.COM in same DOS box. Overwriting.
Neuroquila	N	Y	N	N	Illegal Op Dialogue
Nightfall.4518.B	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box. Fatal Exception 06 at 9EDD:00000560 when exiting DOS box. Win 95 crashed.
No_Frills.Dudley	Y	N	Y	Y	Infected *.COM *.EXE in same ALL DOS boxes, and files executed from Explorer. Infected COMMAND.COM..
No_Frills.No_Frills.843	Y	N	Y	Y	Infected *.EXE in same DOS box.
Nomenklatura.A	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
November_17th.800.A	Y	N	Y	Y	Infected *.COM in same DOS box.
Npox.963.A	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box. Infected COMMAND.COM
One-Half.3544	Y	N	Y	Y	MBR infected. Encrypted cylinders 256-259
Ontario.1024	Y	N	Y	Y	Infected *.COM in same DOS box.
Pathogen:Smeg.0_1	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Ph33r.1332	Y	N	Y	Y	Infected *.COM & *.EXE in same DOS box.
PHX.965	Y	N	Y	Y	Infected *.COM *.EXE in same DOS box.
Predator.2448	N				Reboot system.
Reverse.948	Y	N	Y	Y	Infected *.COM & *.EXE in same DOS box.
Sayha	N				Nothing infected.
Scitzo.1329	Y	N	Y	Y	Infected *.COM & *.EXE in same DOS box.
Screaming_Fist.II.696	Y	N	Y	Y	Infected *.COM & *.EXE in same DOS box.
SVC.3103.A	Y	N	Y	Y	Infected *.COM & *.EXE in same DOS box.
Taipan.438	Y	N	Y	Y	Infected *.EXE files in same DOS box.
Tentacle.1996	Y	N	Y	Y	Infected DEFRAG.EXE, TWUNK_16.EXE, SCANDSKW.EXE
Taipan.666	Y	N	Y	Y	Infected *.COM files in same DOS box.
Tequila	N				Nothing infected.
Three_Tunes.1784	Y	N	Y	Y	Infected *.EXE files in ALL DOS boxes, but not from Explorer. Infected COMMAND.COM.
Tremor	N				Fatal Exception Error 06 at 9EF5:000090AF.
Vacsina.TP-05.A	Y	N	Y	Y	Infected *.EXE files in same DOS box.
Vacsina.TP-16.A	Y	N	Y	Y	Infected *.COM & *.EXE files in same DOS box.
Vienna.648.Reboot.A	Y	N	Y	Y	Infected *.COM in same DOS box. DIR Stealth?
Yankee Doodle.XPEH.4928	Y	N	Y	Y	Infected *.COM & *.EXE in same DOS box.
Yankie-Doodle.TP39	Y	N	Y	Y	Infected *.COM & *.EXE files in same DOS box.
Yankie-Doodle.TP44	Y	N	Y	Y	Infected *.COM & *.EXE files in same DOS box.

Shall I Compare Thee …. to NT?

As an interesting aside, it seemed useful to compare the results above with those reported by David

Aubrey-Jones in his paper on NT[Jones].

Why, you may ask?

Well the test set of viruses used here is a superset of those used for that paper. Therefore it seems useful to do some form of comparison of how viruses behave under GUI operating systems, well some of you may think so at least, so lets begin….

DBR infectors:
It is interesting that like FAT32, NT does like seem to like DBR infectors. Both *Form.A* and *Boot-437* stopped NT dead in its tracks.

MBR Infectors:
This set of viruses' results under NT when compared to those reported in this paper is a little more varied. Of those that were unable to infect NTFS, only *Chinese Fish* also balked at FAT32 infection. The others that refused on NTFS, but did not object to FAT32 were: *ExeBug.C, ParityBoot.B and V-Sign*.

Those that infected NTFS fine without causing a hang were: *AntiCMOS.A, NYB, Ripper, NYB and Stoned.Standard.A.* All of these were perfectly able to infect and either refused to infect another host, or spread only under limited circumstances on FAT32.

Those that caused NT to fail to boot were: *Kampana.A, StealthBoot.C and Monkey.B*. The results on FAT32 were not as drastic as on NFTS, all infected the MBR without incident and went resident. Kampana.A refused to infect any other host, both Monkey.B and StealthBoot.C would only infect under condition 4[13].

File Infectors:
This set of viruses most closely matched the results of the NT tests on NTFS. Of the 44 successful file infecting viruses used in the NTFS test and in this paper, only 6 refused to infect and spread under FAT32. These were: *Die-Hard, HLLC.Even_Beeper.B, Markt.1533, Predator.2448, Sayha and Tremor*.

Of the 19 file infecting viruses that refused to operate on NT on NTFS, that were also used in the tests for this paper, 10 refused to work at all or produced error messages. The remaining 9 that failed under NTFS worked at least partially under FAT32. These were: *BootExe.451, GreenCaterpillar.1575, Junkie, Maltese Amoeba, Natas.4744, One-half.3544, Pathogen:Smeg.0_1, SVC.3103.A and Tentacle*.

It appears that the greater part of the viruses tested under NTFS and FAT32 appear to work at least reasonably, though many shoot themselves in the foot by trying to be too clever.

[13] Restart, F8 and Command Prompt Only

Conclusions

As stated in the 1996 Virus Bulletin opening address by Steve White "*Microsoft has done more to solve the virus problem than the anti-virus industry*", this I believe is still true today, although the anti-virus community have not been napping.

FAT32 has brought a new level of problems for the virus writer to overcome. The simpler viruses appear to work best, those that are trying to be clever, use excessive stealth or undocumented or unusual features seem most likely to come unstuck.

It is clear from other papers written on Windows 95 and viruses, when compared to the tests carried out for this paper, that FAT32 has caused more problems for certain classes of viruses[14]. In some situations either causing the virus to be unable to go resident or the more annoying and potentially dangerous situation where the virus is resident, but cannot replicate although the trigger routine is still viable and potentially destructive.

The main viruses that appear to be seriously inconvenienced are the DBR infectors. These in the tests conducted give themselves away very quickly and noticeably.

Macro viruses appear to be the least affected by the appearance of FAT32[15], which is not surprising in that the operating system that macro viruses run within are currently Word, Excel and WordPro. A small number of these viruses may be caught out, but in the main this is likely to be the main threat to Windows 95 users, at least until FAT32 compatible DBR infectors and more 32-bit Windows 95/NT viruses appear.

Furthermore, it is clear that the anti-virus software tested for this paper, that non-FAT32 compatible scanners cannot remove DBR viruses from an infected FAT32 partition. Of course before long all anti-virus software will have to be FAT32 compatible because it is certain that some miscreant will write a FAT32 DBR infector just to prove it can be done.

The appearance of Dodgy is rather timely, although this is not a FAT32 specific virus it uses known anti-Windows '95 32 driver attacks. Could this the forerunner to the first FAT32 compatible DBR virus?

[14] As did NT and NTFS.

[15] Although no structured testing on macro viruses was carried out for this paper, research to date clearly show that Microsoft Office is the macro viruses' host 'operating system', and unless they attempt to call another operating system (DOS, etc.) then they are unlikely to be inconvenienced.

Appendices

Technical Implementation

The following information is supplied to show the changes that have taken place with the advent of FAT32. This not only covers the changes in the DBR but other interrupt routines for disk access and free space detection, amongst others. There is little discussion of the information raised here as I feel that this would be only useful to the virus authors, rather than the AV industry as they already have this information available to them and more besides.

The following are all the valid partition types and their corresponding values for use in the **Part_FileSystem** member of the **s_partition (FAT32)** structure.

Partition Types Value	Description
PART_UNKNOWN(00h)	Unknown
PART_DOS2_FAT(01h)	12-bit FAT
PART_DOS3_FAT(04h)	16-bit FAT. Partitions smaller than 32MB.
PART_EXTENDED(05h)	Extended MS-DOS Partition
PART_DOS4_FAT(06h)	16-bit FAT. Partitions larger than or equal to 32MB.
PART_DOS32(0Bh)	32-bit FAT. Partitions up to 2047GB.
PART_DOS32X(0Ch)	Same as PART_DOS32(0Bh), but uses Logical Block Address Int 13h extensions.
PART_DOSX13(0Eh)	Same as PART_DOS4_FAT(06h), but uses Logical Block Address Int 13h extensions.
PART_DOSX13X(0Fh)	Same as PART_EXTENDED(05h), but uses Logical Block Address Int 13h extensions.

Microsoft have added two new partition type markers to identify FAT32 partitions, these are 0Bh and 0Ch. Both these partition markers clearly identify the partition as FAT32.

FAT32 File System Structures

With the addition of the FAT32 file system, the BPB, DPB, and DEVICEPARAMS structures were updated to accommodate FAT32 information. Additionally, subordinate structures have been implemented to support the FAT32 file system main structures. These changes are effective for Windows OEM Service Release 2 and later.

BPB (FAT32)
BIGFATBOOTFSINFO (FAT32)
DPB (FAT32)
EA_DEVICEPARAMETERS (FAT32)
ExtGetDskFreSpcStruc (FAT32)
***s*_partition (FAT32)**
SDPDFormatStruc (FAT32)

Note: Many data structures in this section are listed as **reserved**. This indicates that the user is not to assume or modify the values within these fields. They are used by the file system itself and are not available for any enhancements.

Boot Sector and Bootstrap Modifications [MS]

Reserved Sectors	FAT32 drives contain more reserved sectors than FAT16 or FAT12 drives. The number of reserved sectors is usually 32, but can vary.
Boot Sector Modifications	Because a FAT32 BIOS Parameter Block (BPB), represented by the **BPB (FAT32)** structure, is larger than a standard BPB, the boot record on FAT32 drives is greater than 1 sector. In addition, there is a sector in the reserved area on FAT32 drives that contains values for the count of free clusters and the cluster number of the most recently allocated cluster. These values are members of the **BIGFATBOOTFSINFO (FAT32)** structure which is contained within this sector. These additional fields allow the system to initialize the values without having to read the entire file allocation table.
Root Directory	The root directory on a FAT32 drive is not stored in a fixed location as it is on FAT16 and FAT12 drives. On FAT32 drives, the root directory is an ordinary cluster chain. The **A_BF_BPB_RootDirStrtClus** member in the **BPB (FAT32)** structure contains the number of the first cluster in the root directory. This allows the root directory to grow as needed. In addition, the **BPB_RootEntries** member of **BPB (FAT32)** is ignored on a FAT32 drive.
Sectors Per FAT	The **A_BF_BPB_SectorsPerFAT** member of **BPB (FAT32)** is *always* zero on a FAT32 drive. Additionally, the **A_BF_BPB_BigSectorsPerFat** and **A_BF_BPB_BigSectorsPerFatHi** members of the updated **BPB (FAT32)** provide

equivalent information for FAT32 media.

Equipment Used

Dell Optiplex GXi 500
200Mhz MMX Processor
32Mb Memory
2GB SCSI Hard discSCSI (2GB Hard Disk on Adaptec Controller)

- Drive partitioned into 2 x1GB partitions.
- Formatted to FAT32.

Windows 95 OEM OSR 2.1

116 viruses used in the tests were selected from the March 1997 edition of the 'Wild List' published by Joe Wells[16]. These were chosen as they are considered to be those most likely encountered by the user-community at large.

Clean Boot Disk

Created by running FORMAT.COM from the WINDOWS\SYSTEM directory with the /S switch and then copying SYS.COM and FDISK.EXE to it.

[16] This did not include Dodgy. As this was felt to be of interest it was included at the last moment.

Alt.Comp.Virus Newsgroup Postings

```
From: bontchev@complex.is (Vesselin Bontchev)
Newsgroups: alt.comp.virus
Subject: Re: McAfee VirusScan 3.0 and Fat32
Date: 11 Apr 1997 12:37:09 -0000
Organization: Frisk Software International
Message-ID: <5ilb9l$m1i@banani.complex.is>
References: <3349ba7e.17705931@news.dfwmm.net>
NNTP-Posting-Host: banani.complex.is
X-Newsreader: TIN [UNIX 1.3 950824BETA PL0]
Lines: 62
Xref: demon alt.comp.virus:59264

David Levin (dlevin@dfwmm.net) wrote:

> "Chengi J. Kuo" <cjkuo@alumnae.caltech.edu> wrote:
>
> > 1) A Master Boot Record infection is independent of whether it's on a
> > FAT32 system or not.  FAT32 is in boot sectors.  If any virus infects the
> > MBR of a FAT32 machine, any present day AV can handle it.
>
> Then why in the activity log when I run your product does it say 'error
> reading boot record'.   How can it clean it if it can't read it ?

The error occurs when reading the _DOS Boot Sector_ of the FAT32
partition - not when reading the MBR. The scanners have no problems
reading the MBR of a machine that has FAT32 partitions, finding viruses
in that MBR, and disinfecting them. It's the DBS that is problematic -
but, as Jimmy said, if the scanner reports a problem with that DBS, it
means that the DBS is *not* infected. If it becomes infected, the
scanner will be able to read it and disinfect it too.

> > 2) There are no present day boot sector viruses which infect a FAT32 boot
> > sector and doesn't destroy it in the process.  And in so doing, it
> > converts it into a FAT16 infected boot sector.  So any present day
> > infected FAT32 system will be detectable by present day AV.
>
> It's one thing to detect a virus, it is another to CLEAN it.   If the
> virus converts the FAT32 boot record to a FAT16, how will McAfee CLEAN
> it ?

The scanners in general and McAfee's scanner in particular have no
problems cleaning the boot records of FAT16 partitions. Since the
infected FAT32 partition looks like a FAT16 partition to the scanner, it
will have no problems cleaning it.

> It  might be able to clean it to be an uninfected FAT16 boot record,
> but it won't be able to convert it back to the original FAT32 boot
> record

Yes, it *will* be. Trust me - or try it for yourself, if you don't.
However, note that some of the existing boot sector viruses can *damage*
a FAT32 partition and make it non-bootable when infecting it. Removing
the virus won't restore the damage caused by it; you'll have to run SYS
on that partition.

> How can FAT32 McAfee users be 'safe',  when if a virus attacks their
> boot sector,  McAfee will not be able to CLEAN it or restore it from the
> emergency disk ?

It will be able to CLEAN it. Just as any other disinfector.

> In other words,  their hard drive will probably be unusable.

It might be non-bootable, but that would be caused by the virus, not by
the disinfector.

Regards Vesselin
--
Vesselin Vladimirov Bontchev, not speaking for FRISK Software International,
Postholf 7180, IS-127, Reykjavik, Iceland              producers of F-PROT.
e-mail: bontchev@complex.is, tel.: +354-561-7273, fax: +354-561-7274
PGP 2.6.2i key fingerprint: E5 FB 30 0C D4 AA AB 44  E5 F7 C3 18 EA 2B AE 4E
```

From: "Chengi J. Kuo" <cjkuo@alumnae.caltech.edu>
Newsgroups: comp.virus
Subject: Re: McAfee VirusScan 3.0 and Fat32 (WIN95)
Date: 15 Apr 1997 13:19:14 -0000
Lines: 149
Sender: news@Lehigh.EDU
Approved: virus-l@Lehigh.EDU
Message-ID: <0021.01IHR6JG5DL09FNGZC@csc.canterbury.ac.nz>
NNTP-Posting-Host: fidoii.cc.lehigh.edu
X-Date: Sat, 12 Apr 1997 20:24:04 +0000 (GMT)
X-Digest: Volume 10 : Issue 63

David Levin <dlevin@dfwmm.net> writes:
>"Chengi J. Kuo" <cjkuo@alumnae.caltech.edu> wrote:

Sigh. I hated writing my first response and now I must do it again.

Mr. Levin,

It is obvious that you have not been infected on the FAT32 system
and are making assumptions.

>> 1) A Master Boot Record infection is independent of whether it's on a
>> FAT32 system or not. FAT32 is in boot sectors. If any virus infects the
>> MBR of a FAT32 machine, any present day AV can handle it.
>
>Then why in the activity log when I run your product does it say 'error
>reading boot record'.   How can it clean it if it can't read it ?

Let me go back to the one point I made previously, "And in so doing, it
converts it into a FAT16 infected boot sector." (see in point 2 below)

No. It *is* clean. If it were infected, the virus would have turned it
into a FAT16 boot sector. And any present day AV would be able to handle
it. Even ones which do not claim to know about FAT32 boot sectors.

Of course, after it's restored, and the next time you reboot, it's
FAT32 and our scanner will refuse to scan it. But it will be clean!
And we will have restored it. (Not just us. Any current day product
will.) But as I noted earlier, the next version will support FAT32.

>> 2) There are no present day boot sector viruses which infect a FAT32 boot
>> sector and doesn't destroy it in the process. And in so doing, it
>> converts it into a FAT16 infected boot sector. So any present day
>> infected FAT32 system will be detectable by present day AV.
>
>It's one thing to detect a virus, it is another to CLEAN it.   If the
>virus converts the FAT32 boot record to a FAT16, how will McAfee CLEAN
>it ?

Generally, it cleans by finding the original boot sector. It does this
by knowing, "I've found XYZ. XYZ relocates the original to (cylinder,
track,sector). Get it. Put it back." It matters not what the original
was. (You may now join into the debate between Mr. Bontchev and one of
his customers about the validity of this approach.)

> It might be able to clean it to be an uninfected FAT16 boot
>record, but it won't be able to convert it back to the original FAT32
>boot record since McAfee STILL does not support it (after 7+ months
>since WIN95 OSR2 came out).

This is an incorrect assumption. See above.

> The emergency disk will be no help, because
>unlike Norton, McAfee does not back up the Boot record to the emergency
>disk.

This is correct.

>> 3) What does FAT32 support mean? It means if you're up and running on
>> FAT32, you don't get the "cannot access" message. But if you get that
>> message today, you're clean!
>>
>> The fact is, the same reason why AV had to be rewritten, none of the
>> viruses understand FAT32 either.
>>
>> On the question of whether we support FAT32. Version 3.0 was supposed to.

>> But it didn't make it. But you can find FAT32 support in today's beta.
>> And it will be in 3.0.2.
>
>It is still not on your BETA site. How many more months will it take to
>support FAT32 ?

Are you looking for the DOS version or the 95 version? Only the DOS
version is available there (http://beta.mcafee.com/public/datafiles).
(And the next DOS version will be numbered 3.0.1.)

The next DOS version will be released this month. The other platforms to
follow shortly.

>> So in direct response to the suggestion that McAfee users are not safe
>> if using a FAT32 system, you are incorrect. McAfee users today are safe.
>> And furthermore, there are no boot sector viruses that correctly infect
>> a FAT32 boot sector today.
>
>How can FAT32 McAfee users be 'safe', when if a virus attacks their
>boot sector, McAfee will not be able to CLEAN it or restore it from the
>emergency disk ?

An incorrect statement. I covered that above.

> In other words, their hard drive will probably be unusable.

An incorrect assumption.

> Why is this incapability problem not stated in the
>documentation or in the 'Know Issues' section of the Read Me file ?

Since we made no claims of FAT32 compatibility, I didn't see a need to
have such a warning. Since there are no FAT32 boot sector viruses, there
is no "issue" to be "known."

Now, if we made such a claim and it was not true, that would be an issue
where I would go and berate someone.

> Why is it taking so long to support an operation/disk system that came out
>over 7 months ago ? Your competitors have.

Ah. Someone is questioning my decision making in supporting our users.
(Those were my decisions and they do represent McAfee's position on this.)

[I pulled up my other response to you. But apparently, you changed your
question from "8 months" to "7 months". No matter. It'll be 8 months
soon enough.]

We've been concentrating on macro viruses because *I* think it's
more important. In the 8 months, there hasn't been a native FAT32
boot virus.

Would you ask our "competitors" who support FAT32 how their Office97
support compares to McAfee's? Office97 was released in January. We
had betas available immediately. And we shipped late Feb. The first
Word97 virus was dicovered on a Microsoft Web site late January or
early February. Only 2 products at the time, I believe, could even claim
to be able to handle it. I think we're approaching 10 such beasts
now. I think there's 4 or 5 companies claiming to handle them.

I'm glad there are companies who feel a compunction to supply you with
FAT32 support. One such company you mentioned earlier also claimed
they could detect all Java viruses last year. My marketing people
were on me immediately. "Look," I said, "we detect all the Java
viruses there are. No changes necessary. And a year from now, it'll
still be true." (It's a year now.)

All companies I'm sure have limited resources. I have to assign my
people to where I assess the dangers will be for our customers.

But, as I said, our next version will have FAT32 support. But, I will
also tell those people who do not quickly upgrade to that version.
"Look, we detect all FAT32 viruses there are. No changes necessary.
And many months from now, it'll still be true."

Mr. Levin, unless you're not a user of Word and Excel, you will come to
realize that the time we have spent to crack OLE2 and Office97 (and

de facto, Word6 and 7 and Excel 5) will be more significant to you in
the near term as well as the long run.

Jimmy Kuo
Director, AV Research
cjkuo@mcafee.com

From: Nick FitzGerald <n.fitzgerald@csc.canterbury.ac.nz>
Newsgroups: comp.virus
Subject: Re: Please clarify some FAT32 issues (WIN95)
Date: 15 Apr 1997 13:19:12 -0000
Lines: 80
Sender: news@Lehigh.EDU
Approved: virus-l@Lehigh.EDU
Message-ID: <0020.01IHR6JG5DL09FNGZC@csc.canterbury.ac.nz>
NNTP-Posting-Host: fidoii.cc.lehigh.edu
X-Date: Fri, 28 Mar 1997 10:10:02 +1300
X-Digest: Volume 10 : Issue 63

John Humphries <jh@sherpanet.com> wrote:

> Reading the moderator's note appended to Doug Muth's "Re: onehalf.mbr &
> win95 problem" I'm left somewhat confused. The pre-pended note says
> "...the important thing about booting clean is to do so with a non-Win95
> boot disk...": will files on a FAT32 disk be accessible when booted from
> an earlier version of DOS (e.g., DOS6.22)?

No. MS-DOS 7, build 950 (the one that reports "Windows 95. [Version
4.00.950]" in response to the VER command) and all earlier DOSes (MS and
others) do not "understand" the FAT32 file allocation system *and* could
otherwise be tripped up by other aspects of the FAT32 file system.

My recommendation when facing an MBR infection on a Windows 95 machine is
to boot with a pre-Win95 DOS diskette. This is true of "classic" Win95
and OSR2 systems (whether the latter have FAT32 drives or not). This is
because of a difference in operation between earlier DOSes and MS-DOS 7
that means very often your AV software will warn you that the virus is "in
memory" (and usually refuse to continue!) even though you really have
"booted clean". I recently learned (thanks Ilia) that this ghost positive
problem is easily averted with MS-DOS 7 by the simple expedience of
setting BUFFERS=5 in the CONFIG.SYS file on your boot floppy (for some of
the technical details look in the archives for digests around V10 #50-52--
also Jimmy Kuo addresses some of these issues in a post in this Digest).

> The post-pended note says "...with Win95 OSR2's FAT32 you may need an
> updated DOS AV s/w...": what are some examples of such software,
> especially are there any shareware versions which can freely distributed
> to people?

I'll leave it to the vendors to answer this...

However, the issues are that with FAT32 the (D)OS Boot Sector is not as
simple or rigid a structure as it has been, and a few new avenues of
infection are probably possible under FAT32. The potentially "mobile"
nature of various parts of the FAT32 file system that are accessed after
the MBR during the boot process means that (eventually) FAT32-aware AV s/w
will be necessary. However, although I referred to it as "DOS AV s/w" it
may be that such s/w will require a DOS 7 build 1111 (that which comes
with OSR2) or later to perform FAT32 disk and file I/O.

To the best of my knowledge, as I am writing this, there are no known
viruses that utilize any FAT32-specific attack methods.

> The note goes on "...deal with DBS infectors (see recent thread)...":
> searching through DejaNews about a week ago I was unable to find any
> references to DBS in their comp.virus archive - where can I find this?

There had been several posts mentioning FAT32 support and querying whether
certain products had it or not. Some of these have been posted in the
interim between John submitting his post and my response. Hopefully these
have (helped) answer the question.

> Still more "...MBR infectors should still be dealt with on FAT32 drives
> with 'old' DOS AV's..."; does this mean that we need to boot with a
> pre-FAT32 disk to check for MBR/boot sector viruses and with a FAT32

> disk to check for file infectors and macro viruses?

That will work, but was not (literally) what I meant. Had I written that more coherently (aka "less hurriedly") I may have written "'old' DOS AV's should still be able to deal with MBR infectors on FAT32 drives...". FAT32-aware AVs should be able to deal with MBR, DBS and file viruses (so long as you work around that false positive problem I mentioned earlier).

> I'm painfully aware that my understanding of these issues is sketchy at
> best, so please answer (or, at least raise) the questions that I should
> have asked about FAT32 (but didn't know enough to frame them) as well
> as the few that I managed to put into words.

Well, you certainly picked up a few too-roughly-sketched-out comments of mine...

Hope that helps!

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 Nick FitzGerald, PC Applications Consultant, CSC, Uni of Canterbury, N.Z.
 n.fitzgerald@csc.canterbury.ac.nz  TEL:+64 3 364 2337, FAX:+64 3 364 2332
              Virus-L/comp.virus moderator and FAQ maintainer
   PGP fingerprint =  2E 7D E9 0C DE 26 24 4F  1F 43 91 B9 C4 05 C9 83
```

References

[Jones] David Aubrey-Jones, What Threat Are Viruses On Windows NT – Virus Bulletin Conference 1996.

[Whalley] Ian Whalley, Viruses in Chicago: The Threat to Windows 95 – IVPC ’96.

[Overton] Martin Overton, Anti-Virus in the Corporate Arena – Virus Bulletin Conference 1996.

[MS] Microsoft, MSDN Web Site.

[Dr. Sol] Dr. Solomon’s Virus Alert.

[Emm] David Emm, Windows 95 and Viruses – Dr. Solomon’s Technical Paper.

[CN] Carey Nachenburg.

[VB2] Virus Bulletin, Viruses on Windows 95 – Virus Bulletin - June 1995 pp15-17

[Kuo] Jimmy Kuo, Public Posting To The Alt.Comp.Virus Newsgroup.

[Bontchev] Vesselin Bontchev, Public Posting To The Alt.Comp.Virus Newsgroup.

[Fitzgerald] Nick Fitzgerald, Public Posting To The Alt.Comp.Virus Newsgroup.