Professional System Integrators Ltd.

438 Mt Albert Road
Mt Roskill
P O Box 9767
Auckland, New Zealand

Phone: (09) 629 0937
Mobile: (025) 922 088
Fax: (09) 629 0927
Email:bruce@help.co.nz

# File Extensions Overview

6 December 2001

When you receive an email there are times when there is a file attached to the message. The file typically has an extension ( the last 3 or 4 letters of the FileName ) that describes to the computer what it needs to view the file.

For example:

you receive a message with a file named: **myletter.doc**

the file extension starts after the last full stop, so this is a DOC file which as you see below is a MS Word Word Processing document. ( If you have a file called **myletter.doc.exe** this is a EXE file not DOC !! )

Note windows can be configured to NOT show the file extension, a number of viruses use this shortfall to fool you into thinking a file may be safe. For example a file called **fred.txt.exe** will show as **fred.txt** if you do not have the displaying of extensions turned on. Be very careful!!

## Sound/Image/Film Files (Safe)

These are generally safe files and can be opened if your computer has a program compatible with them.

| | | | |
|---|---|---|---|
| AVI | Movie | MP3 | Music File |
| AAS | Animation | MPG | Movie |
| AIFF | Sound | MPEG | Movie |
| AWA | Animation | MMM | Movie |
| AWM | Animation | MOV | Movie |
| AU | Sound | MOD | Music |
| BM | Graphic | PCX | Graphic |
| FLI | Animation | SND | Sound |
| FLC | Animation | TGA | Graphic |
| GIF | Graphic | TIF | Graphic |
| JPG | Graphic | TIFF | Graphic |
| JPEG | Graphic | VOC | Sound |
| MID | Music | WAV | Sound |

## Document Files (Safe to use)

The risk of a virus or Trojan in these is very low.

| | |
|---|---|
| CSV | Text |
| PDF | Adobe Acrobat Document |
| TXT | Text |
| WPD | Document WordPerfect document format |
| WPS | MS Works |

**Document Files (You need to Check these)**

These file May contain Viruses called MACRO VIRUSES
You need to check where these came from before opening them.

| | | | |
|---|---|---|---|
| DBF | Database | PPS | PowerPoint |
| DOC | Document MS Word or Windows95 WordPad | PPT | PowerPoint |
| | | XLS | Spreadsheet |
| RTF | Document Transferrable | WK1 | Spreadsheet |
| HTM | Web page | WK3 | Spreadsheet |
| HTML | Web page | WK4 | Spreadsheet |
| MCW | Document MS Word for MAC | WKS | Spreadsheet |
| MDB | Database | | |

**Program / Data files (Use only if known what they are)**

These file type contain instructions for the computer, and as such could cause problems. You need to check where these came from before opening them.

| | |
|---|---|
| .mdb | Microsoft Access program |
| .mde | Microsoft Access MDE database |

**Encoded or Compressed files (You need to Check these)**

These can contain one or more files of any type. Seek assistance before opening these.

| | | | |
|---|---|---|---|
| ARJ | Compressed | | |
| ARC | Compressed | UUE | Encoded |
| GZ | Compressed | USR | Encoded |
| HQX | Encoded (MAC) | Z | Compressed |
| LZH | Compressed | ZIP | Compressed |
| SIT | Compressed Mac | ZOO | Compressed |

**Program files (You should NEVER need to run one of these if emailed)**

There should be no reason to run a file with the following extension as these files should already be on your computer and any new ones emailed to you are more than likely a virus. Seek assistance if you receive one of these.

| | |
|---|---|
| .ade | Microsoft Access project extension |
| .adp | Microsoft Access project |
| .asx | Windows Media Audio / Video |
| .bas | Microsoft Visual Basic class module |
| .bat | Batch file |
| .chm | Compiled HTML Help file |
| .cmd | Microsoft Windows NT Command script |
| .com | Executable Program |
| .cpl | Control Panel extension |
| .crt | Security certificate |
| .dll | Program Component |
| .exe | Executable Program |
| .hlp | Help file |
| .hta | HTML program |
| .inf | Setup Information |
| .ins | Internet Naming Service |
| .isp | Internet Communication settings |
| .js | JScript file |
| .jse | Jscript Encoded Script file |
| .lnk | Shortcut |
| .msc | Microsoft Common Console document |
| .msi | Microsoft Windows Installer package |
| .msp | Microsoft Windows Installer patch |
| .mst | Microsoft Windows Installer transform; Microsoft Visual Test source file |
| .pcd | Photo CD image; Microsoft Visual compiled script |
| .pif | Shortcut to MS-DOS program |
| .prf | Microsoft Outlook profile settings |
| .reg | Registration entries |
| .scf | Windows Explorer command |
| .scr | Screen saver or Virus Trojan |
| .sct | Windows Script Component |
| .shb | Shell Scrap object |
| .shs | Shell Scrap object |
| .vb | VBScript file |
| .vbe | VBScript Encoded script file |
| .vbs | VBScript file |
| .wsc | Windows Script Component |
| .wsf | Windows Script file |
| .wsh | Windows Script Host Settings file |

# A Primer on Viruses and Generic AV

20 June 2000

Computer viruses are just computer code, deliberately written to serve a purpose - to replicate, there is absolutely nothing mysterious about them. There exist thousands of them – more than 60,000 in late 2001, including more than 2,000 macro viruses of Word and Excel, and new viruses add to the list every day.

Computer viruses are passed in many ways; by sharing software, in Word documents and in Excel worksheets, by downloading files from the Internet, in e-mail attachments, with OEM software bundled with computers, and sometimes even on pre-formatted floppies. There exist's no way to prevent ever picking a computer virus, except by never using a computer at all, just the same as one cannot avoid ever getting ill.

The threats that should raise most concern are those imposed by MS Word and Excel macros, and the new PE (Portable Executable) infectors, affecting Windows 95/98 and NT programs.

Macro viruses first appeared only in the summer of 1995. Since then, their number increased at the highest rate – 300 new macro viruses or variants per month – compared to the 'traditional' boot and program infectors, the latter 'suffer' from a rapidly decreasing production rate. The reasons are:

- MS Word, as well as Excel, are in common use as means of data interchange in both the private sector and in the corporate environment.

- What's required to write macro malware are just Word, or Excel itself, and minimum knowledge on how to use the Microsoft macro language. If writing virus code was in reach of thousands before, then tens of millions, maybe more, of users can now write macro malware. Corporate internal e-mail, the Internet and the increasing dependence on communication and data sharing makes the distribution of malware extremely easy.

There is a trend in macro malware that should raise even more concern. While conventional viruses found in the wild do not have an immediately destructive payload – as if they had, then their chances to spread would be nil, many macros are found to have a 'short fuse' until they trigger destructive routines. 'MDMA' (clears the entire C:\ root directory on the first of every month) and 'Appder' (kills crucial files in ..\Windows and ..\Windows\System the twentieth time Word is started), are just a couple of such macros. Since the appearance of this new threat, 'known' macro viruses aren't the real problem anymore. The threat are macro Trojans and bombs that are built in-house, based on techniques used in macro viruses. The latter techniques are now common knowledge, as result of macro viruses being so widely spread. No virus scanner, even the most up-to-date one, won't protect you from these new threats.

Categories of Computer Viruses

Generally, there exist four virus categories listed below by decreasing order of their prevalence in the wild:

- Macro viruses. They affect MS Word documents and Excel worksheets.
- Viruses that infect through the boot sector or partition sector (MBR), known as 'boot infectors'
- Viruses that infect through executable programs, known as 'file infectors'.
- Viruses that uniquely infect Windows 95/98 and NT PE (Portable Executable) objects, known as 'PE infectors' or PEI.

All DOS viruses fall into the second or third categories or both. There are also bipartite or multipartite viruses that combine the properties of the two categories (boot and file). Examples of common multipartite infectors are Junkie and Natas.

In late 1991, a new variant of file viruses emerged, known as cluster infectors. These viruses manipulate the file allocation table (FAT) pointers through the directory entries in order to infect. To this date, there are only three cluster infectors known to be in the wild, only two of survive in later than the Dos 5.0 environment.

A last type are the 'companion viruses', these are a variant on the file infector. A companion virus takes advantage of the properties of the operating system by spawning a companion to the victim program.

*Below is a quick definition of terms that are used to describe viruses and techniques employed by viruses*:

**Macro Viruses**

Most macro viruses known to be in the wild infect MS Word files, yet there exist macros that infect Excel files, although the latter are far less common than Word macro infectors. Word macro viruses replicate into other documents by first copying themselves into the Word global template (normal.dot). Then, the virus macros copy themselves into other documents, when opened or created with the affected template. In
order to assure the virus succession, infected documents are saved as templates, as only the latter can have active macros in them.

Excel macro viruses show a less distinctive pattern, when compared to Word viruses. From the few that exist, they all replicate by creating their own workbook, containing an auto startup macro (auto_open), and place that workbook in the Excel startup directory - normally ..\Excel\XLStart.

**PE Infectors**

Portable Executable (PE) objects were introduced with Windows 95 and NT. PE EXE files have a more complex structure than ordinary DOS executable files (EXE) and until recently, PE were considered beyond the reach of virus writers. Yet in mid-1998, a number of new PE infectors that were released in the wild became globally wild spread.

**Boot Viruses**

Boot viruses attack the boot sector and the MBR (master boot record, sometimes referred to as the partition sector). When the computer is turned on, it runs a couple of tiny program contained in these special sectors, first the partition bootstrap and then the system bootstrap, to ready itself for work. In case of a boot infection, one of these programs may simply be a virus. Boot viruses will remain active in memory while the computer is on. During this time they will infect write enabled floppies put in the floppy drive.

**File (Program) Infectors**

File infectors attacks executable program files, usually those having a COM or EXE extension name. Sometimes also files having an executable structure are targeted by viruses, regardless of their extension name. File infectors may corrupt non-executable files as well but they cannot spread this way.

Many file viruses are memory resident (TSR). After an infected file is executed, they will remain resident in the computer's memory until the computer is turned off. While in memory they will continue to infect other programs and may interfere with normal operations. If the computer is turned off they will lie dormant in an infected file until the program is executed and then load themselves back into memory again until the next time the computer is turned off.

### Multipartite Viruses (boot and file infectors)

Multipartite viruses infect both executable files and boot-partition sectors, sometimes the boot sector on floppies too. Some multipartite become infectious only after rebooting the computer from the infected MBR, like Tequila, others are equally infectious if loaded from file or through the boot process.

*Techniques used by Computer Viruses*

### Stealth

Stealth viruses are so named because they actively seek to hide themselves to prevent detection. Stealth viruses that infect files will subtract their own size (in bytes) from the infected host file at any time that a directory (DIR) command is executed or actually remove themselves from the file, to reinfect it again when the inspection is over.

Stealth file infectors are effectively handled by InVircible for DOS. For more information see in the IV on-line hypertext manual for DOS.

Some boot viruses use stealth (spoofing) techniques too. Stealth boot viruses will deceit disk editing tools, except ResQdisk. Examples of stealth boot viruses are Monkey, AntiEXE and B1-NYB. Natas and Gingerbread Man are multipartite viruses that use boot stealth too.

### Encryption

Most of modern viruses use encryption to evade detection by scanners. An encrypted virus has a very short common encryptor (from as few as 3 bytes, to a couple of dozen bytes) and the rest of the virus code is encrypted and differs from copy to copy of the virus. The detection of encrypted viruses cause high false alarm rates due to the ambiguity in the detection of the short common string. The removal of encrypted
viruses by scanners is rather difficult, in many instances it may result in the destruction of the program (especially in case of virus misidentification, which is very likely given their large numbers) and in even more instances - is simply impossible.

### Mutation Engine or Polymorphism

Polymorphic viruses have variable encryption. A polymorphic virus mutates itself so that the encryption varies between each occurrence of an infection. The detection of polymorphic viruses requires more complex than just plain string matching methods, like heuristics, which slows down scanning speed and increases false alarm rate. The detection and recovery from polymorphic viruses by scanner is even more difficult and dubious than with just encrypted viruses.

### Companion Viruses

Companion viruses take advantage of the precedence DOS gives to COM over EXE files in the order of execution. If there are two files bearing the same name, one with a COM extension name and the other with an EXE extension, then DOS will execute the COM file first. A companion virus is basically a Trojan that "infects" EXE files by spawning itself into a companion COM file, bearing the same name as the EXE file.
Sometimes the companion virus file will have its attribute set to 'hidden', to avoid its detection by the DIR command.

## Email Program

A number of viruses attack specific email programs and as microsoft seem to dominate the market place their applications MS Outlook, MS Exchange & MS Outlook Express are the main targets.
Microsoft in their wisdom have built smart features into these programs as well as in the newer versions of windows which give the virus writers even easier ways to write and send dangerous virus codes.
The typical scenario for a virus designed for Outlook etc.. Is for it when run to grab addresses out of your address book and send its self on to people who you normally communicate with.

## Prevention

I know you have heard this a million times, but here it is again.

**DO NOT DOWNLOAD AND RUN FILES ATTACHED TO EMAIL!**

Yes, I know, your best friend just sent you this game and he would never send you a Trojan file.
Well...these Trojans use the victims address book to send email out to their friends. Your friend will not know he sent it to you. Contact the source of any file and then use your best judgment before running it. It is totally up to you!!!

Just because you use a virus checker that's up to date (it is isn't it?) Don't assume everyone's is.