TheV-Files: A dictionary of file threats

Paul Ducklin, Head of Research, Sophos Plc, Oxford, England

First published: May 1999

SUMMARY

This White Paper is an alphabetical lexicon containing descriptions of file types, formats, and virus information. Its purpose is to offer information about the types of files that can be infected by particular viruses. It also contains tips on how you can better protect your computer.

Important Note

Deciding that a file cannot contain a virus purely on the basis of its extension is impossible, because a file's type is determined by what it contains, not by what it is called. So, if you renamed an infected program called DODGY.EXE to PERFECT.BMP (see BMP), it would still contain a virus. It would not actually be a BMP file, but it would look like one to the casual observer.

Just because the entry under BMP says "BMPs are not programs and cannot be infected with a virus", it does not mean that it is routinely safe to double-click on email attachments that appear to be BMP files.

ASCII
(American Standard Code for Information Interchange)

Basic ASCII allows only 7 bits per character (128 characters), and the first 32 characters are unprintable (they issue commands such as Line Feed, Form Feed and Bell). Generally, ASCII files are text files. However, with a little effort, it is possible to write programs that consist only of printable characters (see *EICAR*). Also, Windows batch (BAT) files and Visual Basic Script (see *VBS*) files are typically pure text, and yet are programs. So it is possible for ASCII files to contain program code, and thus to contain viruses.

When sending out emails, especially those intended for a wide audience, using simple ASCII text to get your message across is the best choice. A pure-text email lets you control both content and layout exactly, and ensures that your mail will be legible by users of even the most old-fashioned email programs.

BMP
(Bitmap file)

A bitmap is a grid of coloured dots (pixels) which combine to make an image. BMP files record such images for display on a computer screen. Unlike other bitmap storage formats (see *JPEG*), BMP files are fairly primitive, and make only a modest attempt at compression. This means that large bitmaps tend to result in large BMP files. Nevertheless, BMP files are common on Windows systems because BMP is one of the standard Windows image formats. BMPs are not programs and cannot be infected with a virus.

CGI
(Common Gateway Interface)

CGI scripts are commonly used on Web sites to achieve customised results. Generally, when the visitor performs some action, such as filling in a form or clicking on a link, the server executes a script using information input by the visitor. This allows the appearance or behaviour of the Web site to be customised for that visitor.

Of course, this means that the server is executing a program at the request of an outsider, using input provided by that outsider. Since many programs behave incorrectly when presented with illegal or invalid input, it may be possible for an attacker to "feed" a CGI script with input that will cause it to misbehave in such a way that the attacker can hack the site.

It may be possible for an attacker to “feed” a CGI script with input that will cause it to misbehave in such a way that the attacker can hack the site.

Additionally, some CGI scripts record the information input by the visitor (for example, scripts to allow on-line shopping may record the contents of the current visitor’s virtual shopping basket) in temporary files. If the scripts are incorrectly configured by the administrator, these files may be written in amongst the data files making up the Web site itself, from where an informed attacker might be able to retrieve them later using a Web browser.

CLP
(Clipboard file)

Windows has a virtual clipboard which transparently saves anything you cut (Ctrl-X) or copy (Ctrl-C) from one application until you Paste (Ctrl-V) it into another. The clipboard contains one object at a time, but may store many different representations of the object. Sometimes, the clipboard will not contain the object itself, but a reference to it. If you copy an EXE file to the clipboard from Explorer, for instance, the clipboard remembers the name and location of the file, not the file itself. The contents of the clipboard can be saved to disk as a CLP file.

So although CLP files may contain viruses or virus fragments that have been copied from another application, they cannot themselves be infected.

DOC
(Document file)

Microsoft Word document files usually contain just document data. However, they may also contain programs (called macros) written in a high-level programming language that is part of Word itself. There are various versions of this macro language, including *Word Basic* in Word 95, *Visual Basic for Applications 5* (VBA5) in Word 97, and *Visual Basic for Applications 6* in Word 2000. All of these languages are designed to be easy to learn, and all are powerful enough to be used to write viruses.

DOC files can contain viruses, so it is better to avoid sending information using this file type.

This means that when someone sends you a DOC file by email, it may be more than just a data file. It may also contain an embedded macro program which will automatically be fired up when you double-click on the DOC attachment in the email. DOC files are commonly exchanged, and this has allowed Word viruses to become extremely common. Seven out of ten viruses in the March 1999 Sophos Top Ten were able to infect DOC files.

Anti-virus software can stop you accidentally opening infected DOC attachments sent by email, and you should certainly use it for protection. However, it is also worth trying to avoid sending DOC files unless it is strictly necessary. Sometimes, people send out DOCs containing short messages that could more efficiently have been sent as simple text emails (see *ASCII*). At other times, they send out more complex documents, but still do not need all the bells and whistles offered by DOC files. In these cases, it would have been safer and more efficient to use Rich Text Format (see *RTF*).

EICAR
(The EICAR Standard Anti-Virus Test File)

This is a simple text file (see *ASCII*) that can also act as a program. It consists of one line of printable characters; if saved into a file called EICAR.COM, it can actually be executed. It prints the message:

EICAR-STANDARD-ANTIVIRUS-TEST-FILE!

Most anti-virus products detect this file as if it were a virus. This provides a safe and simple way of testing the installation and behaviour of your anti-virus software without needing to use a real virus. Using a real virus for testing on your corporate network is rather like setting fire to your wastepaper basket to test the smoke alarm — an unnecessary risk.

Using a real virus for testing purposes on your corporate network is rather like setting fire to your wastepaper basket to test the smoke alarm — an unnecessary risk.

To make your own EICAR test file, create a text file called EICAR.COM containing a single line that looks like this:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

Note that the "O" in the third character position is the letter "oh", not the digit "zero". If you have typed (or pasted) the text correctly, Sophos Anti-Virus will tell you the file contains "EICAR-AV-Test".

EXE
(Executable file)

EXE files contain programs that you can run directly. Usually, you do this by double-clicking on the program's icon, by clicking on a shortcut on the desktop or start menu, or by entering the name of the program at a command prompt. Programs can also be executed from other programs, or by scripts such as batch files or Visual Basic Script files (see *VBS*). Files with the extension COM are also directly executable under Windows.

According to April 1999 virus statistics, the virus figures show that 80% of known viruses infect program files, yet they are responsible for less than 15% of viruses ' in-the-wild'.

Since programs are designed to be executed and to take control of the computer, it comes as no surprise to find that the vast majority of known viruses infect program files. However, real-world infections (known as "in-the-wild" infections) by program-infecting viruses are much less common. Only two of the viruses in the March 1999 Sophos Top Ten list were EXE infectors.

This is probably because people exchange programs far less frequently than they exchange document files (see *DOC*) and spreadsheets (see *XLS*), so that infected programs are relatively less likely to be passed from computer to computer.

However, experience suggests that people are easily persuaded to execute unknown programs if they are sent EXEs by email. You are advised to reject unsolicited programs (see *Trojan*) even if you seem to know the source, because it is rarely necessary to accept them.

FAX
(Fax transmission files)

Generally speaking, fax data files contain a bitmap image of the contents of a fax. The contents will have been generated by scanning a printed document (conventional fax machines consist of an integrated scanner, modem and printer, in order to acquire, transmit and display transmitted images) or by a computer program designed to build fax-format images from computer files such as Word documents.

When a Word document is sent by fax, only an image of what the document would look like if printed out is produced, so program macros (see *DOC*) do not get sent. This means you cannot get a Word macro virus in your fax machine.

Today, the biggest risk posed to company fax machines is probably that of unsolicited faxes, which waste company resources. Some unsolicited faxes offer prizes (usually of modest value) which you can win by entering a draw. This involves marking your answers on the fax and re-faxing it to a premium-line number. In the UK, you may be paying £1 per minute to make the call, which may last up to nine minutes.

GOODTIMES
(Virus hoaxes)

Often, pseudo-technical "information" is included to make the hoax more believeable.

Sometimes, non-viruses can cause as much trouble as viruses. Numerous email virus hoaxes exist in which alleged new viruses are described. Readers are warned that these "viruses" are extremely dangerous, and are urged to pass on the warning to as many of their friends as possible. Often, pseudo-technical "information" is included to make the hoax more believable. Bogus "comments" supposedly from software companies and anti-virus vendors are sometimes added, usually suggesting that the new "threat" is undetectable, unremovable, or both.

The result is a flurry of unnecessary email. Even if you receive an email which provides accurate information about a genuine new virus threat, you should resist the temptation to forward it to as many people as possible. This creates an Internet chain letter, which does little more than waste bandwidth.

Most companies would prefer that new threats be reported via the corporate intranet, or via a single company-wide email sent by the security administrator. If each person in the company were suddenly to mail everyone else with an "urgent virus alert" (whether hoax or genuine), the email overload could be disastrous.

HTML
(Hypertext Mark-Up Language)

This is the "language" of the World Wide Web, used to define the look and behaviour of Web sites. HTML itself is a descriptive language, not a programming language, but HTML files can be extended by embedding programs inside them. These programs are usually written in JavaScript, Visual Basic Script (see *VBS*) or Java. When an HTML file containing this sort of embedded program is downloaded, the program is automatically executed on the local computer.

In most cases, this sounds worse than it actually is, because embedded programs downloaded from remote Web sites are usually executed by your browser with extremely limited powers. By default, for example, Java programs from remote sites are unable to manipulate system configuration information, and are prevented from writing to the local hard disk. A similar sort of security restriction applies to VBS programs. This means that Java and VBS viruses cannot, in general, spread via Web site access.

Of course, the above remarks do not always apply. By relaxing the security settings (the details of which depend on both operating system and browser), it is possible to create an environment in which both VBS-based and Java-based viruses could spread automatically from a Web site to your computer. Over time, you may find that you need to adjust security settings on your computer in order to get the most from the sites you use frequently on the Web. Before making such adjustments, be sure that you understand the risks associated with them.

IDE
(Identity file)

Sophos customers are entitled to subscribe free of charge to an automatic alerting service which advises of new IDE files by email. This helps you keep as protected as possible.

These are add-on files for Sophos Anti-Virus which allow the product to be updated quickly to detect and disinfect new viruses. They are usually downloaded via the Web or distributed by email, but because IDE files are typically very small (tens or hundreds of bytes), and consist only of ASCII hexadecimal characters, they can even be distributed by fax and typed in by the recipient, for remote users who are stuck without network access.

JPEG
(Joint Photographic Experts Group file)

These files (pronounced "jay-peg") are image bitmaps (see *BMP*). They typically offer excellent compression and are thus popular on the Web, as they are quick to download.

Because high compression is achieved by reducing the quality of the image, JPEG files sometimes show unnatural-looking effects in parts of the image. These side-effects do not generally reduce the usability of the picture, especially on the Web, and are regarded as a satisfactory trade-off of file size against image quality. JPEG files are not programs, and cannot be infected with a virus.

However, a hoax (in numerous guises) exists which warns you of viruses which infect JPEG files. The hoax asks you to look out for defects in image quality, which are said to be symptomatic of infection. Of course, the defects described are those that are common in JPEGs, but since you are unlikely to notice them until they are pointed out, the hoax appears to be credible, and you may believe you are "infected". You are not.

KEY FILE

Some encryption programs store your encryption keys in a file where they can be conveniently accessed. Usually, the keys are themselves strongly encrypted — this means that you need to enter a pass-phrase to begin using the key file, but you do not then need to enter each key as it is used. This helps ensure that if your key file is stolen, it will be of limited use to the attacker.

Storing your encryption files on a floppy disk will better insure against potential problems, provided you do *not* store the keyfile unencrypted.

Even so, you are advised not to store key files on your hard disk because of the risk of compromise. Store them on a removable floppy disk if you can. That way there is less to go wrong. Be aware, also, that some key files are stored unencrypted (see *PWL*). You are advised to avoid such files at all costs.

Recently, a virus appeared (WM97/Caligula) which can find your PGP secret keyring (if you have PGP installed) and send it via FTP, behind your back, to a virus writers' Web site. The virus styles itself "an exercise in espionage-enabled viruses", and serves as a reminder that anything that can be done in software can be done in a virus.

LIBRARY FILE

These are files containing groups of often-used computer code which can be shared amongst many programs. This has several advantages: programmers who use library code do not need to keep reinventing the wheel; programs which invoke library code do not each need to include a copy of that code, making their files smaller; updates to library code can be applied in one place, rather than in many programs. In Windows systems, the commonest form of library is the Dynamic Link Library (DLL).

There are certain disadvantages to DLLs, too. A bug in library code produces a bug in every program which uses that library. A single missing library file might prevent dozens of other programs from executing. A virus which infects a DLL automatically "infects" any program which uses that DLL.

One virus which does this is W32/Ska-Happy99, which infects the file WSOCK32.DLL, allowing the virus to intercept all future attempts to send email, regardless of the email software you are using. The virus then emails a copy of itself along with every email you send.

MP3
(Moving Picture Experts Group Audio Layer 3 file)

MP3 files contain compressed audio tracks. Like JPEG (see *JPEG*), the amount of compression can be increased by reducing the quality of the sound track when it is replayed. Because very high compression can be achieved without excessive loss in quality, MP3 audio is very popular on the Internet.

As with JPEG, MP3 files are not programs, and cannot be infected with a virus. A hoax exists about an MP3 'virus', in similar vein to the hoax about JPEG.

NORMAL.DOT
(Word global template)

Write-protecting your NORMAL.DOT file *does not* prevent virus infection.

For most users, the file NORMAL.DOT is the global template for Microsoft Word. Anything that you store in the global template effectively becomes a built-in part of your installation of Word. This is not the only way of adding features to Word, but it is the best-known and the most common.

NORMAL allows you to store all kinds of customisations, including keystroke shortcuts, text styles, toolbars and macros. Since Word macros are basically programs (see *DOC*), adding macros to NORMAL allows you to change the programmatic behaviour of Word altogether. In many ways, NORMAL is to Word as AUTOEXEC.BAT is to Windows. It contains macros that are always loaded when Word is started.

Write-protecting NORMAL may slow down the spread of a virus, because the virus is not automatically reloaded every time Word starts. But as a protective measure it is of very limited use.

This means that a virus which infects the global template is effectively "memory resident" inside Word, and will automatically be reloaded every time Word is started. Worse still, a virus does not have to write itself explicitly into the NORMAL file. All it needs to do is to go resident, thereby altering the global template. When Word exits, it will detect these changes, and automatically save them back into NORMAL. Although you can ask Word to prompt you about such changes (which could give warning of a virus infection), it takes only one line of program code to switch this warning off. Most viruses do this.

Some people still believe that write-protecting NORMAL prevents virus infection. This is false — it merely stops Word automatically updating (and infecting) NORMAL when you exit. As long as Word is loaded, any resident virus will remain resident and active. Write-protecting NORMAL may slow down the spread of a virus, because the virus is not automatically reloaded every time Word starts. But as a protective measure it is of very limited use.

OBJ
(Object file)

These are similar to library files (see *Library*), though they cannot be loaded dynamically when a program is run. Instead, they are created when a programmer is building a piece of software as an intermediate step between the source code (written in a language such as C or C++) and the finished program.

OBJ viruses do not have a ready supply of victims because most users do not have OBJ files on their computers—these files are used primarily by programmers.

Because most programs are constructed out of several source code files, the programmer usually runs a compiler, which converts each source file into an OBJ file, and then runs a linker, which gathers all the OBJ files together and builds them into a single program.

OBJ files are usually recreated many times whilst a program is under development, so they change frequently. This means a virus which could infect OBJs would be manipulating files that the programmer would expect to be changing, thus avoiding notice. And it would end up being linked into any program which used that particular infected OBJ. Like libraries, OBJs may be shared between multiple programs, so an OBJ virus might find its way into several programs having infected only one file on your disk.

OBJ viruses exist, but are uncommon. They find it hard to spread because most users are not programmers, and do not have OBJ files on their computer. This means that OBJ viruses do not have a ready supply of victims.

PWL
(Password List file)

When you log onto a network under Windows, you will usually see a dialog asking for your username and password. This dialog often also includes a check box offering to save your password for next time, so you do not need to enter it next time you log on.

You are advised not to do this, because it means that anyone who has access to your computer will be able to access the network as if they were you. Windows already knows the password that it would normally ask you to supply when you restart the computer, so they will not need to enter it.

Windows stores this information in a PWL file using a scrambling algorithm that makes the actual password invisible to a casual observer. But because Windows is able to unscramble the PWL file by itself, without any help from you, it follows that an attacker with a copy of your PWL file could unscramble the file, too.

This is another reason why PWL files should be regarded as insecure, and you should avoid asking Windows to "remember" your passwords. It is well worth the inconvenience of being asked for your password each time you log on.

QUARANTINE AREA

This is a term used by anti-virus programs to describe the holding area to which suspicious or infected files are moved so that they are unavailable to the user, but not lost for ever. This allows security-conscious organisations to remove infected files from general circulation without deleting them permanently. An administrator can then attempt to disinfect them under controlled circumstances, and make an informed decision about whether to return cleaned files to their original owner.

One benefit of allowing the administrator to decide whether files should be returned is that many macro viruses make deliberate and malicious changes to documents or spreadsheets they infect. This means that even after cleaning, files may contain damage, possibly subtle, which affects their validity or usefulness.

The virus XM/Compat, for example, which infects spreadsheets (see *XLS*), makes small and gradual changes to the contents of numeric cells in the file. Each time a file is opened, about 1% of numbers are adjusted up or down by up to 5%. In some environments, policy might deem it unacceptable to continue using files that have been damaged in this way: with quarantine, the administrator can act to enforce this policy.

One disadvantage of quarantine is that it can place a heavy burden on the administrator, particularly on a large server supporting many users. In the event of a significant virus outbreak, the administrator may end up with hundreds, even thousands, of documents to process. Furthermore, administrators may end up being called upon to vet the contents of documents that they would not ordinarily be authorised to read, which may contravene company policy.

RTF
(Rich Text Format file)

This is an alternative format to the DOC file (see *DOC*) which is supported by Microsoft Word. Files can be saved, with most of their formatting information intact, and then loaded back into Word as RTFs instead of DOCs.

RTF files are actually made up of ASCII text, with formatting commands embedded in them. For example, a word that appears in **boldface** would be marked in an RTF file using the characters `{\b boldface}`. RTF files cannot contain macros, so they cannot be infected with a macro virus.

By sending documents in RTF, you effectively do away with the possibility that you might transmit a virus by mistake.

This provides a useful way of communicating with people outside your company. By sending documents in RTF, you effectively do away with the possibility that you might transmit a virus by mistake. Your recipients will be able to read your file directly into Word, and even to convert it back to a DOC file if they wish. But if it is then found to be infected, you will know that the infection was introduced after it reached them.

Note that the process of converting from DOC to RTF is imperfect. Some formatting features that are possible in Word do not survive the journey from DOC to RTF and back. Before committing to using RTF for sending and receiving email attachments, you may need to experiment with the conversion of common company documents. This will soon reveal any potential layout problems. You may need to simplify some formatting tricks that you are accustomed to using, but you will almost always find there is a simpler way to achieve the same result.

There is an important caveat here — you cannot assume that a file really is in RTF simply because its has an RTF extension. There are some macro viruses which intercept the attempt to save a file as RTF and force it to be saved in DOC format, but with an RTF extension. If someone sends you such a file via email, and you double-click it, Word will attempt to load the file. Since Word recognises it as a DOC file, despite its name, it loads it as a DOC file and activates the virus.

Fortunately, it is easy to check for yourself that an RTF really is what it claims. Try looking at a DOC file and an RTF file using NOTEPAD. The RTF file will load as legible ASCII text, starting with `{\rtf`. The DOC file will load as binary gobbledygook. Although checking like this is inconvenient, it does let you make sure that things are as they seem, on those occasions when it really matters.

SCR
(Screen saver files)

These are special types of program file (see *EXE*). They cannot be executed directly, but can be automatically launched by Windows after a specified time of inactivity.

Because most Windows machines have numerous SCR files installed, and because the system executes them for you without awaiting an explicit instruction to do so, there are viruses which infect them. Popular screen savers are often exchanged via email or downloaded from the Web, often without the same level of caution that would be afforded to an EXE or COM file.

TROJAN
(Trojan Horse file)

Legend says that after a prolonged war between the Greeks and the Trojans, the Greeks finally surrendered, left behind a gift of truce, abandoned Troy and set off home. Their gift was a large wooden horse, which the Trojans accepted eagerly (despite the advice of their chief priest, who suspected a deception). The horse was larger than the city gates, which were duly demolished. The statue was wheeled in and the party commenced.

In fact, the Greeks had merely sailed out of sight to await nightfall. Also, a secret compartment inside the horse contained a select band of Greek fighters, who duly broke out under cover of darkness to initiate the slaughter. Their countrymen sailed back, piled in through the breached defences and completed the rout. Troy was lost.

Do not open unexpected attachments, even if they are from a trusted person. You can usually get the programs you need from your administrator instead of your friends, and you can ask to receive documents in RTF (see *RTF*) instead of accepting DOCs.

And that is why it is generally a bad idea to run a program, look at a document or use a spreadsheet that someone has sent you, especially if you do not know that person, or if you were not expecting them to send it to you. If it comes from an untrusted person, then it has untrusted content, whatever words of comfort they may offer you about it. Listen to the chief priest of the Trojans. Discard it.

Even if it seems to come from someone you trust, do not use it if you were not expecting it. There are viruses (see *Library file*) which send email attachments as if they were you, thus lulling recipients into a false sense of security. Don't feel bad about refusing files with programmatic content from your friends and colleagues. You can usually get the programs you need from your administrator instead of your friends, and you can ask to receive documents in RTF (see *RTF*) instead of accepting DOCs.

UUE
(UUENCODEd file)

UUEENCODE (UUE), XXENCODE (XXE) and MIME64 (also known as BASE64) are all encoding schemes which allow binary files to be converted into simple ASCII files (see *ASCII*) for transmission via email. Since text files generally pass unmolested from one mail system to another, this provides a reliable way of sending binary attachments in email. Once received, a decoding program converts the file back from its ASCII form into pure binary, thus completing the delivery of the attachment.

Always understand the "full' implications when you change your computer's security settings.

Most email programs automatically recognise the presence of encoded files inside an email, and present the user with an icon which can be clicked to detach or launch the attachment. “Launching” causes the attachment to be decoded, stored as a temporary file on the hard disk, and then deployed. DOC files (see *DOC*) are usually launched into Word, thus activating any virus they may contain. EXE files (see *EXE*) are launched directly, as programs.

Clearly, the convenience with which encoding and decoding is done in email software makes it very easy to send files to your friends and colleagues. Before doing so, always ask yourself if it is totally necessary. Sometimes, mail attachments (which embody an element of risk) are sent when a simple textual email (see *ASCII*) would do, saving both time and worry.

VBS
(Visual Basic Script file)

Visual Basic Script is a new programming language for Windows which builds upon the old-fashioned batch (BAT) language. Unlike BAT files, which are clumsy and rather limited, VBS programs can be as powerful as any application. In fact, they can invoke any system function, and can also start up, use and shut down other applications, such as Word, silently and invisibly.

VBS programs can also be embedded in HTML files (see *HTML*) for providing active content on the World Wide Web. Whilst there are security controls in place to help prevent VBS programs triggered over the Web from gaining too much power over your machine, these controls can be adjusted in such a way that would make Web-borne VBS viruses possible.

This means that you should not make changes to your computer’s security settings without a full understanding of the implications. If you do not know the implications, ask your administrator.

XLS
(Excel Spreadsheet file)

All the observations which apply to Word documents files (see *DOC*) apply to Excel spreadsheets. Excel files may contain macros, thus turning XLS files from data into programs. As with DOC files, these macros automatically become part of the system when a file is loaded.

When the first Excel virus appeared, there was some doubt as to whether it would become widespread because the extent to which XLS files were exchanged between computers was unknown. In fact, this virus (XM/Laroux) has become so common that it was Number One in the March 1999 Sophos Top Ten.

ZIP
(ZIP archive file)

ZIP files contain collections of other files. Because they allow a number of files to be delivered in a single container, and because ZIP files are compressed to save disk space and download time, they are very popular on the Internet.

Unlike JPEG files (see *JPEG*) or MP3 (see *MP3*), ZIP files do not throw away any information when they perform their compression. Whilst this restricts the maximum amount of compression that can be achieved, it ensures that the original files can be restored when decompressing. Obviously, this is vital for files such as programs, which must be preserved exactly.

A ZIP file can contain viruses if any of the files that are packaged into it contain viruses. However, the archive itself is not directly dangerous, because any infected files inside it must be extracted

A ZIP file can contain viruses if any of the files that are packaged into it contain viruses. However, the archive itself is not directly dangerous, because any infected files inside it must be extracted before they can be used and therefore initiate infection.

The most effective way to handle ZIP files (and similar files such as RAR and GZIP) is to use an on-access anti-virus program. In Sophos Anti-Virus, this is the component called InterCheck. It monitors all files as they are created or used to ensure that they are virus-free. This means that ZIP files, which may contain a large assortment of files you may never use, are not treated as threatening until infected files are extracted from them. At this point, InterCheck reports the virus as it emerges from the ZIP archive (but before it can be launched), and prevents infection.

SOPHOS

Sophos Plc • The Pentagon • Abingdon • Oxfordshire • OX14 3YP • UK
Tel +44 01235 559933 • Fax +44 01235 559935

www.sophos.com