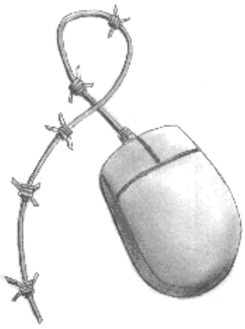
Participating With Safety Briefing no. 5

Computer Viruses



Written by Paul Mobbs for the
Association for Progressive Communications, March 2002.

This briefing is one of a series on Information Security. It looks at:

- What is a virus?
- How viruses work
- How viruses assimilate your computer
- Basic tips on protection against viruses
- Viruses and Linux

What is a virus?

A virus is an executable programme, a set of instructions that manipulate the functions of your computer's operating system. The early, simple computer viruses consisted of just two commands - firstly a check for a particular condition (be it the date or some other criteria) and then a call to the program that formats the computer's hard disk.

Many of the earlier viruses were transmitted from file-to-file on a computer as people shared files or floppy disks. Today the most common way to catch a virus is via the Internet. But instead of something simple, such as formatting your hard disk, Internet-borne viruses are far more complex. Many will read your email address book and forward themselves, when you next check your email, to all your friends.

'Virus' is actually a generic term for software that is harmful to your system. They spread via disks, or via a network, or via services such as email. Irrespective of how the virus travels, its purpose is to use or damage the resources of your computer. The first viruses were spread as part of computer programs, or by hiding in floppy disks. Most modern viruses are spread by Internet services, in particular email.

The problem with viruses is that the threat is often worse than the reality. For that reason a lot of people have made a lot of money out of hyping viruses and then selling the antidote. For example, many of the *X thousand viruses* that software companies talk about have never actually entered the real world. They are the result of laboratory tests of particular security problems on computer systems to see if a virus could work in that way. Having established that it could be a problem, they note the particular signature such a virus would have, and that's what the virus checker looks for.

The greatest effect of viruses tend not to be the destruction of data, but taking up people's time. For example, virus *hoaxes* spread by email tend to surface every now and again, usually under the title 'PEN PAL GREETINGS' or such like. In itself it is the ultimate virus because you consciously spread the panic every time you forward it to your friends. That's the thing about computers - a lot of people don't know how they work, so they are easily deceived.

Viruses are not a marginal issue. Some have talked of viruses as a means of checking for security flaws in computer networks and automatically fixing the flaws in the programs. More recently, the US Federal Bureau of Investigation (FBI) has been rumoured to be developing a virus called 'Magic Lantern' that can penetrate computer systems and, under certain conditions, send copies of encryption keys and security information back to the FBI. Therefore computer viruses are not just a threat to a system - they are also a more general security threat.

How viruses work

It is impossible to receive any type of virus in a plain text email message, or in most word processor files, compressed data files (such as PKZip/GZip), database or spreadsheet files - these are not executable programs. The only exception to this is where a file contains Visual Basic or other code as part of a user-defined algorithm or program, or embedded 'object code' that may be executed by the software application.

To make the virus resident in your system you have to actually execute the program. That means:

- You have to run a program from the Internet that is infected with a virus - the solution is to check them with a virus checker first.
- You have to run a program from a floppy disk infected with a virus - again, the solution is to scan the disk with a virus checker first.
- You have to open/run a file in another programming language (Basic, C, etc.) which has a virus written into it - the solution here is to not run any program you don't understand.
- You have to open and use a file in more advanced word processors or spreadsheets that contains 'object code' or user defined instructions called 'macros' - the simple solution here is to go into the application's set-up and select the 'disable macros' option.

File viruses, where program code transfers from one file to another, whilst a problem some years ago are now in decline. The great problem today are:

- 'macro-viruses', small sections of interpreted code, that are transported as part of emails; and
- worms and trashing programs, that are transported as attachments to emails.

Programs such as Microsoft Outlook are very insecure because they attempt to integrate email into the rest of the operating system. Whilst this is a very useful way of simplifying the operation of the computer for beginners, it is a serious security risk. Virus writers exploit this feature to instal their virus on your system. This feature cannot be turned off from Windows, although following the havoc caused by the 'I Love You' some companies developed software to block viruses exploiting the flaws in Microsoft Outlook.

When people try to read email which contains visual basic code they will, when people try to real emails, Outlook forces the system to interpret the code and in the process this activates the macro-virus.

Attachments are another problem. When people receive a screen saver or 'promotional program' they will often, because they are not aware of the risk, run the program. But the flaws in the Microsoft system mean that the vast majority of viruses are specific to Microsoft software, and so users of the Macintosh and Linux systems are relatively immune to virus problems.

Any message sent through commonly available email programs is either just plain text or an encoded plain text file. As such it can harbour no executable code, and most operating systems would reject a request to try and execute such a file. So you can't get a virus by reading an email, or exchanging/chopping the text of an email into another application.

The only danger is that you may unknowingly download a programme as part of an attachment to an email.

But if you keep your email attachment directory separate from your system files the program cannot be accidentally run unless you specifically request it to be.

How viruses assimilate your computer

Your greatest likelihood of contracting a virus today is from the Internet. The use of virus checkers in the computer industry has stopped the spread of most viruses via disks. But viruses exploit the way computers execute other types of programs or scripts as part of email or shared software.

There are four common sources of viruses via the Internet:

- **Computer programs** - you can ensure 99% safety by using an up-to-date virus checker to scan the program files before you run them. This of course does not protect you from trashing programs, and totally new viruses.
- **Java and other Internet/Word-Wide-Web scripts** - it is possible for computers to upload code to your computer as part of proprietary Internet software (e.g., closed server programs such as those used in computer banking, etc.). It is becoming increasingly common for web site to load Java scripts - short programs - into your WWW browser to execute sounds and animated graphics (but the available instructions in these are limited, so there's not much problem with this at the moment). You can limit the possible damage by turning off Java and other plug-ins on your Web browser. When a web server requests to upload, you browser will ask first before proceeding. Basically, you never say yes when inside a risky site.
- **Embedded code** - this is the object code, visual basic, C, Pascal, programs or scripts that are embedded in many modern word processor, spreadsheet, and database applications. As applications become more complex it is not possible for programmers to write code for every eventuality. To get around this small chunks of code are included in the files you save to perform special functions. User defined functions, particularly in word processor, spreadsheet and database applications, are held as short text 'scripts'. It is possible to include instructions in scripts and certainly in object code which could act as a virus, Trojan or trashing program - damaging your system at a pre-determined time. Most applications allow you to open a file without activating the macros if you first enable the particular option in the program's set up menu. Of course the way around such problems is to only accept files in older formats that do not contain these features, or only receive files from trusted sources.
- **Source code** - programs are written as a set of instructions, which are then translated into machine instructions by an interpreter, or written as a program by a compiler. This is something that is more commonly done on Linux systems since many programs are distributed as a source code, which you then compile to work with the configuration of your own system. There are also many programs available on the Internet in Basic, Visual Basic, C, Pascal, etc. In large programs, particularly where the user doesn't know much about the language, or where the program is poorly structured, it is very easy to hide a trashing command, Trojan or virus. You should not compile/execute any source file unless you know it is safe. The source code - usually a text file - is completely harmless, even when included in emails/attachments. It's only when you load the source code into a compiler or interpreter that it becomes dangerous.

The practical meaning of the above is that you can't catch a virus from a plain text file, or a standard plain text HTML file, or an FTP/Gopher/Telnet connection. The main danger comes from WWW browsers - if the 'helpers' are set to execute programs such as '.EXE' or '.BAT' files when they are loaded, you will be unable to prevent loading a virus.

How you deal with viruses is also dependent upon your role. This briefing deals with the individual computer user. For users who are part of local networks there are different issues related to networked systems. For example, it is important to prevent a virus accessing one part of the network; therefore the use of floppy disk on networked computers might be restricted. Those who run email servers also have a role to play. Servers can have anti-virus software running with the email server, preventing the transmission of attachments that are known to contain viruses. Internet users should ask if their service provider is blocking viruses at the server, and to install this feature if they are not.

Basic tips on protection against viruses

There are three very simple tips for significantly reducing the risks of having problems with viruses:

- Be cautious when using Internet services -
  - don't click on attachments,
  - turn off macros in Word,
  - turn off Javascript,
  - configure the web browser not to run programs,
  - if possible, don't use Microsoft Outlook (Microsoft Outlook is the least secure of the commonly used email programs);
- If you use Microsoft Outlook get the latest version, or a patch of existing versions, and configure it not to run attachments or programs;
- Use some sort of virus checking software to scan any files that arrive as attachments, or that you receive on disk.

If you have a little more knowledge on the use of computers, the following may be helpful:

- Configure your operating system so that you can see the filename extension - this will allow you to see what type of file it is and identify executable from non-executable files. You should also beware of files that have a double extension, such as 'picture.jpeg.vb'.
- Don't execute any program you receive on floppy disks, or over the Internet, without first scanning it for viruses or checking what instructions the code contains. That includes executable ('.exe'/'.com') files, screen savers ('.scr'), executable ('.exe.) PKZIP and other archive files, batch ('.bat') files, Visual Basic or script files such as VBScript ('.vbs'/'.bas') and any programs interpreted/compiled from source code files.
- Make sure the 'helpers' or 'settings' part of your Web browser has the switches for '.exe', '.bat', '.doc', '.vbs' etc. (basically, all the file extensions involving potentially infected executable code) set to 'Ask User' (or the equivalent on your browser). Never let your browser automatically execute any program! Set all Java and other plug-in options to 'off' or 'ask'. This can make using the web a little more time consuming, but safer.
- Make sure that the 'boot sector protection' in your BIOS system set-up is turned on to prevent the boot sectors of disks being overwritten if an older-style boot virus installs itself.
- Make sure that the 'boot order' switch in your system set-up is set to 'C: only' (or C: A:' if 'C only' is not permitted) - that way if you turn on with a floppy in the drive it won't execute the boot sector program on the floppy and potentially infect your system.
- Make sure that the attachments downloaded with email are stored in a dedicated directory, and that there is no 'path' statement pointing to that directory (the 'path' statement in the 'autoexec.bat' file informs your system which directories to look in if a requested program cannot be found in the current working directory - it usually says 'path' or 'set path'). The simplest option is to create your own directory, and then make your email program point to it.
- The most effective and simple means of virus protection is a regular full system scan about every few weeks, or following the downloading of a number of programs (that's where the virus software checks every executable file and object code file on your system). Using 'checksums' (that's where

the number in a file are added up and the result stored to see if one part has been changed) is very effective, but it's not foolproof, and it's really annoying when you recheck because it will flag up many files that have been innocently changed.

- Don't run programs from unverified sources - even if they do check out with a virus scanner. It is very easy to insert a rogue instruction into a program to trash your system and these will not be picked up by a virus scanner.
- Always keep a backup system/boot up disk with virus software installed on it - that way if the system is infected you can boot from the floppy without activating the virus on the hard disk and then clean the system.
- Clean out your system regularly using Scandisk - it cleans up any stray data from your disks, truncated files, etc. Also, keep an eye out for undeleted temporary ('.tmp') files in your system. Virus protection is all about good system management, but it is easier to clean an infected system of viruses if there are no rubbish files stored on your system.

Linux and viruses

Linux systems are far less susceptible to viruses because of the partitioning of the system, and the controls over the installation of software. But because many Linux users share and distributed programs over the 'Net, it is possible that someone could distribute a trashing program. However, the likelihood that such as program would do any significant damage to the system, except to the user who ran it, means that the system would not suffer fatal damage unless the program exploited a security flaw in the operating system.

Free Documentation License:

For more information about the Participating With Safety project, or if you have questions about the briefings, contact secdocs@apc.org