8.2 Virus Scanners

The most obvious defence against viruses is the virus scanner. A virus scanner is essentially a software that tries to prevent a virus from infecting your system. It usually scans incoming e-mail and other incoming traffic. Most virus scanners also have the ability to scan portable media devices such as USB drives.

In general, virus scanners work in two ways. The first method is that they contain a list of all known virus files. Generally, one of the services that vendors of virus scanners provide is a periodic update of this file. This list is typically in a small file, often called a .dat file (short for data). When you update your virus definitions, what actually occurs is that your current file is replaced by a more recent one on the vendor’s website.

The antivirus program then scans your PC, network, and incoming e-mail for known virus files. Any file on your PC or attached to an e-mail is compared to the virus definition file to see whether there are any matches. With e-mail, this can be done by looking for specific subject lines and content. Known virus files often have specific phrases on the subject line and on the body of the messages they are attached to. Yet viruses and worms can have a multitude of headers, some of which are very common, such as re:hello or re:thanks.

Scanning against a list of known viruses alone would result in many false positives. Therefore, the virus scanner also looks at attachments to see whether they have a certain size and creation date that matches a known virus or whether it contains known viral code. The file size, creation date, and location are the tell-tale signs of a virus. Depending on the settings of your virus scanner, you may be prompted to take some action, the file may be moved to a quarantined folder, or the file may simply be deleted outright. This type of virus scanning works only if the .dat file for the virus scanner is updated, and only for known viruses.

Another way a virus scanner can work is by monitoring your system for certain types of behaviour that are typical of a virus. This might include programs that attempt to write to a hard drive’s boot sector, change system files, alter the system registry, automate e-mail software, or self-multiply. Another technique virus scanners often use is searching for files that stay in memory after they have executed.

This is called a Terminate and Stay Resident (TSR) program. This can be performed by a number of legitimate programs, however, more often than not is a sign of a virus.

Many virus scanners have begun employing additional methods to detect viruses. Such methods include scanning system files and then monitoring any program that attempts to modify those files. This means the virus scanner must first identify specific files that are critical to the system. The registry, the boot.ini, and possibly other files are included within a Windows system. Then, if any program attempts to alter these files, the user is warned. Therefore the procedure cannot be proceeded unless authorization is given.

It is also important to differentiate between on-demand virus scanning and ongoing scanners. An ongoing virus scanner runs in the background and is constantly checking a PC for any sign of a virus. On-demand scanners run only when you launch them. Most modern antivirus scanners offer both options.

8.2.1 Email and Attachment Scanning

Since the primary propagation method for a virus is e-mail, e-mail and attachment scanning is the most important function of any virus scanner. Some virus scanners actually examine your e-mail on the e-mail server before downloading it to your machine. Other virus scanners work by scanning your e-mail and attachments on your computer before passing it to your e-mail program. In either case, the e-mail and its attachments should be scanned prior having any chance to open it and release the virus on your system. This is a critical difference. If the virus is first brought to your machine, and then scanned, there is a chance, however small, that the virus will still be able to infect your machine. Most commercial network virus scanners will scan the e-mail on the server before sending it on to the workstations.

8.2.2 Download Scanning

Anytime you download anything from the Internet, either via a web link or with an FTP program, there is a chance you might download an infected file. Download scanning works much like e-mail and attachment scanning, but does so on files you select for downloading.

8.2.3 File Scanning

Download and e-mail scanning will only protect your system against viruses that you might get downloading from a site, or that come to you in e-mail. Those methods will not help with viruses that are copied over a network, deposited on a shared drive, or that are already on your machine before you install the virus scanner.

This is the type of scanning in which files on your system are checked to see whether they match any known virus. This sort of scanning is generally done on an on-demand basis instead of an ongoing basis. It is a good idea to schedule your virus scanner to do a complete scan of the system periodically. I personally recommend a weekly scan, preferably at a time when no one is likely to be using the computer.

It does take time and resources to scan all the files on a computer's hard drive for infections. This type of scanning uses a method similar to e-mail and download scanning. It looks for known virus signatures. Therefore, this method is limited to finding viruses that are already known and will not find new viruses.

8.2.4 Heuristic Scanning

This is perhaps the most advanced form of virus scanning. This sort of scanning uses rules to determine whether a file or program is behaving like a virus, and is one of the best ways to find a virus that is not a known virus. A new virus will not be on any virus definition list, so you must examine its behaviour to determine whether it is a virus. However, this process is not fool proof. Some actual virus infections will be missed, and some non-virus files might be suspected of being a virus.

The unfortunate side effect of heuristic scanning is that it can easily lead to false positives. This means that it might identify a file as a virus, when in fact it is not. Most virus scanners do not simply delete viruses. They put them in a quarantined area, where you can manually examine them to determine whether you should delete the file or restore it to its original location. Examining the quarantined files rather than simply deleting them all is important because some can be false positives. In this author's personal experience, false positives are relatively rare with most modern virus scanners.

As the methods for heuristic scanning become more accurate, it is likely that more virus scanners will employ this method, and will rely on it more heavily. Such algorithms are constantly being improved. One area of research now is adding machine learning to antivirus algorithms.

8.2.5 Active Code Scanning

Modern websites frequently embed active codes, such as Java applets and ActiveX. These technologies can provide some stunning visual effects to any website. However, they can also be vehicles for malicious code. Scanning such objects before they are downloaded to your computer is an essential feature in any quality virus scanner.

8.2.6 Instant Messaging Scanning

Instant message scanning is a relatively new feature of virus scanners. Virus scanners which use this technique scan instant messaging communications looking for signatures of known viruses or Trojan horse files. In recent years the use of instant messaging has increased dramatically. It is now frequently used for both business and recreational purposes. This growing popularity makes virus scanning for instant messaging vital. If your antivirus scanner does not scan instant messaging, then you should either avoid instant messaging or select a different antivirus package.

Most commercial virus scanners use a multi-modal approach to scanning. They employ a combination of most, if not all, of the methods we have discussed here. Any scanner that does not employ most of these methods will have very little value as a security barrier for your system.