How to know what computer files threaten you

Copyright 2016 by Richard Schenkar

One of the continuing frustrations we all face in the continuing din of warnings and threats of computer invasion is the powerlessness we feel every time there is a warning or threat.

The good news is that by knowing what to look for in the file stream cascading through your practice, you can guess, with reasonable certainty, what files could cause you problems. You can then isolate them, test them on other computers not connected to your network, or examine them independently to satisfy yourself that they are problem-free.

What you look for are executable programs that can launch themselves or that use other programs already on your system to launch themselves and do damage. In most cases, you can tell the suspect programs by looking at the file extension-- the three-character series to the right of the dot in the filename. The bad news is that there are over 1600 file extensions in use. The good news is that you have to worry about only eight.

The eight you have to worry about will be described here. There are two major archives online that you can use to decode the rest. The website at extsearch.com provides you with a list of about 250 file extensions.

Watch for These File Extensions

These are the file extensions that you should note. Do not get paranoid or assume that every file with these extensions deserves exorcism. Perfectly good programs are distributed with these file extensions every day with no problems. Those suspect file extensions include, but are not limited to, the following: .*vbs* (Visual Basic Script); .*asp* (Active Server Pages); *.bat* (BATch file); *.com* (COMmand file); *.exe* (EXEcutable program file); *.html* or *.htm* (Hypertext Markup Language); *.js* (JavaScript); and *.pl* (PERL Script (Practical Extraction and Report Language).

Visual Basic Script (.vbs) files are used in many web sites to accomplish many tasks and effects automatically. Because they are versatile and are accepted without question by many browsers, it is easy to slip destructive code into them. Some browsers allow you to block visual basic script files or make a decision on which ones you will accept. If you have an option, make sure you find it, understand it, and exercise it.

Active Server Pages (.asp) are hypertext markup language files with scripts in them that run on servers, rather than on client computers. Here, we should note that "server" computers are often larger computers that do heavy tasks like data housing and searching; "client" computers are generally the computers we see and work on daily. If you have a server in your office, you should watch for active server pages. This is Microsoft technology and is part of its Internet Information Server. These files may also run on the Microsoft Personal Web Server.

Batch files (.bat) are lists of commands that call up programs for execution one after the other. They are often used to automate tasks and introduce efficiencies. They are particularly accessible to most of us because they use programs that are already on your computer and integrate those programs helpfully. That is what makes them insidious. Since they are always text files, you should examine each line of the batch file to understand precisely what the command on that line will do to your system before you release it.

Command files (.com) are executable programs. You probably will not be able to inspect or back-engineer them (unless you write them yourself and compile them using computer programming languages and compilers). The best you can reasonably do is to get them from reliable sources and know what they are supposed to do. A good practice is to try them on a computer that is not going to ruin your practice if it crashes. (That is a good reason to keep an old computer around the office. You can get used computers from salvage agencies and some stores that specialize in recycled computers. But know what you are getting and be ready to fix it if you must.)

Executable program files (.exe) have the same properties and should be handled with the same cautions as command files.

Hypertext markup language files (.html or .htm) are interpreted by web browsers to create images, text, and other features on your screen. Even though they are written in ASCII (American Standard Code for Information Interchange) which is plain text, they can include scripts where destructive code can hide. Inspect the file with a word-processor in non-document or programming mode or check it out on that old computer mentioned above.

Javascript files (.js) and **Practical Extraction and Report Language (PERL) Script files (.pl)** are interpreted by web browsers to accomplish various tasks. Be sure you know what they do and why they are on your system.