What are parasite or Rogue Software?

They are unsolicited commercial software also known as PUPS (Possibly Unwanted Programs) — that is, a program that gets installed on your computer which you never asked for, and which does something you probably don't want it to, for someone else's profit.

The parasite problem has grown enormously recently, and many millions of computers are affected. These PUPS can typically:

- plague you with unwanted advertising ('adware');
- watch everything you do on-line and send information back to marketing companies ('spyware' or 'Tracking Cookies);
- add advertising links to web pages, for which the author does not get paid, and redirect the payments from affiliate-fee schemes to the makers of the software;
- set browser home page and search settings to point to the makers' sites (generally loaded with advertising), and prevent you changing it back ('homepage hijackers');
- leave security holes allowing the makers of the software — or, in particularly bad cases, anyone at all — to download and run software on your machine;
- degrade system performance and cause errors thanks to being badly-written;
- provide no uninstall feature, and put its code in unexpected and hidden places to make it difficult to remove.

Where do they come from?

There are three major ways unsolicited commercial software can make its way on to your machine:

- Some freeware programs are 'bundled' with parasites, which are installed at the same time. The Peer to Peer file-sharing programs are notorious for this. Beware of software that allows you to download copywritten media. They are not well protected and something that looks like a program or music file or video clip can run scripts that install rogue software on you computer.

- Many parasites load using ActiveX installation option. When a web page includes a link to an ActiveX program, a window will appear asking the user if they wish to execute it. If 'Yes' is clicked (or if security settings are set lower than normal so that it never even asks), the software is allowed to run and can do anything at all it likes on your computer, including installing parasites.

  For this reason, you should *never* click 'Yes' to a "Do you wish to download and install..." prompt unless you are 100% sure you trust the publisher of the software, which might not be the publisher of the web site you are viewed — read the dialogue box very carefully.

  Sometimes sites (or pop-up ads) try to fool you into clicking 'Yes' by stating that the software is necessary to view the site, or opening endless error windows if you click 'No', or claiming that the digital certificate on the code means it is safe.

- Some of the really sleazy parasites, particularly homepage-hijackers and diallers, execute by exploiting security holes. Ways of getting code to run that are not supposed to be possible, but are due to mistakes in the browser code.

  You can do your best to guard against this by ensuring you have the latest updates and patches from Microsoft. Still, there are usually a handful of security holes that have not yet been corrected, so you can never be 100% sure you are safe.

Why doesn't my anti-virus software detect this?

Technically, most unsolicited commercial software isn't viral: it doesn't spread from computer to computer, it just installs and runs on one system.

That doesn't mean it's not harmful, but anti-virus software does not attempt to detect all software that could be harmful. Whether it *should* is a tricky argument that ends up a question of where you draw the line.

Actually some anti-virus programs do detect *some* of the parasites outlined on these pages, but not nearly all, and not all versions of them and the selection of targets seems for the most part to be pretty arbitrary.