

Malware

Full article: <http://en.wikipedia.org/wiki/Malware>

Malware is software designed to infiltrate or damage a computer system without the owner's informed consent. The term is a portmanteau of the words *malicious* and *software*. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

Many normal computer users are however still unfamiliar with the term, and most never use it. Instead, "computer virus" is incorrectly used in common parlance and even in the media to describe all kinds of malware, though not all malware are viruses.

Software is considered malware based on the perceived intent of the creator rather than any particular features. Malware includes computer viruses, worms, trojan horses, most rootkits, spyware, dishonest adware, and other malicious and unwanted software. In law, malware is sometimes known as a computer contaminant, for instance in the legal codes of California, West Virginia, and several other American states.

Malware should not be confused with defective software, that is, software which has a legitimate purpose but contains harmful bugs.

Of all computer code released today the majority may be malicious. Preliminary results from Symantec sensors published in 2008 suggested that "the release rate of malicious code and other unwanted programs may be exceeding that of legitimate software applications." According to F-Secure, "As much malware was produced in 2007 as in the previous 20 years altogether." Malware's most common pathway from criminals to users is through the Internet, by email and the World Wide Web.

Purposes

Many early infectious programs, including the first Internet Worm and a number of MS-DOS viruses, were written as experiments or pranks generally intended to be harmless or merely annoying rather than to cause serious damage to computers. Young programmers learning about viruses and the techniques used to write them only to prove that they could or to see how far it could spread. As late as 1999, widespread viruses such as the Melissa virus appear to have been written chiefly as pranks.

A slightly more hostile intent can be found in programs designed to vandalize or cause data loss. Many DOS viruses, and the Windows ExploreZip worm, were designed to destroy files on a hard disk, or to corrupt the filesystem by writing junk data. Network-borne worms such as the 2001 Code Red worm or the Ramen worm fall into the same category. Designed to vandalize web pages, these worms may seem like the online equivalent to graffiti tagging, with the author's alias or affinity group appearing everywhere the worm goes.

However, since the rise of widespread broadband Internet access, more malicious software has been designed for a profit motive. For instance, since 2003, the majority of widespread viruses and worms have been designed to take control of users' computers for black-market exploitation. Infected "zombie computers" are used to send email spam, to host contraband data such as child pornography, or to engage in distributed denial-of-service attacks as a form of extortion.

Another strictly for-profit category of malware has emerged in spyware -- programs designed to monitor users' web browsing, display unsolicited advertisements, or redirect affiliate marketing revenues to the spyware creator. Spyware programs do not spread like viruses; they are generally installed by exploiting security holes or are packaged with user-installed software, such as peer-to-peer applications.

Infectious malware: viruses and worms

Main articles: Computer virus (http://en.wikipedia.org/wiki/Computer_virus) and Computer worm ([../wiki/Computer_worm](http://en.wikipedia.org/wiki/Computer_worm))

The best-known types of malware, viruses and worms, are known for the manner in which they spread, rather than any other particular behavior. The term computer virus is used for a program which has infected some executable software and which causes that software, when run, to spread the virus to other executable software. Viruses may also contain a payload which performs other actions, often malicious. A worm, on the other hand, is a program which actively transmits itself over a network to infect other computers. It too may carry a payload.

These definitions lead to the observation that a virus requires user intervention to spread, whereas a worm spreads automatically. Using this distinction, infections transmitted by email or Microsoft Word documents, which rely on the recipient opening a file or email to infect the system, would be classified as viruses rather than worms.

Some writers in the trade and popular press appear to misunderstand this distinction, and use the terms interchangeably.

Capsule history of viruses and worms

Before Internet access became widespread, viruses spread on personal computers by infecting programs or the executable boot sectors of floppy disks. By inserting a copy of itself into the machine code instructions in these executables, a virus causes itself to be run whenever the program is run or the disk is booted. Early computer viruses were written for the Apple II and Macintosh, but they became more widespread with the dominance of the IBM PC and MS-DOS system. Executable-infecting viruses are dependent on users exchanging software or boot floppies, so they spread heavily in computer hobbyist circles.

The first worms, network-borne infectious programs, originated not on personal computers, but on multitasking Unix systems. The first well-known worm was the Internet Worm of 1988, which infected SunOS and VAX BSD systems. Unlike a virus, this worm did not insert itself into other programs. Instead, it exploited security holes in network server programs and started itself running as a separate process. This same behavior is used by today's worms as well.

With the rise of the Microsoft Windows platform in the 1990s, and the flexible macro systems of its applications, it became possible to write infectious code in the macro language of Microsoft Word and similar programs. These macro viruses infect documents and templates rather than applications, but rely on the fact that macros in a Word document are a form of executable code.

Today, worms are most commonly written for the Windows OS, although a small number are also written for Linux and Unix systems. Worms today work in the same basic way as 1988's Internet Worm: they scan the network for computers with vulnerable network services, break in to those computers, and copy themselves over. Worm outbreaks have become a cyclical plague for both home users and businesses, eclipsed recently in terms of damage by spyware.

Concealment: Trojan horses, rootkits, and backdoors

Main articles: Trojan horse (http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), Rootkit ([../wiki/Rootkit](http://en.wikipedia.org/wiki/Rootkit)), and Backdoor ([../wiki/Backdoor_%28computing%29](http://en.wikipedia.org/wiki/Backdoor_%28computing%29))

For a malicious program to accomplish its goals, it must be able to do so without being shut down, or deleted by the user or administrator of the computer it's running on. Concealment can also help get the malware installed in the first place. When a malicious program is disguised as something innocuous or desirable, users may be tempted to install it without knowing what it does. This is the technique of the Trojan horse or trojan.

Broadly speaking, a Trojan horse is any program that invites the user to run it, but conceals a harmful or malicious payload. The payload may take effect immediately and can lead to many undesirable effects, such as deleting all the user's files, or more commonly it may install further harmful software into the user's system to serve the creator's longer-term goals. Trojan horses known as droppers are used to start off a worm outbreak, by injecting the worm into users' local networks.

One of the most common ways that spyware is distributed is as a Trojan horse, bundled with a piece of desirable software that the user downloads from the Internet. When the user installs the software, the spyware is installed alongside. Spyware authors who attempt to act in a legal fashion may include an end-user license agreement which states the behavior of the spyware in loose terms, and which the users are unlikely to read or understand.

Once a malicious program is installed on a system, it is often useful to the creator if it stays concealed. The same is true when a human attacker breaks into a computer directly. Techniques known as rootkits allow this concealment, by modifying the host operating system so that the malware is hidden from the user. Rootkits can prevent a malicious process from being visible in the system's list of processes, or keep its files from being read. Originally, a rootkit was a set of tools installed by a human attacker on a Unix system where the attacker had gained administrator (root) access. Today, the term is used more generally for concealment routines in a malicious program.

Some malicious programs contain routines to defend against removal: not merely to hide themselves, but to repel attempts to remove them. An early example of this behavior is recorded in the Jargon File tale of a pair of programs infesting a Xerox CP-V timesharing system:

Each ghost-job would detect the fact that the other had been killed, and would start a new copy of the recently slain program within a few milliseconds. The only way to kill both ghosts was to kill them simultaneously (very difficult) or to deliberately crash the system.

Similar techniques are used by some modern malware, wherein the malware starts a number of processes which monitor one another and restart any process which is killed off by the operator.

A backdoor is a method of bypassing normal authentication procedures. Once a system has been compromised (by one of the above methods, or in some other way), one or more backdoors may be installed, in order to allow the attacker access in the future. The idea has often been suggested that computer manufacturers preinstall backdoors on their systems to provide technical support for customers, but this has never been reliably verified. Crackers typically use backdoors to secure remote access to a computer, while attempting to remain hidden from casual inspection. To install backdoors crackers may use Trojan horses, worms, or other methods.

Malware for profit: spyware, botnets, keystroke loggers, and dialers

Main articles: Spyware (<http://en.wikipedia.org/wiki/Spyware>), Botnet ([../wiki/Botnet](http://en.wikipedia.org/wiki/Botnet)), Keystroke logging ([../wiki/Keystroke_logging](http://en.wikipedia.org/wiki/Keystroke_logging)), and Dialer#Fraudulent dialers

During the 1980s and 1990s, it was usually taken for granted that malicious programs were created as a form of vandalism or prank (although some viruses were spread only to discourage users from illegal software exchange.) More recently, the greater share of malware programs have been written with a financial or profit motive in mind. This can be taken as the malware authors' choice to monetize their control over infected systems: to turn that control into a source of revenue.

Since 2003 or so, the most costly form of malware in terms of time and money spent in recovery has been the broad category known as spyware.[citation needed] Spyware programs are commercially produced for the purpose of gathering information about computer users, showing them pop-up ads, or altering web-browser behavior for the financial benefit of the spyware creator. For instance, some spyware programs redirect search engine results to paid advertisements. Others, often called "stealware" by the media, overwrite affiliate marketing codes so that revenue goes to the spyware creator rather than the intended recipient.

Spyware programs are sometimes installed as Trojan horses of one sort or another. They differ in that their creators present themselves openly as businesses, for instance by selling advertising space on the pop-ups created by the malware. Most such programs present the user with an end-user license agreement which purportedly protects the creator from prosecution under computer contaminant laws. However, spyware EULAs have not yet been upheld in court.

Another way that financially-motivated malware creator can profit from their infections is to directly use the infected computers to do work for the creator. Spammer viruses, such as the Sobig and Mydoom virus families, are commissioned by e-mail spam gangs. The infected computers are used as proxies to send out spam messages. The advantage to spammers of using infected computers is that they are available in large supply (thanks to the virus) and they provide anonymity, protecting the spammer from prosecution. Spammers have also used infected PCs to target anti-spam organizations with distributed denial-of-service attacks.

In order to coordinate the activity of many infected computers, attackers have used coordinating systems known as botnets. In a botnet, the malware or malbot logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously. Botnets can also be used to push upgraded malware to the infected systems, keeping them resistant to anti-virus software or other security measures.

Lastly, it is possible for a malware creator to profit by simply stealing from the person whose computer is infected. Some malware programs install a key logger, which copies down the user's keystrokes when entering a password, credit card number, or other information that may be useful to the creator. This is then transmitted to the malware creator automatically, enabling credit card fraud and other theft. Similarly, malware may copy the CD key or password for online games, allowing the creator to steal accounts or virtual items.

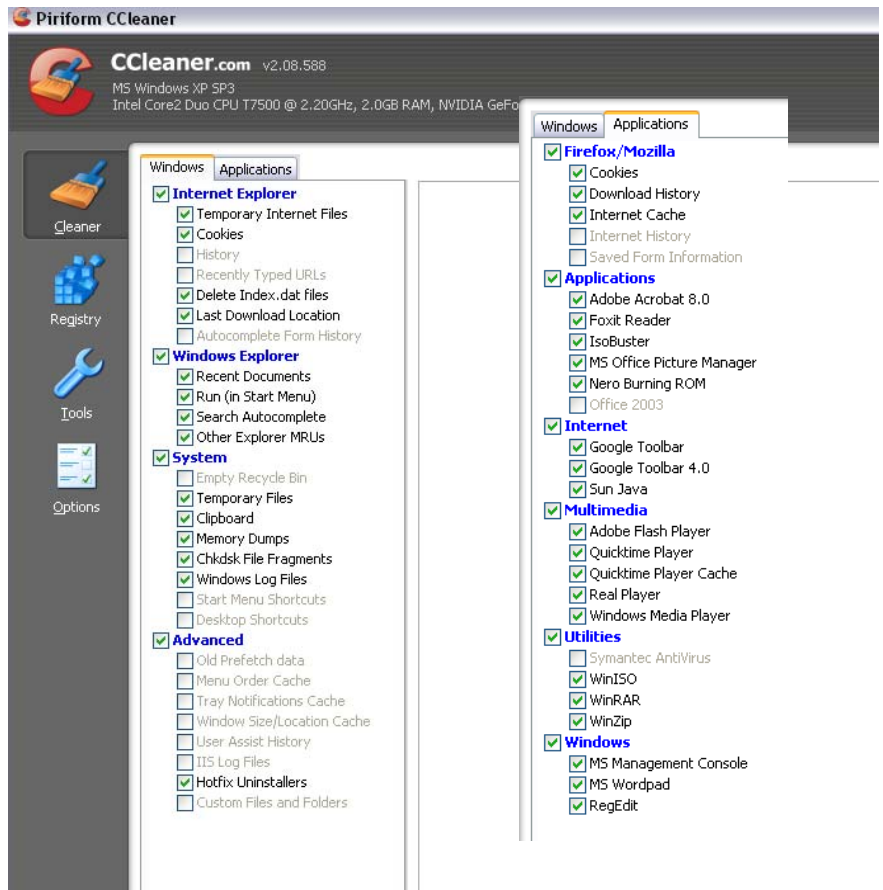
Another way of stealing money from the infected PC owner is to take control of the modem and dial an expensive toll call. Dialer (or porn dialer) software dials up a premium-rate telephone number such as a U.S. "900 number" and leave the line open, charging the toll to the infected user.

Cleaning up your computer

Remove temporary files, cookies & MRU's using CCleaner

What is CCleaner? It's an excellent freeware tool that removes unnecessary files and cleans the registry. Download the program from www.ccleaner.com. Double click to install, then click *Next, I Agree, Next*. At the next screen, I recommend that only the 1st, 2nd and 4th (from the top) are checked, and click *Install*.

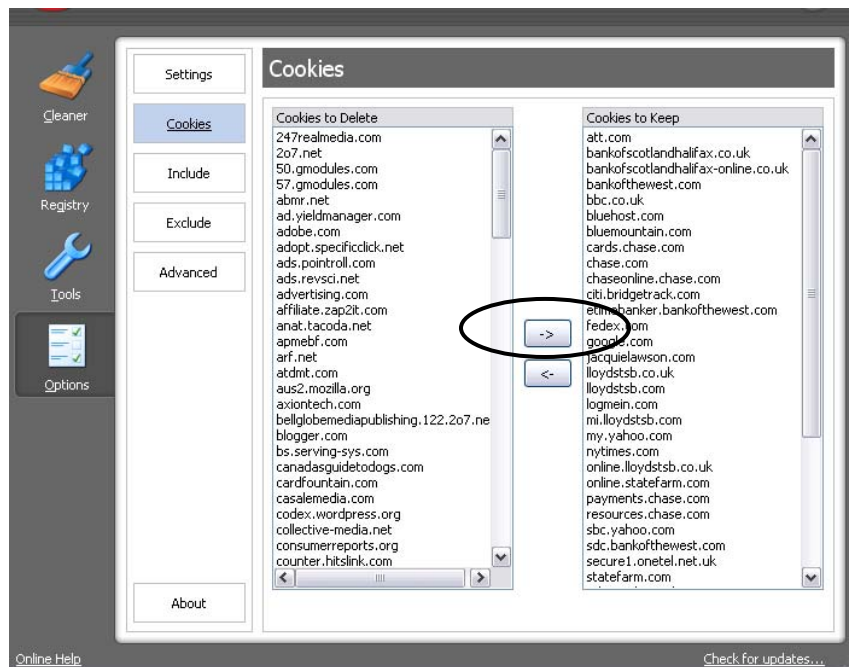
Open CCleaner and you will see the main cleaner page. All the items that can be removed are shown in various groups, together with a check mark to indicate if you want that item cleaned. There are two tabs, "Windows" and "Applications". In the Windows tab, I normally check all items as shown. Similarly for the Application tab. There is further help about using CCleaner on <http://www.ccleanerbegingersguide.com/>.



The next step is to set up the options – particularly for cookies. This is a great feature of this utility – that you can select cookies you do not want to remove. Click Options and Cookies and then use the arrow buttons to move the cookies between the two columns.

Having made the selections, return to Cleaner and click the analyze button. This runs a simulation, allowing a check of all the files that will be deleted. If all is ok, click the "Run Cleaner" button to remove much of the junk from your computer.

From now on, all that's needed on a weekly basis, is to open CCleaner,

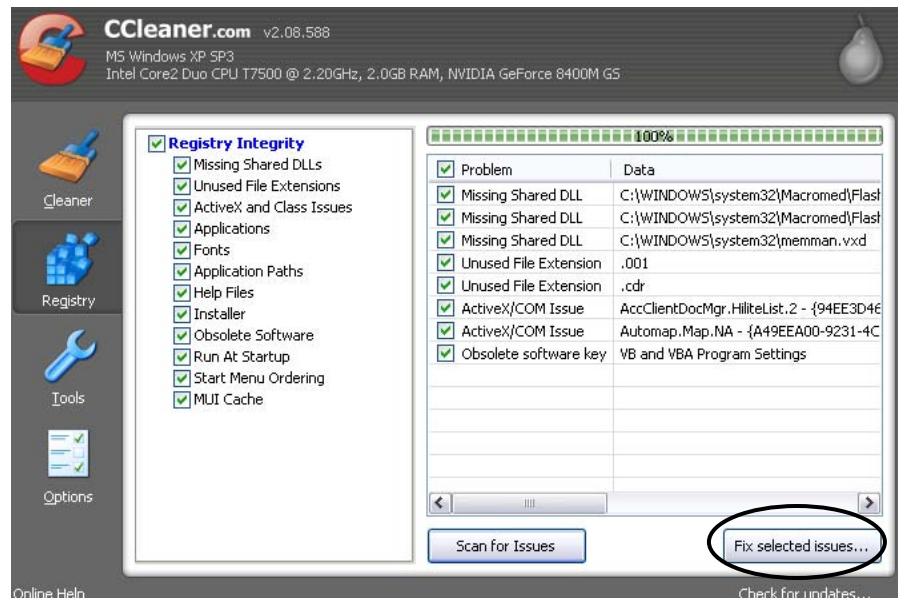


click the “Run Cleaner” button and the junk will be removed as per the options selected.

Cleaning the registry.

The registry is a large file where programs keep information they need about where you keep your documents, or where a program keeps its data file, etc. Often, when programs are removed from your computer, they don’t “clean up” all their entries from the registry. CCleaner has a very safe registry cleanup function.

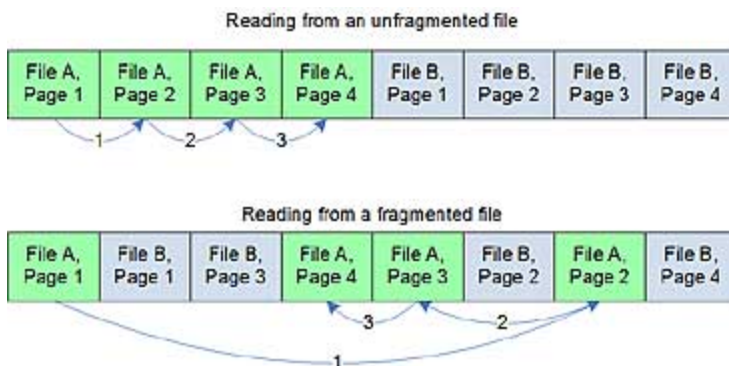
Open CCleaner and click the *Registry* button. Leave all the check marks checked, and click *Scan for Issues*. When complete, click *Fix Selected Issues*. I recommend you click “Yes” to make a backup of the deleted items. Then click “Fix all Selected Issues” and OK and then Close. You should repeat this process until no issues are found



Defragment Hard Drives

I hate newspaper articles that start on the front page but continue somewhere in the middle of the newspaper. I could get through the article much faster if it was printed on consecutive pages like a magazine article. Files on your computer can either be **fragmented** like a newspaper, or **unfragmented** like a magazine. Over time, more and more files become fragmented. When a file is fragmented, it takes longer for the computer to read it because it has to skip to different sections of the hard disk—just like it takes me a few seconds to find a page in the middle of a newspaper. The figure compares how a computer reads unfragmented and fragmented files.

You cannot work on your computer and defrag your computer at the same time. It is common for disk defragmenter to take a long time. The time can vary from 10 minutes to many hours, so run the Disk Defragmenter when you don’t need to use the computer! If you defragment regularly, the time taken to complete will be quite short.



To run the Disk Defrag utility do the following.

- Make sure ALL programs are closed
- If necessary, turn off your screensaver.
- Click on **Start** on the task bar.
- Point to **All Programs**.

- Point to **Accessories**. Point to **System Tools**.
- Click **Disk Defragmenter**. The Disk Defragmenter window appears.



Note: You can also get to this screen as follows. Double-click **My Computer**. Right-click the drive (volume) you want to analyze or defragment. Click **Properties**. Click the **Tools** tab. Click the **Defragment Now** button.

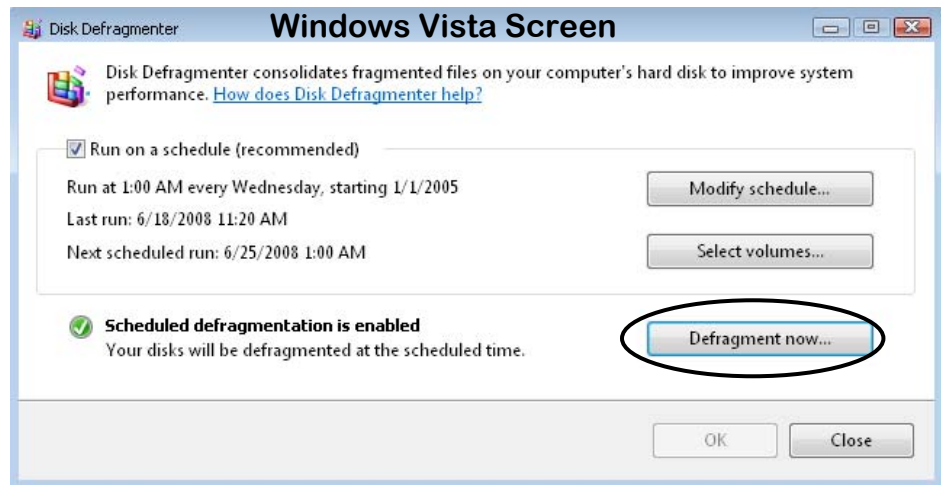
For Windows XP, select the hard drive to defragment, and click the **Defragment** button.

The Disk Defragmenter window consists of two main areas. The upper portion lists the disk (volume) on your computer. The lower portion displays graphical representations of

the amount of fragmentation on the disk before and after running defrag.

For Vista, click the **Defragment now** button, select the hard drive to defragment, and click **OK**.

If you have more than one hard drive, repeat the process for the other drives



Scheduling CCleaner and Disk Defragmentation

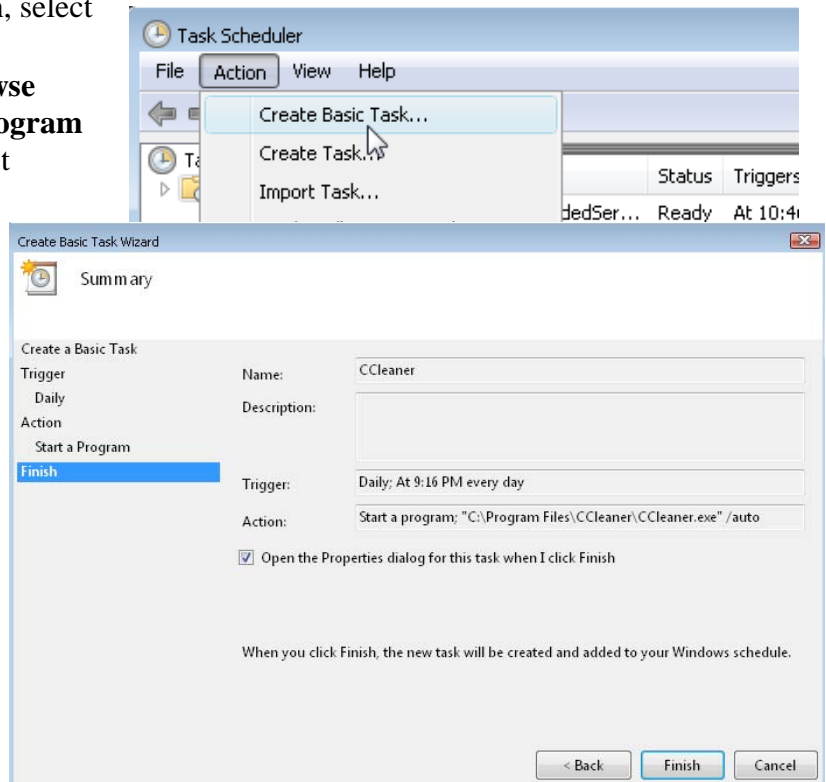
Vista

As can be seen from the above screenshot, Vista has scheduling built in for the Disk Defragmenter. Check **Run on a schedule** and click **Modify Schedule** to set day and time.

CCleaner

1. Open Control Panel, double click **Administrative Tools** and then **Task Scheduler**.
2. In Task Scheduler, click **Action>Create Basic Task**. Give the task a name (e.g. CCleaner), click **Next**. Select when you want to run the task (e.g. daily), click **Next** and select Time/Frequency/etc.

3. Click **Next** and at the next screen, select **Start a Program**.
4. At the next screen click the **Browse** button and navigate to the **C:\Program Files\CCleaner** folder and select **CCleaner.exe** and in the **Add arguments box**, type **/auto** and click **Next**.
5. Check **Open the properties....** and review all the settings. If they look correct (similar to this screenshot), then click **Finish**. In the Window that now opens, check the box next to **Run with highest privileges** and then click **OK**.



Windows XP

First, we will create a batch file to run CCleaner and do a defrag of the C: drive

1. Open Notepad (Start>All Programs>Accessories>Notepad)
2. Type in the following 2 lines:

```
"c:\program files\ccleaner\ccleaner.exe" /auto
"c:\windows\system32\defrag.exe" c:
```
3. Click **File>Save** as and in the "**Save in**" drop down window select the **C: drive** and type **cleanup.bat** as the file name and click the **Save** button.
4. Close the notepad file

Scheduler

1. In the Control Panel, double click **Scheduled Task** and then **Add Scheduled Task**.
2. Click **Next** and when the list of programs appears, click the **Browse** button and select **cleanup.bat** and click **Open**.
3. Now select how often you'd like to run CCleaner, click **Next** and select days/time, etc. and click **Next** and **Next**. Check **Open advanced properties...** and click **Finish**. If a warning window appears, click **OK** to dismiss. On the window that opens, it's *important* to check **Run only if logged on**, and click **OK**.

