**Malware**





[Beast](http://en.wikipedia.org/wiki/Beast_Trojan_%28trojan_horse%29), a Windows-based [backdoor](http://en.wikipedia.org/wiki/Backdoor_%28computing%29) [Trojan horse](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29).

Malware includes [computer viruses](http://en.wikipedia.org/wiki/Computer_virus), [ransomware](http://en.wikipedia.org/wiki/Ransomware_%28malware%29), [worms](http://en.wikipedia.org/wiki/Computer_worm), [trojan horses](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), [rootkits](http://en.wikipedia.org/wiki/Rootkit), [keyloggers](http://en.wikipedia.org/wiki/Keystroke_logging), [dialers](http://en.wikipedia.org/wiki/Dialer#Fraudulent_dialer), [spyware](http://en.wikipedia.org/wiki/Spyware), [adware](http://en.wikipedia.org/wiki/Adware), malicious [BHOs](http://en.wikipedia.org/wiki/Browser_Helper_Object), [rogue security software](http://en.wikipedia.org/wiki/Rogue_security_software) and other malicious programs; the majority of active malware threats are usually worms or trojans rather than viruses.[[3]](http://en.wikipedia.org/wiki/Malware#cite_note-3) In [law](http://en.wikipedia.org/wiki/Law), malware is sometimes known as a **computer contaminant**, as in the legal codes of several [U.S.](http://en.wikipedia.org/wiki/United_States) states.[[4]](http://en.wikipedia.org/wiki/Malware#cite_note-4)[[5]](http://en.wikipedia.org/wiki/Malware#cite_note-5) Malware is different from defective software, which is a legitimate software but contains harmful [bugs](http://en.wikipedia.org/wiki/Software_bug) that were not corrected before release. However, some malware is disguised as genuine software, and may come from an official company website in the form of a useful or attractive program which has the harmful malware embedded in it along with additional tracking software that gathers marketing statistics.[[6]](http://en.wikipedia.org/wiki/Malware#cite_note-6)

Software such as [anti-virus](http://en.wikipedia.org/wiki/Anti-virus), anti-malware, and [firewalls](http://en.wikipedia.org/wiki/Firewall_%28computing%29) are relied upon by users at home, small and large organisations around the globe to safeguard against malware attacks which helps in identifying and preventing the further spread of malware in the network.

|  |
| --- |
| **Contents*** [1 Purposes](http://en.wikipedia.org/wiki/Malware#Purposes)
* [2 Proliferation](http://en.wikipedia.org/wiki/Malware#Proliferation)
* [3 Infectious malware: viruses and worms](http://en.wikipedia.org/wiki/Malware#Infectious_malware:_viruses_and_worms)
* [4 Concealment: Viruses, trojan horses, rootkits, and backdoors](http://en.wikipedia.org/wiki/Malware#Concealment:_Viruses.2C_trojan_horses.2C_rootkits.2C_and_backdoors)
	+ [4.1 Viruses](http://en.wikipedia.org/wiki/Malware#Viruses)
	+ [4.2 Trojan horses](http://en.wikipedia.org/wiki/Malware#Trojan_horses)
	+ [4.3 Rootkits](http://en.wikipedia.org/wiki/Malware#Rootkits)
	+ [4.4 Backdoors](http://en.wikipedia.org/wiki/Malware#Backdoors)
* [5 Vulnerability to malware](http://en.wikipedia.org/wiki/Malware#Vulnerability_to_malware)
	+ [5.1 Security defects in software](http://en.wikipedia.org/wiki/Malware#Security_defects_in_software)
	+ [5.2 Insecure design or user error](http://en.wikipedia.org/wiki/Malware#Insecure_design_or_user_error)
	+ [5.3 Over-privileged users and over-privileged code](http://en.wikipedia.org/wiki/Malware#Over-privileged_users_and_over-privileged_code)
	+ [5.4 Use of the same operating system](http://en.wikipedia.org/wiki/Malware#Use_of_the_same_operating_system)
* [6 Anti-malware strategies](http://en.wikipedia.org/wiki/Malware#Anti-malware_strategies)
	+ [6.1 Anti-virus and anti-malware software](http://en.wikipedia.org/wiki/Malware#Anti-virus_and_anti-malware_software)
	+ [6.2 Backup and recovery strategies](http://en.wikipedia.org/wiki/Malware#Backup_and_recovery_strategies)
	+ [6.3 Website security scans](http://en.wikipedia.org/wiki/Malware#Website_security_scans)
	+ [6.4 Eliminating over-privileged code](http://en.wikipedia.org/wiki/Malware#Eliminating_over-privileged_code)
* [7 Grayware](http://en.wikipedia.org/wiki/Malware#Grayware)
* [8 History of viruses and worms](http://en.wikipedia.org/wiki/Malware#History_of_viruses_and_worms)
* [9 Academic research](http://en.wikipedia.org/wiki/Malware#Academic_research)
* [10 See also](http://en.wikipedia.org/wiki/Malware#See_also)
* [11 References](http://en.wikipedia.org/wiki/Malware#References)
* [12 External links](http://en.wikipedia.org/wiki/Malware#External_links)
 |

**Purposes**





Malware by categories on March 16, 2011.

Many early infectious programs, including the first [Internet Worm](http://en.wikipedia.org/wiki/Morris_worm), were written as experiments or pranks. Today, malware is used primarily to steal sensitive information of personal, financial, or business importance by black hat hackers with harmful intentions.[*[citation needed](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed%22%20%5Co%20%22Wikipedia%3ACitation%20needed)*]

Malware is sometimes used broadly against government or corporate websites to gather guarded information, or to disrupt their operation in general. However, malware is often used against individuals to gain personal information such as social security numbers, bank or credit card numbers, and so on. Left unguarded, personal and [networked](http://en.wikipedia.org/wiki/Computer_network) computers can be at considerable risk against these threats. (These are most frequently counter-acted by various types of [firewalls](http://en.wikipedia.org/wiki/Firewall_%28computing%29), [anti-virus](http://en.wikipedia.org/wiki/Anti-virus) software, and [network hardware](http://en.wikipedia.org/wiki/Network_switch)).[*[citation needed](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed%22%20%5Co%20%22Wikipedia%3ACitation%20needed)*]

Since the rise of widespread [broadband](http://en.wikipedia.org/wiki/Broadband) [Internet](http://en.wikipedia.org/wiki/Internet) access, malicious software has more frequently been designed for profit. Since 2003, the majority of widespread [viruses](http://en.wikipedia.org/wiki/Computer_virus) and worms have been designed to take control of users' computers for black-market exploitation.[[7]](http://en.wikipedia.org/wiki/Malware#cite_note-7) Infected "[zombie computers](http://en.wikipedia.org/wiki/Zombie_computer)" are used to send [email spam](http://en.wikipedia.org/wiki/Email_spam), to host contraband data such as [child pornography](http://en.wikipedia.org/wiki/Child_pornography),[[8]](http://en.wikipedia.org/wiki/Malware#cite_note-8) or to engage in [distributed denial-of-service](http://en.wikipedia.org/wiki/Distributed_denial-of-service) [attacks](http://en.wikipedia.org/wiki/Attack_%28computing%29) as a form of [extortion](http://en.wikipedia.org/wiki/Extortion).[[9]](http://en.wikipedia.org/wiki/Malware#cite_note-9)

Another strictly for-profit category of malware has emerged, called [spyware](http://en.wikipedia.org/wiki/Spyware). These programs are designed to monitor users' web browsing, display unsolicited advertisements, or redirect [affiliate marketing](http://en.wikipedia.org/wiki/Affiliate_marketing) revenues to the [spyware](http://en.wikipedia.org/wiki/Spyware) creator. Spyware programs do not spread like [viruses](http://en.wikipedia.org/wiki/Computer_virus); instead they are generally installed by exploiting security holes. They can also be packaged together with user-installed software, such as peer-to-peer applications.[*[citation needed](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed%22%20%5Co%20%22Wikipedia%3ACitation%20needed)*]

**Proliferation**

Preliminary results from [Symantec](http://en.wikipedia.org/wiki/Symantec) published in 2008 suggested that "the release rate of malicious [code](http://en.wikipedia.org/wiki/Source_code) and other unwanted programs may be exceeding that of legitimate software applications."[[10]](http://en.wikipedia.org/wiki/Malware#cite_note-10) According to [F-Secure](http://en.wikipedia.org/wiki/F-Secure), "As much malware [was] produced in 2007 as in the previous 20 years altogether."[[11]](http://en.wikipedia.org/wiki/Malware#cite_note-11) Malware's most common pathway from criminals to users is through the [Internet](http://en.wikipedia.org/wiki/Internet): primarily by e-mail and the [World Wide Web](http://en.wikipedia.org/wiki/World_Wide_Web).[[12]](http://en.wikipedia.org/wiki/Malware#cite_note-12)

The prevalence of malware as a vehicle for Internet crime, along with the challenge of anti-malware software to keep up with the continuous stream of new malware, has seen the adoption of a new mindset for individuals and businesses using the Internet. With the amount of malware currently being distributed, some percentage of computers will always be infected. For businesses, especially those that sell mainly over the Internet, this means they need to find a way to operate despite security concerns. The result is a greater emphasis on back-office protection designed to protect against advanced malware operating on customers' computers.[[13]](http://en.wikipedia.org/wiki/Malware#cite_note-13) A 2013 Webroot study shows that 64% of companies allow remote access to servers for 25% to 100% of their workforce and that companies with more than 25% of their employees accessing servers remotely have higher rates of malware threats.[[14]](http://en.wikipedia.org/wiki/Malware#cite_note-14)

On March 29, 2010, [Symantec Corporation](http://en.wikipedia.org/wiki/Symantec_Corporation) named [Shaoxing](http://en.wikipedia.org/wiki/Shaoxing), China, as the world's malware capital.[[15]](http://en.wikipedia.org/wiki/Malware#cite_note-15) A 2011 study from the [University of California, Berkeley](http://en.wikipedia.org/wiki/University_of_California%2C_Berkeley), and the Madrid Institute for Advanced Studies published an article in *Software Development Technologies*, examining how entrepreneurial [hackers](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29) are helping enable the spread of malware by offering access to computers for a price. [Microsoft](http://en.wikipedia.org/wiki/Microsoft) reported in May 2011 that one in every 14 downloads from the Internet may now contain malware [code](http://en.wikipedia.org/wiki/Source_code). Social media, and Facebook in particular, are seeing a rise in the number of tactics used to spread malware to computers.[[16]](http://en.wikipedia.org/wiki/Malware#cite_note-16)

**Infectious malware: viruses and worms**

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

|  |  |
| --- | --- |
| Question book-new.svg | This section **does not** [**cite**](http://en.wikipedia.org/wiki/Wikipedia%3ACiting_sources) **any** [**references or sources**](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability). Please help improve this section by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help%3AIntroduction_to_referencing/1). Unsourced material may be challenged and [removed](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability#Burden_of_evidence). *(March 2013)*  |

The best-known types of malware, [viruses](http://en.wikipedia.org/wiki/Computer_virus) and worms, are known for the manner in which they spread, rather than any specific types of behavior. The term [*computer virus*](http://en.wikipedia.org/wiki/Computer_virus) is used for a program that has infected some [executable](http://en.wikipedia.org/wiki/Executable) software and, *when run*, causes the virus to spread to other [executables](http://en.wikipedia.org/wiki/Executable). On the other hand, a [*worm*](http://en.wikipedia.org/wiki/Computer_worm) is a program that *actively* transmits itself over a [network](http://en.wikipedia.org/wiki/Computer_network) to infect other computers. These definitions lead to the observation that a [virus](http://en.wikipedia.org/wiki/Computer_virus) requires user intervention to spread, whereas a worm spreads itself automatically.[[17]](http://en.wikipedia.org/wiki/Malware#cite_note-17)

Using this distinction, infections transmitted by [email](http://en.wikipedia.org/wiki/Email) or [Microsoft Word](http://en.wikipedia.org/wiki/Microsoft_Word) documents, which rely on the recipient opening a file or email to infect the system, would be classified as [viruses](http://en.wikipedia.org/wiki/Computer_virus) rather than worms. Some writers in the trade and popular press misunderstand this distinction and use the terms interchangeably.

**Concealment: Viruses, trojan horses, rootkits, and backdoors**

**Viruses**

Strategies that viruses use to conceal themselves are described in the [computer virus](http://en.wikipedia.org/wiki/Computer_virus) article.

**Trojan horses**

|  |  |
| --- | --- |
| Question book-new.svg | This section **does not** [**cite**](http://en.wikipedia.org/wiki/Wikipedia%3ACiting_sources) **any** [**references or sources**](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability). Please help improve this section by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help%3AIntroduction_to_referencing/1). Unsourced material may be challenged and [removed](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability#Burden_of_evidence). *(March 2013)*  |

For a malicious program to accomplish its goals, it must be able to run without being detected, shut down, or deleted. When a malicious program is disguised as something normal or desirable, users may willfully install it without realizing it. This is the technique of the [*Trojan horse*](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29) or *trojan*. In broad terms, a Trojan horse is any program that invites the user to run it, concealing harmful or malicious [code](http://en.wikipedia.org/wiki/Source_code). The code may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or installing additional harmful software.

One of the most common ways that spyware is distributed is as a [Trojan horse](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), bundled with a piece of desirable software that the user downloads from the Internet. When the user installs the software, the spyware is installed along with it. Spyware authors who attempt to act in a legal fashion may include an [end-user license agreement](http://en.wikipedia.org/wiki/End-user_license_agreement) that states the behavior of the spyware in loose terms, which users may not read or understand.

**Rootkits**

Once a malicious program is installed on a system, it is essential that it stay concealed, to avoid detection. Techniques known as [*rootkits*](http://en.wikipedia.org/wiki/Rootkit) allow this concealment, by modifying the host's operating system so that the malware is hidden from the user. Rootkits can prevent a malicious [process](http://en.wikipedia.org/wiki/Process_%28computing%29) from being visible in the system's list of [processes](http://en.wikipedia.org/wiki/Process_%28computing%29), or keep its files from being read.[*[citation needed](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed%22%20%5Co%20%22Wikipedia%3ACitation%20needed)*]

Some malicious programs contain routines to defend against removal, not merely to hide themselves, but to resist attempts to remove them. An early example of this behavior is recorded in the [Jargon File](http://en.wikipedia.org/wiki/Jargon_File) tale of a pair of programs infesting a Xerox [CP-V](http://en.wikipedia.org/w/index.php?title=CP-V&action=edit&redlink=1) time sharing system:

Each ghost-job would detect the fact that the other had been killed, and would start a new copy of the recently stopped 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.[[18]](http://en.wikipedia.org/wiki/Malware#cite_note-18)

**Backdoors**

|  |  |
| --- | --- |
| Question book-new.svg | This section **does not** [**cite**](http://en.wikipedia.org/wiki/Wikipedia%3ACiting_sources) **any** [**references or sources**](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability). Please help improve this section by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help%3AIntroduction_to_referencing/1). Unsourced material may be challenged and [removed](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability#Burden_of_evidence). *(March 2013)*  |

A [backdoor](http://en.wikipedia.org/wiki/Backdoor_%28computing%29) is a method of bypassing normal [authentication](http://en.wikipedia.org/wiki/Authentication) procedures. Once a system has been compromised, one or more backdoors may be installed in order to allow easier access in the future. Backdoors may also be installed prior to malicious software, to allow attackers entry.

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](http://en.wikipedia.org/wiki/Hacker_%28computer_security%29) 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](http://en.wikipedia.org/wiki/Trojan_horse_%28computing%29), [worms](http://en.wikipedia.org/wiki/Computer_worm), or other methods.

**Vulnerability to malware**

Main article: [Vulnerability (computing)](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29)

* In this context, as throughout, it should be borne in mind that the “system” under attack may be of various types, e.g. a single computer and operating system, a [network](http://en.wikipedia.org/wiki/Computer_network) or an application.
* Various factors make a system more vulnerable to malware:

**Security defects in software**

Malware exploits security defects (security bugs, or [vulnerabilities](http://en.wikipedia.org/wiki/Software_vulnerability)) in the design of the operating system, in applications (such as browsers—avoid using Internet Explorer 8 or earlier, e.g. on Windows XP[[19]](http://en.wikipedia.org/wiki/Malware#cite_note-19)), or in (old versions of) browser plugins such as [Adobe Flash Player](http://en.wikipedia.org/wiki/Adobe_Flash_Player#Security), [Adobe Acrobat / Reader](http://en.wikipedia.org/wiki/Adobe_Acrobat#Security), or [Java](http://www.java.com/en/download/testjava.jsp) (see [Java SE critical security issues](http://en.wikipedia.org/wiki/Java_SE#Critical_security_issues_with_the_Java_SE_plugin)).[[20]](http://en.wikipedia.org/wiki/Malware#cite_note-20)[[21]](http://en.wikipedia.org/wiki/Malware#cite_note-21) Sometimes even installing new versions of such plugins does not automatically uninstall old versions. Security advisories from such companies announce security-related updates.[[22]](http://en.wikipedia.org/wiki/Malware#cite_note-22) Common vulnerabilities are assigned [CVE IDs](http://en.wikipedia.org/wiki/Common_Vulnerabilities_and_Exposures) and listed in the US [National Vulnerability Database](http://en.wikipedia.org/wiki/National_Vulnerability_Database). [Secunia PSI](http://en.wikipedia.org/wiki/Secunia#PSI)[[23]](http://en.wikipedia.org/wiki/Malware#cite_note-23) is an example of software, free for personal use, that will check a PC for vulnerable out-of-date software, and attempt to update it.

Most systems contain [bugs](http://en.wikipedia.org/wiki/Software_bug), or loopholes, which may be exploited by malware. A typical example is a [buffer-overrun](http://en.wikipedia.org/wiki/Buffer_overrun) [vulnerability](http://en.wikipedia.org/wiki/Software_vulnerability), in which an interface designed to store data, in a small area of memory, allows the caller to supply more data than will fit. This extra data then overwrites the interface's own [executable](http://en.wikipedia.org/wiki/Executable) structure (past the end of the buffer and other data). In this manner, malware can force the system to execute malicious [code](http://en.wikipedia.org/wiki/Source_code), by replacing legitimate [code](http://en.wikipedia.org/wiki/Source_code) with its own payload of instructions (or data values) copied into live memory, outside the buffer area.

**Insecure design or user error**

|  |  |
| --- | --- |
| Question book-new.svg | This section **does not** [**cite**](http://en.wikipedia.org/wiki/Wikipedia%3ACiting_sources) **any** [**references or sources**](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability). Please help improve this section by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help%3AIntroduction_to_referencing/1). Unsourced material may be challenged and [removed](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability#Burden_of_evidence). *(March 2013)*  |

Originally, PCs had to be booted from floppy disks. Until recently, it was common for a computer to boot from an external [boot device](http://en.wikipedia.org/wiki/Booting#Boot_devices_.28IBM_PC.29) by default. This meant that the computer would, by default, boot from a floppy disk, USB flash drive, or CD—and malicious boot code could be used to install malware or boot into a modified operating system. Autorun or autoplay features may allow [code](http://en.wikipedia.org/wiki/Source_code) to be automatically [executed](http://en.wikipedia.org/wiki/Executable) from a [floppy disk](http://en.wikipedia.org/wiki/Floppy_disk), [CD-ROM](http://en.wikipedia.org/wiki/CD-ROM) or [USB](http://en.wikipedia.org/wiki/USB) device with or without the user’s permission. Older email software would automatically open [HTML email](http://en.wikipedia.org/wiki/HTML_email) containing malicious [JavaScript](http://en.wikipedia.org/wiki/JavaScript) code; users may also unwarily open (execute) malicious email attachments.

**Over-privileged users and over-privileged code**

|  |  |
| --- | --- |
| Question book-new.svg | This section **does not** [**cite**](http://en.wikipedia.org/wiki/Wikipedia%3ACiting_sources) **any** [**references or sources**](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability). Please help improve this section by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help%3AIntroduction_to_referencing/1). Unsourced material may be challenged and [removed](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability#Burden_of_evidence). *(March 2013)*  |

Main article: [principle of least privilege](http://en.wikipedia.org/wiki/Principle_of_least_privilege)

* [Over-privileged](http://en.wikipedia.org/wiki/Administrative_privileges) users: some systems allow all users to modify their internal structures. This was the standard operating procedure for early microcomputer and home computer systems, where there was no distinction between an *Administrator* or *root*, and a regular user of the system. In some systems, [non-administrator](http://en.wikipedia.org/wiki/System_administrator) users are over-privileged by design, in the sense that they are allowed to modify internal structures of the system. In some environments, users are over-privileged because they have been inappropriately granted administrator or equivalent status.
* Over-privileged [code](http://en.wikipedia.org/wiki/Source_code): some systems allow code [executed](http://en.wikipedia.org/wiki/Executable) by a user to access all rights of that user. Also standard operating procedure for early microcomputer and home computer systems. Malware, running as over-privileged code, can use this privilege to subvert the system. Almost all currently popular operating systems, and also many [scripting applications](http://en.wikipedia.org/wiki/Script_%28computing%29) allow code too many privileges, usually in the sense that when a user [executes](http://en.wikipedia.org/wiki/Executable) code, the system allows that code all rights of that user. This makes users vulnerable to malware in the form of [e-mail attachments](http://en.wikipedia.org/wiki/E-mail_attachment), which may or may not be disguised.

**Use of the same operating system**

* Weight of numbers: simply because the vast majority of existing malware is written to attack Windows systems, then Windows systems are more vulnerable to succumbing to malware attacks (regardless of the security strengths or weaknesses of Windows itself).[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed)]
* Homogeneity: e.g. when all computers in a [network](http://en.wikipedia.org/wiki/Computer_network) run the same operating system; upon exploiting one, one [worm](http://en.wikipedia.org/wiki/Computer_worm) can exploit them all:[[24]](http://en.wikipedia.org/wiki/Malware#cite_note-UKan-24) For example, [Microsoft Windows](http://en.wikipedia.org/wiki/Microsoft_Windows) or [Mac OS X](http://en.wikipedia.org/wiki/Mac_OS_X) have such a large share of the market that concentrating on either could enable an exploited vulnerability to subvert a large number of systems. Instead, introducing diversity, purely for the sake of robustness, could increase short-term costs for training and maintenance. However, having a few diverse nodes would deter total shutdown of the [network](http://en.wikipedia.org/wiki/Computer_network), and allow those nodes to help with recovery of the infected nodes. Such separate, functional redundancy could avoid the cost of a total shutdown.

**Anti-malware strategies**

Main article: [Antivirus software](http://en.wikipedia.org/wiki/Antivirus_software)

As malware attacks become more frequent, attention has begun to shift from [viruses](http://en.wikipedia.org/wiki/Computer_virus) and spyware protection, to malware protection, and programs that have been specifically developed to combat malware. (Other preventive and recovery measures, such as backup and recovery methods, are mentioned in the [computer virus](http://en.wikipedia.org/wiki/Computer_virus#Antivirus_software_and_other_preventive_measures) article).

**Anti-virus and anti-malware software**

A specific component of the [Anti virus](http://en.wikipedia.org/wiki/Anti-virus) and anti-malware software commonly referred as the on-access or real-time scanner, hooks deep into the operating system's core or [kernel](http://en.wikipedia.org/wiki/Operating_system_kernel) functions in a manner similar to how certain malware itself would attempt to operate, though with the user's informed permission for protecting the system. Any time the operating system accesses a file, the on-access scanner checks if the file is a 'legitimate' file or not. If the file is considered a malware by the scanner, the access operation will be stopped, the file will be dealt by the scanner in pre-defined way (how the Anti-virus program was configured during/post installation) and the user will be notified. This may considerably slow down the operating system depending on how well the scanner was programmed. The goal is to stop any operations the malware may attempt on the system before they occur, including activities which might exploit [bugs](http://en.wikipedia.org/wiki/Software_bug) or trigger unexpected operating system behavior.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed)]

Anti-malware programs can combat malware in two ways:

1. They can provide real time protection against the installation of malware software on a computer. This type of malware protection works the same way as that of antivirus protection in that the anti-malware software scans all incoming [network](http://en.wikipedia.org/wiki/Computer_network) data for malware software and blocks any [threats](http://en.wikipedia.org/wiki/Threat_%28computer%29) it comes across.
2. Anti-malware software programs can be used solely for detection and removal of malware software that has already been installed onto a computer. This type of anti-malware software scans the contents of the Windows registry, operating system files, and installed programs on a computer and will provide a list of any threats found, allowing the user to choose which files to delete or keep, or to compare this list to a list of known malware components, removing files that match.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed)]

Real-time protection from malware works identically to real-time antivirus protection: the software scans disk files at download time, and blocks the activity of components known to represent malware. In some cases, it may also intercept attempts to install start-up items or to modify browser settings. Because many malware components are installed as a result of [browser exploits](http://en.wikipedia.org/wiki/Browser_exploit) or user error, using security software (some of which are anti-malware, though many are not) to "sandbox" browsers (essentially isolate the browser from the computer and hence any malware induced change) can also be effective in helping to restrict any damage done.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed)]

Examples of Microsoft Windows [anti virus](http://en.wikipedia.org/wiki/Anti-virus) and anti-malware software include the optional [Microsoft Security Essentials](http://en.wikipedia.org/wiki/Microsoft_Security_Essentials)[[25]](http://en.wikipedia.org/wiki/Malware#cite_note-25) (for Windows XP, Vista and Windows 7) for real-time protection, the [Windows Malicious Software Removal Tool](http://en.wikipedia.org/wiki/Windows_Malicious_Software_Removal_Tool)[[26]](http://en.wikipedia.org/wiki/Malware#cite_note-26) (now included with [Windows (Security) Updates](http://en.wikipedia.org/wiki/Windows_Update) on "[Patch Tuesday](http://en.wikipedia.org/wiki/Patch_Tuesday)", the second Tuesday of each month), and [Windows Defender](http://en.wikipedia.org/wiki/Windows_Defender) (an optional download in the case of Windows XP).[[27]](http://en.wikipedia.org/wiki/Malware#cite_note-27) Additionally, several capable antivirus software programs are available for free download from the Internet (usually restricted to non-commercial use).[[28]](http://en.wikipedia.org/wiki/Malware#cite_note-28) A test has found a free program to be competitive with commercial competitors.[[29]](http://en.wikipedia.org/wiki/Malware#cite_note-29) Microsoft's [System File Checker](http://en.wikipedia.org/wiki/System_File_Checker) can be used to check for and repair corrupted system files.

Some viruses disable [System Restore](http://en.wikipedia.org/wiki/System_Restore) and other important Windows tools such as [Task Manager](http://en.wikipedia.org/wiki/Task_Manager) and [Command Prompt](http://en.wikipedia.org/wiki/Command_Prompt). Many such viruses can be removed by [rebooting](http://en.wikipedia.org/wiki/Booting) the computer, entering Windows [safe mode](http://en.wikipedia.org/wiki/Safe_mode) with networking, and then using system tools or [Microsoft Safety Scanner](http://en.wikipedia.org/wiki/Microsoft_Safety_Scanner).[[30]](http://en.wikipedia.org/wiki/Malware#cite_note-30)

**Backup and recovery strategies**

Backup and recovery strategies are mentioned in the [computer virus](http://en.wikipedia.org/wiki/Computer_virus#Recovery_strategies_and_methods) article.

**Website security scans**

As malware also harms the compromised websites (by breaking reputation, blacklisting in search engines, etc.), some websites offer vulnerability scanning. [[31]](http://en.wikipedia.org/wiki/Malware#cite_note-31) [[32]](http://en.wikipedia.org/wiki/Malware#cite_note-32) [[33]](http://en.wikipedia.org/wiki/Malware#cite_note-33) [[34]](http://en.wikipedia.org/wiki/Malware#cite_note-Google-34) Such scans check the website, detect malware, may note outdated software, and may report known security issues.

**Eliminating over-privileged code**

|  |  |
| --- | --- |
| Question book-new.svg | This section **does not** [**cite**](http://en.wikipedia.org/wiki/Wikipedia%3ACiting_sources) **any** [**references or sources**](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability). Please help improve this section by [adding citations to reliable sources](http://en.wikipedia.org/wiki/Help%3AIntroduction_to_referencing/1). Unsourced material may be challenged and [removed](http://en.wikipedia.org/wiki/Wikipedia%3AVerifiability#Burden_of_evidence). *(March 2013)*  |

Over-privileged [code](http://en.wikipedia.org/wiki/Source_code) dates from the time when most programs were either delivered with a computer or written in-house, and repairing it would at a stroke render most antivirus software almost redundant. It would, however, have appreciable consequences for the user interface and system management.

The system would have to maintain privilege profiles, and know which to apply for each user and program. In the case of newly installed software, an administrator would need to set up default profiles for the new code.

Eliminating vulnerability to rogue [device drivers](http://en.wikipedia.org/wiki/Device_drivers) is probably harder than for arbitrary rogue [executable](http://en.wikipedia.org/wiki/Executable). Two techniques, used in [VMS](http://en.wikipedia.org/wiki/OpenVMS), that can help are memory mapping only the registers of the device in question and a system interface associating the driver with interrupts from the device.

Other approaches are:

* Various forms of [virtualization](http://en.wikipedia.org/wiki/Platform_virtualization), allowing the code unlimited access only to virtual resources
* Various forms of [sandbox](http://en.wikipedia.org/wiki/Sandbox_%28computer_security%29) or [jail](http://en.wikipedia.org/wiki/Jail_%28computer_security%29)
* The security functions of [Java](http://en.wikipedia.org/wiki/Java_%28programming_language%29), in java.security

Such approaches, however, if not fully integrated with the operating system, would reduplicate effort and not be universally applied, both of which would be detrimental to security.

**Grayware**

See also: [Privacy-invasive software](http://en.wikipedia.org/wiki/Privacy-invasive_software)

Grayware (or greyware) is a general term that refers to applications or files that are not directly classified as malware (like worms or trojan horses), but can still negatively affect the performance of computers and involve significant security risks.

It describes applications that behave in an annoying or undesirable manner, and yet are less serious or troublesome than malware. Grayware encompasses [spyware](http://en.wikipedia.org/wiki/Spyware), [adware](http://en.wikipedia.org/wiki/Adware), [dialers](http://en.wikipedia.org/wiki/Dialer#Fraudulent_dialer), joke programs, remote access tools and any other program apart from a virus, that is designed to harm the performance of computers. The term is in use since around 2004.[[35]](http://en.wikipedia.org/wiki/Malware#cite_note-35)

Another term is PUP which stands for *Potentially Unwanted Program*. Applications unwanted despite have been downloaded by the user, users may fail to read a download agreement. PUPs include spyware, adware, and dialers.

**History of viruses and worms**

Before [Internet](http://en.wikipedia.org/wiki/Internet) access became widespread, viruses spread on personal computers by infecting the executable [boot sectors](http://en.wikipedia.org/wiki/Boot_sector) of floppy disks. By inserting a copy of itself into the [machine code](http://en.wikipedia.org/wiki/Machine_code) instructions in these [executables](http://en.wikipedia.org/wiki/Executable), a virus causes itself to be run whenever a program is run or the disk is booted. Early computer viruses were written for the [Apple II](http://en.wikipedia.org/wiki/Apple_II) and [Macintosh](http://en.wikipedia.org/wiki/Apple_Macintosh), but they became more widespread with the dominance of the [IBM PC](http://en.wikipedia.org/wiki/IBM_PC) and [MS-DOS](http://en.wikipedia.org/wiki/MS-DOS) system. [Executable](http://en.wikipedia.org/wiki/Executable)-infecting viruses are dependent on users exchanging software or boot-able floppies and thumb drives so they spread rapidly in computer hobbyist circles.[*[citation needed](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed%22%20%5Co%20%22Wikipedia%3ACitation%20needed)*]

The first worms, [network](http://en.wikipedia.org/wiki/Computer_network)-borne infectious programs, originated not on personal computers, but on multitasking [Unix](http://en.wikipedia.org/wiki/Unix) systems. The first well-known worm was the [Internet Worm](http://en.wikipedia.org/wiki/Morris_worm) of 1988, which infected [SunOS](http://en.wikipedia.org/wiki/SunOS) and [VAX](http://en.wikipedia.org/wiki/VAX) [BSD](http://en.wikipedia.org/wiki/BSD) systems. Unlike a virus, this worm did not insert itself into other programs. Instead, it exploited security holes ([vulnerabilities](http://en.wikipedia.org/wiki/Vulnerability_%28computing%29)) in network [server](http://en.wikipedia.org/wiki/Server_%28computing%29) programs and started itself running as a separate [process](http://en.wikipedia.org/wiki/Process_%28computing%29). This same behavior is used by today's worms as well.[*[citation needed](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed%22%20%5Co%20%22Wikipedia%3ACitation%20needed)*]

With the rise of the [Microsoft Windows](http://en.wikipedia.org/wiki/Microsoft_Windows) platform in the 1990s, and the flexible [macros](http://en.wikipedia.org/wiki/Macro_%28computer_science%29) of its applications, it became possible to write infectious code in the macro language of [Microsoft Word](http://en.wikipedia.org/wiki/Microsoft_Office_Word) and similar programs. These [*macro viruses*](http://en.wikipedia.org/wiki/Macro_virus_%28computing%29) infect documents and templates rather than applications ([executables](http://en.wikipedia.org/wiki/Executable)), but rely on the fact that macros in a Word document are a form of [executable](http://en.wikipedia.org/wiki/Executable) code.[[*citation needed*](http://en.wikipedia.org/wiki/Wikipedia%3ACitation_needed)]

Today, worms are most commonly written for the Windows OS, although a few like Mare-D[[36]](http://en.wikipedia.org/wiki/Malware#cite_note-36) and the [Lion worm](http://en.wikipedia.org/wiki/L10n_worm)[[37]](http://en.wikipedia.org/wiki/Malware#cite_note-37) are also written for [Linux](http://en.wikipedia.org/wiki/Linux) and [Unix](http://en.wikipedia.org/wiki/Unix) systems. Worms today work in the same basic way as 1988's Internet Worm: they scan the [network](http://en.wikipedia.org/wiki/Computer_network) and use vulnerable computers to replicate. Because they need no human intervention, worms can spread with incredible speed. The [SQL Slammer](http://en.wikipedia.org/wiki/SQL_Slammer) infected thousands of computers in a few minutes.[[38]](http://en.wikipedia.org/wiki/Malware#cite_note-38)

**Academic research**

Main article: [Malware research](http://en.wikipedia.org/wiki/Malware_research)

The notion of a self-reproducing computer program can be traced back to initial theories about the operation of complex automata.[[39]](http://en.wikipedia.org/wiki/Malware#cite_note-39) [John von Neumann](http://en.wikipedia.org/wiki/John_von_Neumann) showed that in theory a program could reproduce itself. This constituted a plausibility result in [computability theory](http://en.wikipedia.org/wiki/Computability_theory_%28computer_science%29). [Fred Cohen](http://en.wikipedia.org/wiki/Fred_Cohen) experimented with computer viruses and confirmed Neumann's postulate and investigated other properties of malware such as detectability, self-obfuscation using rudimentary encryption, and others. His Doctoral dissertation was on the subject of computer viruses.[[40]](http://en.wikipedia.org/wiki/Malware#cite_note-40)

**See also**

|  |  |
| --- | --- |
| Portal icon | [***Information technology portal***](http://en.wikipedia.org/wiki/Portal%3AInformation_technology) |
| Portal icon | [***Computer security portal***](http://en.wikipedia.org/wiki/Portal%3AComputer_security) |

* [Browser hijacking](http://en.wikipedia.org/wiki/Browser_hijacking)
* [Category:Web security exploits](http://en.wikipedia.org/wiki/Category%3AWeb_security_exploits)
* [Comparison of antivirus software](http://en.wikipedia.org/wiki/Comparison_of_antivirus_software)
* [Computer insecurity](http://en.wikipedia.org/wiki/Computer_insecurity)
* [Cyber spying](http://en.wikipedia.org/wiki/Cyber_spying)
* [Identity theft](http://en.wikipedia.org/wiki/Identity_theft)
* [Industrial espionage](http://en.wikipedia.org/wiki/Industrial_espionage)
* [Malvertising](http://en.wikipedia.org/wiki/Malvertising)
* [Riskware](http://en.wikipedia.org/wiki/Riskware)
* [Security in Web applications](http://en.wikipedia.org/wiki/Web_application#Writing_web_applications)
* [Social engineering (security)](http://en.wikipedia.org/wiki/Social_engineering_%28security%29)
* [Targeted threat](http://en.wikipedia.org/wiki/Targeted_threat)
* [Web server overload causes](http://en.wikipedia.org/wiki/Web_server#Overload_causes)