

## **Adware**

Adware is any software package with the sole purpose to automatically play, display, or download advertising material to a computer after the software is installed on it.

---

## **Backdoor**

A backdoor in a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication or securing remote access to a computer, while attempting to remain hidden from casual inspection. The backdoor may take the form of an installed program or could be a modification to a legitimate program.

---

## **Botnet**

Botnet is a jargon term for a collection of software robots, or bots, which run autonomously. This can also refer to the network of computers using distributed computing software. While the term "botnet" can be used to refer to any group of bots, such as IRC bots, the word is generally used to refer to a collection of compromised machines running programs, usually referred to as worms, Trojan horses, or backdoors, under a common command and control infrastructure. A botnet's originator can control the group remotely, usually through a means such as IRC, and usually for nefarious purposes. Individual programs manifest as IRC "bots". Often the command and control takes place via an IRC server or a specific channel on a public IRC network. A bot typically runs hidden. Generally, the perpetrator of the botnet has compromised a series of systems using various tools (exploits, buffer overflows, as well as others). Newer bots can automatically scan their environment and propagate themselves using vulnerabilities and weak passwords. Generally, the more vulnerabilities a bot can scan and propagate through, the more valuable it becomes to a botnet controller community. Botnets have become a significant part of the Internet, albeit increasingly hidden. Often, a botnet will include a variety of connections, ranging from dial-up, ADSL and cable, and a variety of network types, including educational, corporate, government and even military networks. Sometimes, a controller will hide an IRC server installation on an educational or corporate site, where high-speed connections can support a large number of other bots.

---

## **Browser Hijacker**

A Browser hijacker is a form of malware or spyware that replaces the existing internet browser home page, error page, or search page with its own. These are generally used to force hits to a particular website.

---

## **Dialers**

Dialers are programs that set up your modem connection to connect to a 1-900 number. This provides the number's owner with revenue while leaving you with a large phone bill. There are some legitimate uses for dialers, such as for people who do not have access to credit cards. Most dialers, however, are installed quietly and attempt to do their dirty work without being detected.

---

## **Keystroke Logging**

Keystroke logging (often called keylogging) is a diagnostic used in software development that captures the user's keystrokes. It can be useful to determine sources of error in computer systems and is sometimes used to measure employee productivity on certain clerical tasks. Such systems are also highly useful for law enforcement and espionage—for instance, providing a means to obtain passwords or encryption keys and thus bypassing other security measures. However, keyloggers are widely available on the internet and can be used by anyone for the same purposes. Writing software applications for keylogging is trivial, and like any computer program can be distributed as a trojan horse or as part of a virus or worm.

---

## **Malware**

Malware is software designed to infiltrate or damage a computer system, without the owner's informed consent. It is commonly taken to include computer viruses, worms, Trojan horses, spyware and some adware.

---

## **Rootkit**

A rootkit is a set of software tools intended to conceal running processes, files or system data, thereby helping an intruder to maintain access to a system whilst avoiding detection. Rootkits are known to exist for a variety of operating systems. Rootkits often modify parts of the operating system or install themselves as drivers or kernel modules.

---

## **Spyware**

Spyware refers to a broad category of malicious software designed to intercept or take partial control of a computer's operation without the informed consent of that machine's owner or legitimate user. In simpler terms, spyware is a type of program that watches what users do with their computer and then sends that information over the internet. Spyware can collect many different types of information about a user. More malicious versions can try to record what a user types to try to intercept passwords or credit card numbers. Yet other versions simply launch popup advertisements.

---

## **Toolbars**

Toolbars plug into Internet Explorer and provide additional functionality such as search forms or pop-up blockers. Malware toolbars almost always include characteristics of the other malware categories, which is usually what gets it classified as malware. Any toolbar that is installed through underhanded means falls into the category of malware.

---

## **Trojan Horse**

A Trojan horse is a malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. There are two common types of Trojan horses. One, is otherwise useful software that has been corrupted by a cracker inserting malicious code that executes while the program is used. Examples include various implementations of weather alerting programs, computer clock setting software, and peer to peer file sharing utilities. The other type is a standalone program that masquerades as something else, like a game or image file, in order to trick the user into some misdirected complicity that is needed to carry out the program's objectives.

---

## **Virus**

In computer security, a computer virus is a self-replicating computer program that spreads by inserting copies of itself into other executable code or documents. A computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of a virus into the program is termed as an "infection", and the infected file, or executable code that is not part of a file, is called a "host". Viruses are one of the several types of malicious software or malware. In common parlance, the term virus is often extended to refer to worms, trojan horses and other sorts of malware. Viruses are intentionally destructive by destroying data. Some viruses have a delayed payload, which is sometimes called a bomb. For example, a virus might display a message on a specific day or wait until it has infected a certain number of hosts. A time bomb occurs during a particular date or time, and a logic bomb occurs when the user of a computer takes an action that triggers the bomb. The predominant negative effect of viruses is their uncontrolled self-reproduction, which wastes or overwhelms computer resources.

---

## **Worm**

A computer worm is a self-replicating computer program similar to a computer virus. A virus attaches itself to, and becomes part of, another executable program; however, a worm is self-contained and does not need to be part of another program to propagate itself. They are often designed to exploit the file transmission capabilities found on many computers. The main difference between a computer virus and a worm is that a virus cannot propagate by itself whereas worms can. A worm uses a network to send copies of itself to other systems and it does so without any intervention. In general, worms harm the network and consume bandwidth, whereas viruses infect or corrupt files on a targeted computer. Viruses generally do not affect network performance, as their malicious activities are mostly confined within the target computer itself.

---