Virus Glossary

Due to the confusion of terms used in Virus warnings, we include here ***McAfee's Glossary of Virus terminology***.

A B C D E F G H I J K L M N O P R S T U V W Z

ActiveX

- ActiveX controls are software modules based on Microsoft's Component Object Model (COM) architecture. They add functionality to software applications by seamlessly incorporating pre-made modules with the basic software package. Modules can be interchanged but still appear as parts of the original software.

  On the Internet, ActiveX controls can be linked to Web pages and downloaded by an ActiveX-compliant browser. ActiveX controls turn Web pages into software pages that perform like any other program launched from a server.

  ActiveX controls can have full system access. In most instances this access is legitimate, but one should be cautious of malicious ActiveX applications.

Back to Top

Algorithm

- A sequence of steps needed to solve logical or mathematical problems.
  Certain cryptographic algorithms are used to encrypt or decrypt data files and messages and to sign documents digitally.

Back to Top

Anti-antivirus Virus

- Anti-antivirus viruses attack, disable or infect specific anti-virus software. Also: Retrovirus

Back to Top

Anti-virus Software

- Anti-virus software scans a computer's memory and disk drives for viruses. If it finds a virus, the application informs the user and may clean, delete or quarantine any files, directories or disks affected by the malicious code. Also: Anti-virus Scanner

Back to Top

Antivirus Virus

- Antivirus viruses specifically look for and remove other viruses.

Back to Top

Applet

- Any miniature application transported over the Internet, especially as an enhancement to a Web page. Authors often embed applets within the HTML page as a foreign program type.

  Java applets are usually only allowed to access certain areas of the user's system. Computer programmers often refer to this area as the sandbox.

Back to Top

Armored Virus

- An armored virus tries to prevent analysts from examining its code. The virus may use various methods to make tracing, disassembling and reverse engineering its code more difficult.

Back to Top

ASCII

- American Standard Code for Information Interchange. Usually refers to coding system that assigns numerical values to characters such as letter, numbers, punctuation, and other symbols.

  Basic ASCII allows only 7 bits per character (for a total of 128 characters). The first 32 characters are "unprintable" (line feed, form feed, etc.). Extended ASCII adds an additional 128 characters that vary between computers, programs and fonts. Computers use these extra characters for accented letters, graphical characters or other special symbols.

ASCII Files

- ASCII files are usually text files consisting of only ASCII characters. With effort, it is possible to write program files consisting only of printable characters (See: EICAR Standard Anti-virus Test File). Windows batch (BAT) files and Visual Basic Script (See Also: Batch Files, VBS) files are also typically pure text, and program files.

  Because of the danger macro viruses can pose, using ASCII files in e-mail communications may by less risky. While it is possible for ASCII files to contain program code, and thus to contain viruses, ASCII files let you control both content and layout exactly, ensuring your e-mail is legible by the most e-mail programs.

Back to Top

Attack

- An attempt to subvert or bypass a system's security. Attacks may be passive or active. Active attacks attempt to alter or destroy data. Passive attacks try to intercept or read data without changing it. See Also: Brute Force Attack, Denial of Service, Hijacking, Password Attacks, Password Sniffing

Back to Top

Attributes

- Characteristics assigned to all files and directories. Attributes include: Read Only, Archive, Hidden or System.

Back to Top

Back Door

- A feature programmers often build into programs to allow special privileges normally denied to users of the program. Often programmers build back doors so they can fix bugs. If hackers or others learn about a back door, the feature may pose a security risk. Also: Trapdoor.

Back to Top

Back Orifice

- Back Orifice is a program developed and released by The Cult of the Dead Cow (cDc). It is not a virus; it is a remote administration tool with potential for malicious misuse. If installed by a hacker, it has the ability to give a remote attacker full system administrator privileges to your system. It can also 'sniff' passwords and confidential data and quietly e-mail them to a remote site. Back Orifice is an extensible program--programmers can change and "enhance" it over time. See Also: Password Sniffing

Back to Top

Background Scanning

- A feature in some anti-virus software to automatically scan files and documents as they are created, opened, closed or executed.

Back to Top

Background Task

- A task executed by the system but generally remain invisible to the user. The system usually assigns background tasks a lower priority than foreground tasks. Some malicious software is executed by a system as a background task so the user does not realize unwanted actions are occurring.

Backup

- n. A duplicate copy of data made for archiving purposes or for protecting against damage or loss.

  v. The process of creating duplicate data. Some programs backup data files while maintaining both the current version and the preceding version on disk. However, a backup is not considered secure unless it is stored away from the original.

Back to Top

Batch files

- Text files containing one MS-DOS command on each line of the file. When run, each line executes in sequential order. The batch file AUTOEXEC.BAT is executed when the computer is booted and loads a series of controls and programs. This file type has the extension BAT.

Back to Top

Bimodal virus

- A bimodal virus infects both boot records and files. Also: Bipartite; See Also: Boot Sector Infector, File Virus, Multipartite

Back to Top

BIOS

- Basic Input/Output System. The part of the operating system that identifies the set of programs used to boot the computer before locating the system disk.

  The BIOS is located in the ROM (Read Only Memory) area of system and is usually stored permanently.

Back to Top

Boot

- To start (a cold boot) or reset (warm boot) the computer so it is ready to run programs for the user. Booting the computer executes various programs to check and prepare the computer for use. See Also: Cold Boot, Warm Boot

Back to Top

Boot Record

- The program recorded in the boot sector. This record contains information on the characteristics and contents of the disk and information needed to boot the computer. If a user boots a PC with a floppy disk, the system reads the boot record from that disk. See Also: Boot Sector

Back to Top

Boot Sector

- An area located on the first track of floppy disks and logical disks that contain the boot record. Boot sector usually refers to this specific sector of a floppy disk, whereas the term Master Boot Sector usually refers to the same section of a hard disk. See Also: Master Boot Record

Boot Sector Infector

- A boot sector infector virus places its starting code in the boot sector. When the computer tries to read and execute the program in the boot sector, the virus goes into memory where it can gain control over basic computer operations. From memory, a boot sector infector can spread to other drives (floppy, network, etc.) on the system. Once the virus is running, it usually executes the normal boot program, which it stores elsewhere on the disk. Also: Boot Virus, Boot Sector Virus, BSI.

Back to Top

Brute Force Attack

- An attack in which each possible key or password is attempted until the correct one is found. See Also: Attack

Back to Top

BSI

- See: Boot Sector Infector

Bug

- An unintentional fault in a program that causes actions neither the user nor the program author intended.

Back to Top

Cavity Virus

- A cavity virus overwrites a part of its host file without increasing the length of the file while also preserving the host's functionality.

Back to Top

Checksum

- An identifying number calculated from file characteristics. The slightest change in a file changes its checksum.

Back to Top

Clean

- adj. A computer, file or disk that is free of viruses.
  v. To remove a virus or other malicious software from a computer, file or disk. Also: Disinfection.

Back to Top

Cluster Virus

- Cluster viruses modify the directory table entries so the virus starts before any other program. The virus code only exists in one location, but running any program runs the virus as well. Because they modify the directory, cluster viruses may appear to infect every program on a disk. Also: File System Virus

Back to Top

Cold Boot

- To start the computer by cycling the power. A cold boot using a rescue disk (a clean floppy disk with boot instructions and virus scanning capabilities) is often necessary to clean or remove boot sector infectors. See Also: Boot, Warm Boot

Back to Top

COM File

- A type of executable file limited to 64 kb. These simple files are often used for utility programs and small routines. Because COM files are executable, viruses can infect them. This file type has the extension COM.

Back to Top

Companion Virus

- Companion viruses use a feature of DOS that allows software programs with the same name, but with different extensions, to operate with different priorities. Most companion viruses create a COM file which has a higher priority than an EXE file with the same name.

  Thus, a virus may see a system contains the file PROGRAM.EXE and create a file called PROGRAM.COM. When the computer executes PROGRAM from the command line, the virus (PROGRAM.COM) runs before the actual PROGRAM.EXE. Often the virus will execute the original program afterwards so the system appears normal.

Back to Top

Compromise

- To access or disclose information without authorization.

Back to Top

Cookie

- Cookies are blocks of text placed in a file on your computer's hard disk. Web sites use cookies to identify users who revisit the site.

  Cookies might contain login or registration information, "shopping cart" information or user preferences. When a server receives a browser request that includes a cookie, the server can use the information stored in the cookie to customize the Web site for the user. Cookies can be used to gather more information about a user than would be possible without them.

Back to Top

Default Password

- A password on a system when it is first delivered or installed.

Back to Top

Denial Of Service (DoS)

- An attack specifically designed to prevent the normal functioning of a system and thereby to prevent lawful access to the system by authorized users. Hackers can cause denial of service attacks by destroying or modifying data or by overloading the system's servers until service to authorized users is delayed or prevented. See Also: Attack

Back to Top

Direct Action Virus

- A direct action virus works immediately to load itself into memory, infect other files, and then to unload itself.

Back to Top

Disinfection

- Most anti-virus software carries out disinfection after reporting the presence of a virus to the user. During disinfection, the virus may be removed from the system and, whenever possible, any affected data is recovered.

Back to Top

DOC File

- A Microsoft Word Document File. In the past, these files contained only document data, but with many newer versions of Microsoft Word, DOC files also include small programs called macros. Many virus authors use the macro programming language to associate macros with DOC files. This file type has the extension DOC.

Back to Top

DOS

- Disk Operating System. Generally any computer operating system, though often used as shorthand for MS-DOS--the operating system used by Microsoft before Windows was developed.

Back to Top

Dropper

- A dropper is carrier file that installs a virus on a computer system. Virus author often use droppers to shield their viruses from anti-virus software. The term injector often refers to a dropper that installs a virus only in memory.

Back to Top

EICAR

- European Institute of Computer Anti-Virus Research. In conjunction with several anti-virus software companies, EICAR has developed a test file for anti-virus software. See Also: EICAR Standard Anti-Virus Test File

Back to Top

EICAR Standard Anti-Virus Test File

- This text file consists of one line of printable characters; if saved as EICAR.COM, it can be executed and displays message: "EICAR-STANDARD-ANTIVIRUS-TEST-FILE!" This provides a safe and simple way of testing the installation and behavior of anti-virus software without using a real virus.

Back to Top

Encrypted Virus

- An encrypted virus's code begins with a decryption algorithm and continues with scrambled or encrypted code for the remainder of the virus. Each time it infects, it automatically encodes itself differently, so its code is never the same. Through this method, the virus tries to avoid detection by anti-virus software.

Back to Top

Encryption

- Encryption is the scrambling of data so it becomes difficult to unscramble and interpret.

Back to Top

EXE file

- An executable file; as contrasted with a document or data file. Usually, executed by double-clicking its icon or a shortcut on the desktop, or by entering the name of the program at a command prompt. Executable files can also be executed from other programs, batch files or various script files.

  The vast majority of known viruses infect program files. However, real-world infections by program-infecting viruses are much less common. Also: Program File

Back to Top

False Negative

- A false negative error occurs when anti-virus software fails to indicate an infected file is truly infected. False negatives are more serious than false positives, although both are undesirable. False negatives are more common with anti-virus software because the may miss a new or a heavily modified virus. See Also: False Positive

Back to Top

False Positive

- A false positive error occurs when anti-virus software wrongly claims a virus infects a clean file. False positives usually occur when the string chosen for a given virus signature is also present in another program. See Also: False Negative

Back to Top

Fast Infector

- Fast infector viruses, when active in memory, infect not only executed programs, but also those that are merely opened. Thus running an application, such as anti-virus software, which opens many programs but does not execute them, can result in all programs becoming infected. See Also: Slow Infector

Back to Top

FAT

- File Allocation Table. The under MS-DOS, Windows 3.x, 9x, and NT (in some cases), the FAT is located in the boot sector of the disk and stores the addresses of all the files contained on a disk. Viruses and other malicious programs, as well and normal use and extended wear and tear, can damage the FAT. If the FAT is damaged or corrupt, the operating system may be unable to locate files on the disk.

Back to Top

FDISK /MBR

- If you have MS-DOS version 5.0 or later, the command FDISK /MBR can remove viruses which infect the master boot sector but do not encrypt it. Using this command can produce unexpected results and cause unrecoverable damage.

Back to Top

File Viruses

- File viruses usually replace or attach themselves to COM and EXE files. They can also infect files with the extensions SYS, DRV, BIN, OVL and OVY.

  File viruses may be resident or non-resident, the most common being resident or TSR (terminate-and-stay-resident) viruses. Many non-resident viruses simply infect one or more files whenever an infected file runs.

  Also: Parasitic Virus, Fire Infector, File Infecting Virus

Back to Top

Firewall

- A firewall prevents computers on a network from communicating directly with external computer systems. A firewall typically consists of a computer that acts as a barrier through which all information passing between the networks and the external systems must travel. The firewall software analyzes information passing between the two and rejects it if it does not conform to pre-configured rules.

Back to Top

Good Times

- See: Virus Hoaxes

Back to Top

Heuristic Analysis

- Behavior-based analysis of a computer program by anti-virus software to identify a potential virus. Often heuristic scanning produces false alarms when a clean program behaves as a virus might. Also: Heuristic Scan

Back to Top

Hijacking

- An attack whereby an active, established, session is intercepted and used by the attacker. Hijacking can occur locally if, for example, a legitimate user leaves a computer unprotected. Remote hijacking can occur via the Internet.

Back to Top

Hole

- Vulnerability in the design software and/or hardware that allows circumvention of security measures.

Back to Top

Host

- A term often used to describe the computer file to which a virus attaches itself. Most viruses run when the computer or user tries to execute the host file.

Back to Top

In The Wild

- A virus is "in the wild" if it is verified as having caused an infection outside a laboratory situation. Most viruses are in the wild and differ only in prevalence. Also: ITW; See Also: Zoo Virus

Back to Top

Infection

- The action a virus carries out when it enters a computer system or storage device.

Back to Top

Injector

- See: Dropper

Back to Top

JavaScript

- JavaScript is a scripting language that can run wherever there is a suitable script interpreter such as Web browsers, Web servers, or the Windows Scripting Host. The scripting environment used to run JavaScript greatly affects the security of the host machine:

  A Web page with JavaScript runs within a Web browser in much the same way as Java applets and does not have access to host machine resources.

  An Active Server Page (ASP) or a Windows Scripting Host (WSH) script containing JavaScript is potentially hazardous since these environments allow scripts unrestricted access to machine resources (file system, registry, etc.) and application objects.

Back to Top

Joke Programs

- These are not viruses, but may contain a virus if infected or otherwise altered. Also: Practical Joke Programs

Back to Top

Key

- The Windows Registry uses keys to store computer configuration settings. When a user installs a new program or the configuration settings are otherwise altered, the values of these keys change. If viruses modify these keys, they can produce damaging effects.

Back to Top

Library File

- Library files contain groups of often-used computer code that different programs can share. Programmers who use library code make their programs smaller since they do not need to include the code in their program. A virus that infects a library file automatically may appear to infect any program using the library file.

  In Windows systems, the most common library file is the Dynamic Link Library; its extension is DLL.

Logic Bomb

- A logic bomb is a type of trojan horse that executes when specific conditions occur. Triggers for logic bombs can include a change in a file, by a particular series of keystrokes, or at a specific time or date. See: Time Bomb

Back to Top

Macro

- A macro is a series of instructions designed to simplify repetitive tasks within a program such as Microsoft Word, Excel or Access. Macros execute when a user opens the associated file. Microsoft's latest macro programming language is simple to use, powerful, and not limited to Word documents. Macros are in mini-programs and can be infected by viruses. See Also: Macro Virus

Back to Top

Macro Virus

- A macro virus is a malicious macro. Macro viruses are written a macro programming language and attach to a document file (such as Word or Excel). When a document or template containing the macro virus is opened in the target application, the virus runs, does its damage and copies itself into other documents. Continual use of the program results in the spread of the virus.

Back to Top

Mailbomb

- n. Excessively large e-mail (typically many thousands of messages) or one large message sent to a user's e-mail account, for the purpose of crashing the system, or preventing genuine messages from being received.

  v. To send a mailbomb.

Back to Top

Malicious Code

- A piece of code designed to damage a system or the data it contains, or to prevent the system from being used in its normal manner.

Back to Top

Malware

- A generic term used to describe malicious software such as: viruses, trojan horses, malicious active content, etc.

Back to Top

Mapped Drives

- Network drives assigned local drive letters and locally accessible. For example, the directory path \\MAIN\JohnDoe\ might be mapped as drive G: on a computer.

Back to Top

Master Boot Record

- The 340-byte program located in the master boot sector. This program reads the partition table, determines what partition to boot and transfers control to the program stored in the first sector of that partition. There is only one master boot record on each physical hard disk. Also: MBR, Partition Table; See Also: Boot Record

Back to Top

Master Boot Sector

- The first sector of a hard disk. This sector is located at sector 1, head 0, track 0. The sector contains the master boot record. See Also: Master Boot Record

Back to Top

Master Boot Sector Virus

- Master boot sector viruses infect the master boot sector of hard disks, though they spread through the boot record of floppy disks. The virus stays in memory, waiting for DOS to access a floppy disk. It then infects the boot record on each floppy disk DOS accesses. Also: Master Boot Record Virus; See Also: Boot Record

Back to Top

MBR

- See: Master Boot Record

Back to Top

Memory-resident Virus

- A memory-resident virus stays in memory after it executes and infects other files when certain conditions are met. In contrast, non-memory-resident viruses are active only while an infected application runs.

Back to Top

MP3 File

- Moving Picture Experts Group Audio Layer 3 File. MP3 files are highly compressed audio tracks, and are very popular on the Internet. MP3 files are not programs, and viruses cannot infect them. This file type has the extension MP3.

Back to Top

MS-DOS

- The Microsoft Disk Operating System. The operating system Microsoft developed for the IBM platform before Windows. Windows 3.x, 95 and 98 rely heavily on MS-DOS and can execute most MS-DOS commands.

Back to Top

Multipartite Virus

- Multipartite viruses use a combination of techniques including infecting documents, executables and boot sectors to infect computers. Most multipartite viruses first become resident in memory and then infect the boot sector of the hard drive. Once in memory, multipartite viruses may infect the entire system.

  Removing multipartite viruses requires cleaning both the boot sectors and any infected files. Before you attempt the repair, you must have a clean, write-protected Rescue Disk.

  Back to Top

Mutant

- See: Variant

Back to Top

Mutating Virus

- A mutating virus changes, or mutates, as it progresses through its host files making disinfection more difficult. The term usually refers to viruses that intentionally mutate, though some experts also include non-intentionally mutating viruses. See Also: Polymorphic Virus

Back to Top

Newsgroup

- An electronic forum where readers post articles and follow-up messages on a specified topic. An Internet newsgroup allows people from around the globe discuss common interests. Each newsgroup name indicates the newsgroup's subject in terms of increasingly narrow categories, such as alt.comp.virus.

Back to Top

Not In The Wild

- Viruses "not in the wild" are in real world but fail to spread successfully. See Also: In The Wild, Zoo Virus

Back to Top

NTFS:

- NT File System; a Windows NT file system used to organize and keep track of files. See Also: FAT

Back to Top

On-access Scanner

- A real-time virus scanner that scans disks and files automatically and often in the background. An on-access scanner scans files for viruses as the computer accesses the files.

Back to Top

On-demand Scanner

- A virus scanner the user starts manually. Most on-demand scanners allow the user to set various configurations and to scan specific files, folders or disks.

Back to Top

Operating System

- The operating system is usually the underlying software that enables you to interact with the computer. The operating system controls the computer storage, communications and task management functions. Examples of common operating stems include: MS-DOS, MacOS, Linux, Windows 98. Also: OS, DOS

Back to Top

Overwriting Virus

- An overwriting virus copies its code over its host file's data, thus destroying the original program. Disinfection is possible, although files cannot be recovered. It is usually necessary to delete the original file and replace it with a clean copy. Also: Overwrite Virus

Back to Top

Password Attacks

- A password attack is an attempt to obtain or decrypt a legitimate user's password. Hackers can use password dictionaries, cracking programs, and password sniffers in password attacks. Defense against password attacks is rather limited but usually consists of a password policy including a minimum length, unrecognizable words, and frequent changes. See Also: Password Sniffer

Back to Top

Password Sniffing

- The use of a sniffer to capture passwords as they cross a network. The network could be a local area network, or the Internet itself. The sniffer can be hardware or software. Most sniffers are passive and only log passwords. The attacker must then analyze the logs later. See Also: Sniffer

Back to Top

Payload

- Refers to the effects produced by a virus attack. Sometimes refers to a virus associated with a dropper or Trojan horse.

Back to Top

PGP

- Pretty Good Privacy. Considered the strongest program for encrypting data files and/or e-mail messages on PCs and Macintosh computers. PGP includes authentication to verify the sender of a message and non-repudiation to prevent someone denying they sent a message.

Back to Top

Piggyback

- To gain unauthorized access to a system via an authorized user's legitimate connection.

Back to Top

Polymorphic Virus

- Polymorphic viruses create varied (though fully functional) copies of themselves as a way to avoid detection from anti-virus software. Some polymorphic virus use different encryption schemes and requires different decryption routines. Thus, the same virus may look completely different on different systems or even within different files. Other polymorphic viruses vary instruction sequences and use false commands in the attempt to thwart anti-virus software. One of the most advanced polymorphic viruses uses a mutation-engine and random-number generators to change the virus code and its decryption routine. See Also: Mutating Virus

Back to Top

Program Infector

- A program infector virus infects other program files once an infected application is executed and the activated virus is loaded into memory.

Back to Top

Real-time Scanner

- An anti-virus software application that operates as a background task, allowing the computer to continue working at normal speed, with no perceptible slowing. See Also: On-Access Scanner

Back to Top

Redirect

- The action used by some viruses to point a command to a different location. Often this different location is the address of the virus and not the original file or application.

Back to Top

Rename

- The action by which a user or program assigns a new name to a file. Viruses may rename program files and take the name of the file so running the program inadvertently runs the virus.

  Anti-virus programs may rename infected files so the are unusable until they are manually cleaned or deleted.

Back to Top

Replication

- The process by which a virus makes copies of itself in order to carry out subsequent infections. Replication is one of major criteria separating viruses from other computer programs.

Back to Top

Reset

- To restart a computer without turning it off. Also: Warm Boot

Back to Top

Resident Virus

- A resident virus loads into memory and remains inactive until a trigger event. When the event occurs the virus activates, either infecting a file or disk, or causing other consequences. All boot viruses are resident viruses and so are the most common file viruses.

Back to Top

Resident Extension

- A resident extension is a memory-resident portion of a program that remains active after the program ends. It essentially becomes an extension to the operating system. Many viruses install themselves as resident extensions.

Back to Top

Rogue Program

- A term the media use to denote any program intended to damage programs or data, or to breach a system's security. It includes Trojan Horse programs, logic bombs, viruses, and more.

Back to Top

RTF File

- Rich Text Format File. An alternative format to the DOC file type supported by Microsoft Word. RTF files are ASCII text files and include embedded formatting commands. RTF files do not contain macros and cannot be infected with a macro virus.

This makes RTF files a good document format for communicating with others via e-mail. However, some macro viruses attempt to intercept saving a file as an RTF file and instead save it as a DOC file with an RTF extension. Users can catch this trick by first reading the file in a simple text editor like Notepad. DOC files will be nearly unreadable, while RTF files will be readable. This file type has the extension RTF. See Also DOC File

Back to Top

Scanner

- A virus detection program that searches for viruses. See Also: Anti-virus Software, On-demand Scanner, On-Access Scanner

Back to Top

Sector Viruses

- See: Boot Sector Infector, Master Boot Sector Virus

Back to Top

Self-encrypting Virus

- Self-encrypting viruses attempt to conceal themselves from anti-virus programs. Most anti-virus programs attempt to find viruses by looking for certain patterns of code (known as virus signatures) that are unique to each virus. Self-encrypting viruses encrypt these text strings differently with each infection to avoid detection. See Self-garbling Virus, Encrypted Virus

Back to Top

Self-extracting Files

- A self-extracting file decompresses part of itself into one or more parts when executed. Software authors and others often use this file type to transmit files and software via the Internet since the compressed files conserve disk space and reduce download time. Some anti-virus products may not search self-extracting file components. To scan these components, you must first extract the files and then scan them.

Back to Top

Self-garbling Viruses

- A self-garbling virus attempts to hide from anti-virus software by garbling its own code. When these viruses spread, they change the way their code is encoded so anti-virus software cannot find them. A small portion of the virus code decodes the garbled code when activated. See Also: Self-encrypting Virus, Polymorphic Virus

Back to Top

Shared Drive

- A disk drive available to other computers on the network. Shared drives use the Universal Naming Convention to differentiate themselves from other drives. See Also: Mapped Drives, UNC

Back to Top

Shareware

- Software distributed for evaluation without cost, but that requires payment to the author for full rights. If, after trying the software, you do not intend to use it, you simply delete it. Using unregistered shareware beyond the evaluation period is pirating.

Back to Top

Signature

- A search pattern, often a simple string of characters or bytes, expected to be found in every instance of a particular virus. Usually, different viruses have different signatures. Anti-virus scanners use signatures to locate specific viruses. Also: Virus Signatures

Back to Top

Slow Infector

- Slow infectors are active in memory and only infect new or modified files. See Also: Fast Infector

Back to Top

SMTP

- Simple Mail Transport Protocol. The Internet e-mail delivery format for transmitting e-mail messages between servers.

Back to Top

Sniffer

- A software program that monitors network traffic. Hackers use sniffers to capture data transmitted via a network.

Back to Top

Sparse Infector

- A sparse infector viruses use conditions before infecting files. Examples include files infected only on the 10th execution or files that have a maximum size of 128kb. These viruses use the conditions to infect less often and therefore avoid detection. Also: Sparse Virus

Back to Top

Stealth Virus

- Stealth viruses attempt to conceal their presence from anti-virus software. Many stealth viruses intercept disk-access requests, so when an anti-virus application tries to read files or boot sectors to find the virus, the virus feeds the program a "clean" image of the requested item. Other viruses hide the actual size of an infected file and display the size of the file before infection.

  Stealth viruses must be running to exhibit their stealth qualities. Also: Interrupt Interceptors

Back to Top

String

- A consecutive series of letters, numbers, and other characters. "afsH(*&@~" is a string; so is "The Mad Hatter". Anti-virus applications often use specific strings, called virus signatures, to detect viruses. See Also: Signature

Back to Top

System Boot Record

- See: Boot Record

Back to Top

Template

- Certain applications use template files to pre-load default configurations settings. Microsoft Word uses a template called NORMAL.DOT to store information about page setup, margins and other document information.

Back to Top

Time Bomb

- Usually malicious action triggered at a specific date or time. See Also: Logic Bomb

Back to Top

Timestamp

- The time of creation or last modification recorded on a file or another object. Users can usually find the timestamp in the Properties section of a file.

Back to Top

TOM

- Top of Memory. A design limit at the 640kb-mark on most PCs. Often the boot record does not completely reach top of memory, thus leaving empty space. Boot sector infectors often try to conceal themselves by hiding around the top of memory. Checking the top of memory value for changes can help detect a virus, though there is also non-viral reasons this value change.

Back to Top

Triggered Event

- An action built into a virus set off by a specific condition. Examples include a message displayed on a specific date or reformatting a hard drive after the 10th execution of a program.

Back to Top

Trojan Horse Program

- A Trojan horse program is a malicious program that pretends to be a benign application; a Trojan horse program purposefully does something the user does not expect. Trojans are not viruses since they do not replicate, but Trojan horse programs can be just as destructive.

  Many people use the term to refer only to non-replicating malicious programs, thus making a distinction between Trojans and viruses. Also: Trojan

Back to Top

TSR

- Terminate and Stay Resident. TSR programs stay in memory after being executed. TSR programs allow the user to quickly switch back and forth between programs in a non-multitasking environment, such as MS-DOS. Some viruses are TSR programs that stay in memory to infect other files and program. Also: Memory-resident Program

Back to Top

Tunneling

- A virus technique designed to prevent anti-virus applications from working correctly. Anti-virus programs work by intercepting the operating system actions before the OS can execute a virus. Tunneling viruses try to intercept the actions before the anti-virus software can detect the malicious code. New anti-virus programs can recognize many viruses with tunneling behavior.

Back to Top

UNC

- Universal Naming Convention. This is the standard for naming network drives. For example, UNC directory path has the following form: \\server\resource-pathname\subfolder\filename

Back to Top

Vaccination

- A technique of some anti-virus programs to store information about files in order to notify the user about file changes. Internal vaccines store the information within the file itself, while external vaccines use another file to verify the original for possible changes.

Back to Top

Variant

- A modified version of a virus. Usually produced on purpose by the virus author or another person amending the virus code. If changes to the original are small, most anti-virus products will also detect variants. However, if the changes are large, the variant may go undetected by anti-virus software.

Back to Top

VBS

- Visual Basic Script. Visual Basic Script is a programming language that can invoke any system function--including starting, using and shutting down other applications without--user knowledge. VBS programs can be embedded in HTML files and provide active content via the Internet. Since not all content is benign, users should be careful about changing security settings without understanding the implications. This file type has the extension VBS.

Back to Top

Virus

- A computer program file capable of attaching to disks or other files and replicating itself repeatedly, typically without user knowledge or permission. Some viruses attach to files so when the infected file executes, the virus also executes. Other viruses sit in a computer's memory and infect files as the computer opens, modifies or creates the files.

  Some viruses display symptoms, and some viruses damage files and computer systems, but neither symptoms nor damage is essential in the definition of a virus; a non-damaging virus is still a virus.

  There are computer viruses written for several operating systems including DOS, Windows, Amiga, Macintosh, Atari, and UNIX, and others. McAfee.com presently detects more than 57,000 viruses, Trojans, and other malicious software. (Note: The preferred plural is the English form: viruses)

  See Also: Boot Sector Infector, File Viruses, Macro virus, Companion Virus, Worm,

Back to Top

Virus Hoaxes

- Hoaxes are not viruses, but are usually deliberate or unintentional e-messages warning people about a virus or other malicious software program. Some hoaxes cause as much trouble as viruses by causing massive amounts of unnecessary e-mail.

  Most hoaxes contain one or more of the following characteristics:

  Warnings about alleged new viruses and its damaging consequences,
  Demands the reader forward the warning to as many people as possible,
  Pseudo-technical "information" describing the virus,
  Bogus comments from officials: FBI, software companies, news agencies, etc.

  If you receive an e-mail message about a virus, check with a reputable source to ensure the warning is real. Visit McAfee.com's Virus Hoax page (http://vil.mcafee.com/hoax.asp) to learn about hoaxes and the damage they cause. Sometimes hoaxes start out as viruses and some viruses start as hoaxes, so both viruses and virus hoaxes should be considered a threat.

Back to Top

Warm Boot

- Restarting a computer without first turning off the power. Using CTL+ALT+DEL or the reset button on many computers can warm boot a machine. See Also: Cold Boot, Reset

Back to Top

Windows Scripting

- Windows Scripting Host (WSH) is a Microsoft integrated module that lets programmers use any scripting language to automate operations throughout the Windows desktop.

Back to Top

Worm

- Worms are parasitic computer programs that replicate, but unlike viruses, do not infect other computer program files. Worms can create copies on the same computer, or can send the copies to other computers via a network. Worms often spread via IRC (Internet Relay Chat).

Back to Top

ZIP File

- ZIP Archive File. A ZIP archive contains compressed collections of other files. ZIP files are popular on the Internet because users can deliver multiple files in a single container; the compressed files also save disk space and download time. A ZIP file can contain viruses if any of the files packaged in it contain viruses, but the ZIP file itself is not directly dangerous. Other archive files include RAR, and LHA files. This file type has the extension ZIP.

Back to Top

Zoo

- A collection of viruses used for testing by researchers. See Also: In The Wild, Zoo Virus

Back to Top

Zoo Virus

- A zoo virus exists in the collections of researchers and has never infected a real world computer system. See Also: In The Wild

Back to Top