

# Glossary

This document provides a glossary of terms related to our application.

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

## A

**Access 97 macro virus** Affects MS Access 97 or later on any operating system. Written in VBA macro language.

**Address** Coded representation of the origin or destination of data.

**AppleScript worm** Is a script that uses the functionality of AppleScript to spread to other computers or scripts an email application to send itself out.

**ASCII** American Standard Code for Information Interchange - A seven-level code (128 possible characters) used for data transfer.

**Anonymous FTP** Downloading public files using the File Transfer Protocol (FTP). Called anonymous because you don't need to identify yourself before accessing files.

**Attachment** A file attached to an e-mail message.

**Anti-Virus Software** Scans computer's memory and disk drives for viruses. When it finds one, it informs you and allows you to clean, delete or quarantine files, directories or disks infected by it.

**Armored Virus** Tries to prevent analysis of its code.

**Attack** An attempt to compromise or bypass a system's security.

## B

**Batch file worm** Affects Computers connected to a network with DOS, Windows 95/98/Me and Windows NT/2000 operating systems. Spreads by searching for shared areas on remote computers to which it can copy itself.

**Bandwidth** Range of frequencies passing through a given circuit. Greater the bandwidth faster is the information sent or accessed through the circuit.

**Background scanning** Feature in some anti-virus software to automatically scan files and documents as they are created or run.

**Bit** Smallest unit of information in a binary system. Represents either a one or zero ("1" or "0").

**Bimodal Virus** Infects boot records and files.

**BIOS** (Basic Input/Output System) Part of the operating system that identifies a set of programs used to boot the computer before locating the system disk. It is located in the ROM and is usually stored permanently.

**Blended Threat** Combines characteristics of viruses, worms, Trojan horses, and malicious code with server and Internet vulnerabilities to attack the system. Uses multiple means to spread rapidly and cause widespread damage.

**Booting** Starting the computer. Booting runs various programs to check and prepare the computer for use.

**Boot Sector** Area on the first track of disk. Contains the boot record.

**Boot Record** Program in the boot sector. Contains information about characteristics and contents of the disk and booting the computer. If PC is booted with a floppy disk, the system reads the boot record from that disk.

**Boot Sector Virus** Places its code in the boot sector. When the computer tries to read and execute the program in the boot sector, the virus lodges itself in the PC memory and gains control over the PC. From here it spreads to other drives on the system. Once the virus is running, it usually executes the normal boot program, which it stores elsewhere on the disk.

**Bugs** Are not viruses but are unintentional errors in programs.

**Byte** A group of bits normally 8 bits in length.

## C

**Cavity Virus** Overwrites part of its host file without increasing the file size.

**Checksum** Identifying number calculated from file characteristics. Any change in a file changes the checksum.

**Cluster Virus** Changes directory table entries. Virus starts before other programs so they may appear to infect every program on a disk. Virus code exists in one location, but running any program runs the virus.

**Configure** To set up a program or computer system for a particular application.

. **COM Files** Executable file limited to 64 KB with the extension. COM. Used by utility programs and routines. As COM files are executable, viruses can infect them.

**Companion virus** Renames either itself or its target file to trick the user into running the virus rather than another program. For example, a companion virus attacking a file named MOVIE.EXE may rename the target file to MOVIE.EX and create a copy of itself called MOVIE.EXE.

**Corel Script virus** Affects Corel SCRIPT files. Uses Corel SCRIPT macro language.

**Crack** To copy commercial software illegally by breaking (cracking) the various copy protection and registration techniques being used.

**Client** Application that runs on a personal computer or workstation and relies on a server to perform some operations. For example, an e-mail client is an application that enables you to send and receive e-mail.

**Cluster** Is a logical disk-partitioning unit. A Cluster consists of one or several logical disk sectors, sequentially located. The Length of the cluster on floppy disks usually equals to 1 or 2, on hard disk - 4 or 8.

## D

**Daemon** Pronounced demon or damon. Is a process that runs in the background and performs specified operations at predefined times or in response to certain events. Typical daemon processes include print spoolers, e-mail handlers, and other programs that perform administrative tasks for the operating system. The term comes from Greek mythology, where daemons were guardian spirits.

**Denial of Service (DoS)** Attack preventing normal functioning of a system. Genuine users are denied access. Hackers can cause DoS attacks by destroying or modifying data or by overloading system's servers.

**Direct Action Virus** Immediately loads itself into the memory, infects other files, and then unloads itself.

**Distribution** Measure of how quickly a threat spreads

**Disassembler** A utility performing transformation, reverse to assembling, i.e. transforming machine codes to assembler language. Such utilities are required not only for debugging programs but also for virus analysis.

**Downloads** Process of copying a file from an online service to one's own computer. Also refers to copying a file from a network file server to a computer on the network. The opposite of download is upload, which means to copy a file from your own computer to another computer.

**Dropper** A file created specifically to introduce a virus, worm or Trojan into a system. The file may be different type from the virus, worm or Trojan it introduces.

## E

**Encryption Virus** Its code begins with a decryption algorithm and continues with scrambled or encrypted code. Each time it infects, it automatically encodes itself differently, so its code is never the same.

**e-mail** Name that identifies an electronic post office box on a network where e-mail can be sent.

**e-mail Client** Application that runs on a personal computer or workstation and enables you to send, receive and organize e-mail. Called a client because e-mail systems are based on client-server architecture.

**Exploit** Program or technique that takes advantage of vulnerability in software that can be used for breaking security or otherwise attacking a host over the network.

**Excel formula virus** Affects MS Excel 5 or later running on any operating system. Uses Excel formula language. When an infected document is opened the viral formula sheet is copied into a

file in the XLSTART directory. This is automatically loaded into other documents when they are opened.

**.EXE Files** Executable file. Run by double-clicking its icon or a shortcut on the desktop, or by entering the program name at a command prompt. Are also run from other programs, batch files or various script files.

## F

**False Negative Error** Occurs when the anti-virus software fails to indicate an infected file is really infected.

**False Positive Error** Occurs when the anti-virus software wrongly claims a clean file is infected. Error occur when the string chosen for a given virus signature is also present in another program.

**FAT** (File Allocation Table) Stores the addresses of all the files contained on a disk. In MS-DOS and Windows the FAT is located in the boot sector of the disk. Viruses and normal use can damage the FAT. If damaged or corrupt, the operating system is unable to locate files on the disk.

**File Viruses** Replace or attach themselves to COM and EXE files. They also infect files with extensions: SYS, DRV, BIN, OVL and OVY. They can be resident or non-resident, the most common being resident or TSR (terminate-and-stay-resident) viruses. Many non-resident viruses infect other files when an infected file runs.

**Firewall** A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. A firewall is considered a first line of defense in protecting private information.

**FTP** (File Transfer Protocol) Protocol used to send files on the Internet.

## G

**Gateway** Points of entrance and exit from a communications network. Viewed as a physical entity, a gateway is the node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture.

## H

**Heuristic Scanning** Behavior-based analysis of a computer program by anti-virus software to identify a potential virus. Anti Virus software sends alerts when a file has suspicious code or content.

**Hijack** An attack where an active and legitimate session is intercepted and taken over. Remote hijacking can occur via the Internet.

**Host** File to which a virus attaches itself. Virus is launched when the host file is run.

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

**Http** (Hypertext Transfer Protocol) Main protocol used by the World Wide Web. Defines how messages are formatted and transmitted, and what actions Web servers and browsers should take in response to various commands. For example, when you enter a URL in your browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page.

## I

**Internet Address** Also known as an IP address. Is a 32-bit hardware-independent address assigned to hosts using the TCP/IP protocol suite.

**Infection Length** Size of viral code inserted into a program by a virus. If it is a worm or Trojan horse the length represents the file size.

**IP** (Internet Protocol) Networking protocol for providing connectionless services to the higher transport protocol. It is responsible for discovering and maintaining topology information and for routing packets across homogeneous networks. Combined with TCP, it is commonly known as the TCP/IP platform.

**IP Address** Uniquely identifies each host on a network or Internet.

## J

**JavaScript virus** Affects JavaScript scripting files, HTML files with embedded scripts, Microsoft Outlook and Internet Explorer.

**Joke Programs** These are not viruses, but may contain a virus if infected or otherwise altered.

## K

**Keys** The Windows Registry uses keys to store computer configuration settings. When a new program is installed or the configuration settings are altered, values of these keys change. Virus modifies these keys and cause damages.

## L

**LAN** (Local Area Network) Network that interconnects devices over a geographically small area, typically in one building or part of a building. The most popular LAN type is Ethernet, a 10 Mbps standard that works with 10BaseT, 10Base2, or 10Base5 cables.

**Library File** Contains groups of frequently used computer code shared by different programs. Developers use these codes to make their programs smaller. A virus infecting a library file may appear to infect any program using the library file. In Windows systems, the most common library file is the Dynamic Link Library with extension .DLL.

**Linux worm** Take advantage of flaws in networking code to gain unauthorized access to remote computers running Linux. They can spread rapidly between computers permanently connected to the Internet because they require no user intervention to function.

**Log On** To make a computer system or network recognize you so that you can begin a computer session. Most personal computers have no log-on procedure -- you just turn the machine on and begin working. For larger systems and networks, however, you usually need to enter a username and password before the computer system will allow you to execute programs.

## M

**Macro** Set of mini programs that simplify repetitive tasks within a program such as Microsoft Word, Excel or Access. Macros run when a user opens the associated file. Viruses can infect macros.

**Macintosh file virus** Infect Macintosh computers.

**Mailbomb** Many e-mails (thousands of messages) or one large message, sent to the system to make it crash.

**Master Boot Record** A 340-byte program in the master boot sector. It 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.

**Master Boot Sector** First sector of a hard disk located at sector 1, head 0, and track 0. Contains the master boot record.

**Master Boot Sector Virus** Infects the master boot sector of hard disks. They spread through the boot record of floppy disks. The virus stays in memory and infects the boot record of floppy read by DOS.

**Mid infecting** A prefix to denote viruses that infect the middle of a file.

**Mime** (Multipurpose Internet Mail Extensions) Specification for formatting non-ASCII messages so that they can be sent over the Internet. Many e-mail clients now support MIME, which enables them to send and receive graphics, audio, and video files via the Internet mail system. In addition, MIME supports messages in character sets other than ASCII.

**MPEG** (Moving Picture Experts Group) Pronounced m-peg is a working group of ISO. Term refers to the family of digital video compression standards and file formats developed by the group. MPEG generally produces better-quality video than competing formats, such as Video for Windows, Indeo and QuickTime. MPEG files can be decoded by special hardware or software.

**Multipartite Virus** Infect documents, executables and boot sectors. They first become resident in system memory and then infect the boot sector of the hard drive and the entire system.

**Mutating Virus** Changes or mutates as it runs through its host files. Disinfection is more difficult.

**MWL** (MicroWorld Winsock Layer) Anti Virus and content security concept introduced and used by MicroWorld technologies Inc. MWL is placed above the Winsock layer and acts as a secure blanket between the Internet and your system. Any type of data exchanged through your system is monitored by MWL. This stops potential threats from entering your system. While other products allow threats to enter your system and then try to diffuse them, MWL technology has the key advantage of barring them from entering.

## N

**Network** Group of computers connected to each other within an organization. Organization may be spread across a wide geographical area.

## O

**Operating System** The underlying software that allows you to interact with the computer. It controls the computer storage, communications and task management functions. Examples: MS-DOS, MacOS, Linux, Windows 98, UNIX etc.

**Overwriting Virus** Copies its code over the host file's data destroying the original program. Disinfections are possible, although files cannot be recovered. It is usually necessary to delete the original file and replace it with a clean copy.

## P

**Payload** Defines extent of damage caused by a virus.

**Port** Interface of a computer from where an application or physical devices connect.

**Protocol** Formal set of conventions governing the formatting and relative timing of message exchange between two communicating systems.

**POP** (Post Office Protocol) Protocol used to retrieve e-mails from a mail server. Most e-mail applications (sometimes called an e-mail client) use the POP protocol, although some can use the newer IMAP (Internet Message Access Protocol).

**Password** Secret series of characters that enables a user to access a file, computer, or program. Password can be a combination of numbers and alphabets in a random sequence.

**Polymorphic Virus** Creates varied copies of itself to avoid detection from anti-virus software. Some use different encryption schemes and require different decryption routines. So 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 to mislead anti-virus software. Some use mutation-engines and random-number generators to change their virus code and decryption routine.

**Program Infector** Infects other program files after an infected application is run.

## Q

**Quarantine** To move an infected file, such as a virus, into an area where it cannot cause more harm. Antivirus software's come with quarantine options so that the user also can keep track of virus activity.

## R

**Register** Storage device capable of receiving and holding a number of digits

**Real-time Scanner** An anti-virus software application that operates as a background task. Computer continues working at normal speed.

**Resident Virus** Loads into memory and remains inactive until a trigger event occurs like date or time. When this event occurs the virus is activated. All boot and file viruses are of this type.

**Removal** Measure of skill level needed to remove the threat. The three levels are difficult (requires an experienced technician), moderate (requires some expertise), and easy (requires little or no expertise).

**Rogue Program** Malicious program intended to damage programs or data, or to breach system security. It includes Trojans, logic bombs, viruses etc.

## S

**Scalable** Allows to be changed in size or configuration to suit changing conditions. For example, a scalable network can be expanded from a few nodes to thousands of nodes.

**Self-encrypting Virus** 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.

**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.

**Signature** A search pattern, often a simple string of characters or bytes, expected in every instance of a particular virus. Usually, different viruses have different signatures. Anti-virus scanners use signatures to locate specific viruses.

**Sparse-infector Virus** Uses conditions before infecting files. Examples include files infected only on the 12th execution or files of 128kb.

**Stealth Virus** 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.

**Subject of e-mail** Indicates the subject line of the email sent by the worm.

**Synchronous Transmission** Transmission in which data bits are sent at a fixed rate, with the transmitter and receiver synchronized.

**SMTP** (Simple Mail Transfer Protocol) Protocol for sending e-mail messages between servers. Most e-mail systems that send mail over the Internet use SMTP to send messages from one server to another; the messages can then be retrieved with an e-mail client using either POP or IMAP. In addition, SMTP is generally used to send messages from a mail client to a mail server. This is why you need to specify both the POP or IMAP server and the SMTP server when you configure your e-mail application.

**Spam** Electronic junk mail, junk newsgroup postings or unsolicited mail.

## T

**TCP/IP** (Transmission Control Protocol/Internet Protocol) – Also known also as the Internet protocol suite. Combines both TCP and IP. Widely used applications, such as Telnet, FTP and SMTP, interface to TCP/IP.

**Technical Description** Describes technical details of the virus such as registry entry modifications and files that are manipulated by the virus.

**Threat Assessment** Gives severity rating of the threat. Includes damage that the threat causes, how quickly it can spread and how widespread the infections are known to be (wild).

**Threat Containment** Measure of how well current Anti virus technology can keep the threat from spreading. The measures are Easy (the threat is well-contained), Moderate (the threat is partially contained), and Difficult (the threat is not currently containable).

**Time Bomb** Malicious action triggered at a specific date or time.

**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 here. Checking the TOM value for changes can help detect a virus. The value can change for non-viral reasons also.

**Trojan Destructive** program that masquerades as a benign application. Unlike viruses, Trojans do not replicate themselves but they can be just as destructive. One of the most insidious types is a program that claims to rid your computer of viruses but instead introduces viruses onto your computer.

**TSR** (Terminate and Stay Resident) TSR programs stay in memory after being executed. Allow 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.

**Tunneling** 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.

## U

**User Name** Name used to gain access to a computer system. Usernames, and often passwords, are required in multi-user systems. In most such systems, users can choose their own usernames and passwords.

**UNC** (Universal Naming Convention) Is the standard for naming network drives. For example, UNC directory path has the following form: \\server\microworld\subfolder\filename.

**Unix worm** Takes advantage of flaws in networking code called buffer overflows to gain unauthorized access to remote computers running Unix.

## V

**Vaccination** Technique of some anti-virus programs to store information about files in order to notify 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.

**Variant** Modified version of a virus. Usually produced on purpose by the virus author or person amending the virus code. If changes to the original are small, most anti-virus products will also detect variants. If the changes are major, the variant may be undetected by anti-virus software.

**Virus** Program or piece of code that is loaded onto your computer without your knowledge and runs against your wishes. Viruses can also replicate themselves. All computer viruses are manmade. A simple virus that can make a copy of itself over and over again is relatively easy to produce. Even such a simple virus is dangerous because it will quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems.

**Virus Signature** A unique string of bits, or the binary pattern, of a virus. The virus signature is like a fingerprint in that it can be used to detect and identify specific viruses. Anti-virus software uses the virus signature to scan for the presence of malicious code.

**Vulnerability** Characteristic of a system that will allow someone to keep it from operating correctly, or that will let unauthorized users take control of the system.

## W

**WAN** (Wide Area Network) Network that typically spans nationwide distances and usually utilizes public telephone networks.

**WinSock** (Windows Socket) Is an Application Programming Interface (API) for developing Windows programs that can communicate with other machines via the TCP/IP protocol. Windows 95 and Windows NT comes with Dynamic Link Library (DLL) called winsock.dll that implements the API and acts as the glue between Windows programs and TCP/IP connections.

**Wild** Measures the extent to which a virus is spreading. Asses number of independent sites and systems infected, geographic distribution of infection, ability of current technology to combat the threat, and the complexity of the virus. When a virus has attacked an external system it is termed as being 'in the wild'.

**Worm** A program or algorithm that replicates itself over a computer network and usually performs malicious actions, such as using up the computer's resources and possibly shutting the system down.

## X

**XML** (Extensible Markup Language) A specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.

## Y

**Yankee Doodle** Type of memory resident virus. Plays the tune Yankee Doodle when activated.

## Z

**Zombie** A computer that has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner. Zombies are used by malicious hackers to launch DoS attacks. The hacker sends commands to the zombie through an open port. On command, the zombie computer sends an enormous amount of packets of useless information to a targeted Web site in order to clog the site's routers and keep legitimate users from gaining access to the site. The traffic sent to the Web site is confusing and therefore the computer receiving the data spends time and resources trying to understand the influx of data that has been transmitted by the zombies.

**Zoo** Collection of viruses used for testing by researchers.

**Zoo Virus** Exists in the collections of researchers.