A

access (noun) To read data from or write data to a storage device, such as a computer or server.

access (verb) Authorization to read or write data. Most operating systems allow you to define different levels of access, depending on job responsibilities.

action

(Also see target and notification) The operation to be performed when:
—a virus or other threat has been detected, or
—file blocking has been triggered.
Actions typically include clean, delete, or pass (deliver/transfer anyway). Delivering/transferring anyway is not recommended—delivering a risk-infected message can compromise your network.

activate To enable your Trend Micro InterScan for Cisco CSC SSM software during the installation process by entering the Activation Code (on the Activation Codes Configuration window). Until the product is installed and activated, the SSM is not operable.

Activation Code A 37-character code, including hyphens, that is used to activate Trend Micro InterScan for Cisco CSC SSM. Here is an example of an Activation Code: SM-9UE2-HD4B3-8577B-TB5P4-Q2XT5-48PY4

ActiveUpdate A Trend Micro utility that enables on-demand or background updates to the virus pattern file and scan engine, spyware/grayware pattern file, PhishTrap pattern file, anti-spam rules, and anti-spam engine.

ActiveX A type of open software architecture that implements object linking and embedding, enabling some of the standard interfaces, such as downloading of Web pages.

ActiveX malicious code An ActiveX control is a component object embedded in a Web page which runs automatically when the page is viewed. ActiveX controls allow Web developers to create interactive, dynamic Web pages with broad functionality such as HouseCall, Trend Micro's free online scanner.

Hackers, virus writers, and others who want to cause mischief or worse may use ActiveX malicious code as a vehicle to attack the system. In many cases, the Web browser can be configured so that these ActiveX controls do not execute by changing the browser's security settings to “high.”

address Refers to a networking address (see IP address) or an email address, which is the string of characters that specify the source or destination of an email message.

administrator Refers to “system administrator”—the person in an organization who is responsible for activities such as setting up new hardware and software, allocating user names and passwords, monitoring disk space and other IT resources, performing backups, and managing network security.

administrator account A user name and password that has administrator-level privileges.

administrator email address The address used by the administrator of Trend Micro InterScan for Cisco CSC SSM to manage notifications and alerts.

adware Advertising-supported software in which advertising banners display while the program is running. Adware that installs a “backdoor”; tracking mechanism on the user's computer without the user's knowledge is called “spyware.”

anti-spam Refers to a filtering mechanism, designed to identify and prevent delivery of advertisements, pornography, and other “nuisance” mail.

anti-spam rules and engine The Trend Micro tools used to detect and filter spam.

antivirus Computer programs designed to detect and clean computer viruses.

approved sender A sender whose messages are always allowed into your network.

archive A single file containing one or (usually) more separate files plus information to allow them to be extracted (separated) by a suitable program, such as a .zip file.

ASDM Adaptive Security Device Manager.

attachment A file attached to (sent with) an email message.

audio/video file A file containing sounds, such as music, or video footage.

authentication The verification of the identity of a person or a process. Authentication ensures that digital data transmissions are delivered to the intended receiver. Authentication also assures the receiver of the integrity of the message and its source (where or whom it came from).

The simplest form of authentication requires a user name and password to gain access to a particular account. Authentication protocols can also be based on secret-key encryption, such as the Data Encryption Standard (DES) algorithm, or on public-key systems using digital signatures.

Also see public-key encryption *and* digital signature.

B

binary A number representation consisting of zeros and ones used by practically all computers because of its ease of implementation using digital electronics and Boolean algebra.

block To prevent entry into your network.

blocked sender A sender whose messages are never allowed to enter your network.

boot sector virus A boot sector virus is a virus targeted at the boot sector (the operating system) of a computer. Computer systems are most likely to be attacked by boot sector viruses when you boot the system with an infected disk from the floppy drive—the boot attempt does not have to be successful for the virus to infect the hard drive.

Also, there are a few viruses that can infect the boot sector from executable programs. These are known as multi-partite viruses and they are relatively rare. Once the system is infected, the boot sector virus attempts to infect every disk that is accessed by that computer. In general, boot sector viruses can be successfully removed.

browser A program which allows a person to read hypertext, such as Internet Explorer or Mozilla. The browser gives some means of viewing the contents of nodes (or "pages") and of navigating from one node to another. A browser acts as a client to a remote Web server.

C

cache A small fast portion of memory, holding recently accessed data, designed to speed up subsequent access to the same data. The term is most often applied to processor-memory access, but also applies to a local copy of data accessible over a network etc.

case-matching Scanning for text that matches both words and case. For example, if "dog" is added to the content-filter, with case-matching enabled, messages containing "Dog" pass through the filter; messages containing "dog" do not.

cause The reason a protective action, such as URL-blocking or file-blocking, was triggered—this information appears in log files.

clean To remove virus code from a file or message.

CLI Command Line Interface. See Reimaging and Configuring the CSC SSM Using the Command Line, page A-1 for more information.

client A computer system or process that requests a service of another computer system or process (a "server") using some kind of protocol and accepts the server's responses. A client is part of a client-server software architecture.

client-server environment A common form of distributed system in which software is split between server tasks and client tasks. A client sends requests to a server, according to protocol, asking for information or action, and the server responds.

compressed file A single file containing one or more separate files plus information to allow them to be extracted by a suitable program, such as WinZip.

configuration Selecting options for how Trend Micro InterScan for Cisco CSC SSM functions, for example, selecting whether to pass or delete a virus-infected email message.

content filtering Scanning email messages for content (words or phrases) prohibited by your organization's Human Resources or IT messaging policies, such as hate mail, profanity, or pornography.

content violation An event that has triggered the content filtering policy.

CSC SSM console The Trend Micro InterScan for Cisco CSC SSM user interface.

D

daemon A program that is not invoked explicitly, but lies dormant waiting for some condition(s) to occur. The perpetrator of the condition need not be aware that a daemon is lurking.

damage routine The destructive portion of virus code, also called the payload.

default A value that pre-populates a field in the CSC SSM console interface. A default value represents a logical choice and is provided for convenience. Use default values as-is, or change them.

dialer A type of Trojan that when executed, connects the user's system to a pay-per-call location in which the unsuspecting user is billed for the call without his or her knowledge.

digital signature Extra data appended to a message which identifies and authenticates the sender and message data using a technique called public-key encryption. *Also see* public-key encryption *and* authentication.

disclaimer A statement appended to the beginning or end of an email message, that states certain terms of legality and confidentiality regarding the message, To see an example, click the online help for the **SMTP Configuration - Disclaimer** window.

DNS Domain Name System—A general-purpose data query service chiefly used on the Internet for translating host names into IP addresses.

DNS resolution When a DNS client requests host name and address data from a DNS server, the process is called resolution. Basic DNS configuration results in a server that performs default resolution. For example, a remote server queries another server for data on a machine in the current zone. Client software on the remote server queries the resolver, which answers the request from its database files.

domain name The full name of a system, consisting of its local host name and its domain name, such as example.com. A domain name should be sufficient to determine a unique Internet address for any host on the Internet. This process, called “name resolution,” uses the Domain Name System (DNS).

DoS (Denial of Service) attack Group-addressed email messages with large attachments that clog your network resources to the point where messaging service is noticeably slow or even stopped.

DOS virus Also referred to as “COM” and “EXE file infectors.” DOS viruses infect DOS executable programs-files that have the extensions *.COM or *.EXE. Unless they have overwritten or inadvertently destroyed part of the original program's code, most DOS viruses try to replicate and spread by infecting other host programs.

download (noun) Data that has been downloaded, for example, from a Web site via HTTP.

download (verb) To transfer data or code from one computer to another. Downloading often refers to transfer from a larger “host” system (especially a server or mainframe) to a smaller “client” system.

dropper Droppers are programs that serve as delivery mechanisms to carry and drop viruses, Trojans, or worms into a system.

E

ELF Executable and Linkable Format—An executable file format for Unix and Linux platforms.

encryption Encryption is the process of changing data into a form that can be read only by the intended receiver. To decipher the message, the receiver of the encrypted data must have the proper decryption key. In traditional encryption schemes, the sender and the receiver use the same key to encrypt and decrypt data. Public-key encryption schemes use two keys: a public key, which anyone may use, and a corresponding private key, which is possessed only by the person who created it. With this method, anyone may send a message encrypted with the owner's public key, but only the owner has the private key necessary to decrypt it. PGP (Pretty Good Privacy) and DES (Data Encryption Standard) are two of the most popular public-key encryption schemes.

EULA (end user license agreement) An End User License Agreement or EULA is a legal contract between a software publisher and the software user. It typically outlines restrictions on the side of the user, who can refuse to enter into the agreement by not clicking “I accept” during installation. Clicking “I do not accept” ends the installation of the software product.

Many users inadvertently agree to the installation of spyware and adware into their computers when they click “I accept” on EULA prompts displayed during the installation of certain free software.

executable file A binary file containing a program in machine language which is ready to be executed (run).

EXE file infector An executable program with an .exe file extension. *Also see* DOS virus.

exploit An exploit is code that takes advantage of a software vulnerability or security hole. Exploits are able to propagate into and run intricate routines on vulnerable computers.

F

false positive An email message that was “caught” by the spam filter and identified as spam, but is actually not spam.

FAQ Frequently Asked Questions—A list of questions and answers about a specific topic.

file An element of data, such as an email message or HTTP download.

file infecting virus File-infecting viruses infect executable programs (generally, files that have extensions of .com or .exe). Most such viruses simply try to replicate and spread by infecting other host programs, but some inadvertently destroy the program they infect by overwriting a portion of the original code. A minority of these viruses are very destructive and attempt to format the hard drive at a pre-determined time or perform some other malicious action.

In many cases, a file-infecting virus can be successfully removed from the infected file. However, if the virus has overwritten part of the program's code, the original file is unrecoverable.

file type The kind of data stored in a file. Most operating systems use the file name extension to determine the file type. The file type is used to choose an appropriate icon to represent the file in a user interface, and the correct application with which to view, edit, run, or print the file.

filename extension The portion of a file name (such as .txt or .xml) which typically indicates the kind of data stored in the file. Apart from informing the user what type of content the file holds, file name extensions are typically used to decide which program to launch when a file is run.

filter criteria User-specified guidelines for determining whether a message and attachment(s), if any, are delivered, such as:
—size of the message body and attachment
—presence of words or text strings in the message subject
—presence of words or text strings in the message body
—presence of words or text strings in the attachment subject
—file type of the attachment

firewall A gateway machine with special security precautions on it, used to service outside network (especially Internet) connections and dial-in lines.

FTP A client-server protocol which allows a user on one computer to transfer files to and from another computer over a TCP/IP network. Also refers to the client program the user executes to transfer files.

G

gateway An interface between an information source and a Web server.

grayware A category of software that may be legitimate, unwanted, or malicious. Unlike threats such as viruses, worms, and Trojans, grayware does not infect, replicate, or destroy data, but it may violate your privacy. Examples of grayware include spyware, adware, and remote access tools.

group file type Types of files that have a common theme. There are five group file types in the Trend Micro InterScan for Cisco CSS SSM interface, they are:
—Audio/Video
—Compressed
—Executable
—Images
—Microsoft Office

GUI Graphical User Interface—The use of pictures rather than just words to represent the input and output of a program. This contrasts with a command-line interface where communication is by exchange of strings of text.

H

hacker *See* virus writer

hacking tool Tools such as hardware and software that enables penetration testing of a computer system or network for the purpose of finding security vulnerabilities that can be exploited.

header Part of a data packet that contains transparent information about the file or the transmission.

heuristic rule-based scanning Scanning network traffic, using a logical analysis of properties that reduces or limits the search for solutions.

HTML virus A virus targeted at HTML (Hyper Text Markup Language), the authoring language used to create information in a Web page. The virus resides in a Web page and downloads via a user's browser.

HTTP Hypertext Transfer Protocol—The client-server TCP/IP protocol used on the World Wide Web for the exchange of HTML documents. It conventionally uses port 80.

HTTPS HTTP over SSL—A variant of HTTP used for handling secure transactions.

host A computer connected to a network.

I

ICSA ICSA Labs is an independent division of TruSecure Corporation. For over a decade, ICSA has been the security industry's central authority for research, intelligence, and certification testing of products. ICSA Labs sets standards for information security products and certifies over 90% of the installed base of antivirus, firewall, IPSec, crytography, and PC firewall products in the world today.

image file A file containing data representing a two-dimensional scene, in other words, a picture. Images are taken from the real world, for example, via a digital camera, or they may be generated by computer using graphics software.

incoming Email messages or other data routed *into* your network.

IntelliScan IntelliScan is a Trend Micro scanning technology that examines file headers using true file type recognition, and scans only file types known to potentially harbor malicious code. True file type recognition helps identify malicious code that can be disguised by a harmless extension name.

Internet A client-server hypertext information retrieval system, based on a series of networks connected with routers. The Internet is a modern information system and a widely accepted medium for advertising, online sales, and services, as well as university and many other research networks. The World Wide Web is the most familiar aspect of the Internet.

in the wild Describes known viruses that are currently controlled by antivirus products. *Also see* "in the wild."

in the zoo Describes known viruses that are actively circulating. *Also see* "in the zoo."

interrupt An asynchronous event that suspends normal processing and temporarily diverts the flow of control through an "interrupt handler" routine.

intranet Any network which provides similar services within an organization to those provided by the Internet outside it, but which is not necessarily connected to the Internet.

IP Internet Protocol—*See* IP address.

IP address Internet address for a device on a network, typically expressed using dot notation such as 10.123.123.123.

IT Information technology, to include hardware, software, networking, telecommunications, and user support.

J

Java applets Java applets are small, portable Java programs embedded in HTML pages that can run automatically when the pages are viewed. Java applets allow Web developers to create interactive, dynamic Web pages with broader functionality.

Authors of malicious code have used Java applets as a vehicle for attack. Most Web browsers, however, can be configured so that these applets do not execute—sometimes by simply changing browser security settings to "high."

Java file Java is a general-purpose programming language developed by Sun Microsystems. A Java file contains Java code. Java supports programming for the Internet in the form of platform-independent Java "applets." (An applet is a program written in Java programming language that can be included in an HTML page. When you use a Java-technology enabled browser to view a page that contains an applet, the applet's code is transferred to your system and is executed by the browser's Java Virtual Machine.)

Java malicious code Virus code written or embedded in Java. *Also see* Java file.

JavaScript virus JavaScript is a simple programming language developed by Netscape that allows Web developers to add dynamic content to HTML pages displayed in a browser using scripts. Javascript shares some features of Sun Microsystems Java programming language, but was developed independently.

A JavaScript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user's desktop through the user's browser.

Also see VBscript virus.

K

KB Kilobyte—1024 bytes of memory.

keylogger Keyloggers are programs that catch and store all keyboard activity. There are legitimate keylogging programs that are used by corporations to monitor employees and by parents to monitor their children. However, criminals also use keystroke logs to sort for valuable information such as logon credentials and credit card numbers.

L

license Authorization by law to use Trend Micro InterScan for Cisco CSC SSM.

link (also called hyperlink) A reference from some point in one hypertext document to some point in another document or another place in the same document. Links are usually distinguished by a different color or style of text, such as underlined blue text. When you activate the link, for example, by clicking on it with a mouse, the browser displays the target of the link.

listening port A port utilized for client connection requests for data exchange.

load balancing Load balancing is the mapping (or re-mapping) of work to processors, with the intent of improving the efficiency of a concurrent computation.

logic bomb Code surreptitiously inserted into an application or operating system that causes it to perform some destructive or security-compromising activity whenever specified conditions are met.

M

macro A command used to automate certain functions within an application.

MacroTrap A Trend Micro utility that performs a rule-based examination of all macro code that is saved in association with a document. macro virus code is typically contained in part of the invisible template that travels with many documents (.dot, for example, in Microsoft Word documents). MacroTrap checks the template for signs of a macro virus by seeking out key instructions that perform virus-like activity—instructions such as copying parts of the template to other templates (replication), or instructions to execute potentially harmful commands (destruction).

macro virus Unlike other virus types, macro viruses aren't specific to an operating system and can spread via email attachments, Web downloads, file transfers, and cooperative applications.

malware (malicious software) Programming or files that are developed for the purpose of doing harm, such as viruses, worms, and Trojans.

mass mailer (also known as a worm) A malicious program that has high damage potential, because it causes large amounts of network traffic.

match case *See* case-matching.

MB Megabyte—1024 kilobytes of data.

Mbps Millions of bits per second—a measure of bandwidth in data communications.

message An email message, which includes the message subject in the message header, and the message body.

message size The number of KB or MB occupied by a message and its attachments.

message subject The title or topic of an email message, such as “Third Quarter Results” or “Lunch on Friday.”

Microsoft Office file Files created with Microsoft Office tools such as Excel or Microsoft Word.

mixed threat attack Complex attacks that take advantage of multiple entry points and vulnerabilities in enterprise networks, such as the “Nimda” or “Code Red” threats.

multi-partite virus A virus that has characteristics of both boot sector viruses and file-infecting viruses.

N

NAT device — Network Address Translation device—A device that allows organizations to use unregistered IP network numbers internally and still communicate well with the Internet. The purpose is typically to enable multiple hosts on a private network to access the Internet using a single public IP address; a feature called private addressing.

network virus — A type of virus that uses network protocols, such as TCP, FTP, UDP, HTTP, and email protocols to replicate. Network viruses often do not alter system files or modify the boot sectors of hard disks. Instead, they infect the memory of client machines, forcing them to flood the network with traffic, which can cause slowdowns or even complete network failure.

notification

(Also see action and target) — A message that is forwarded to one or more of the following:
—system administrator
—sender of a message
—recipient of a message, file download, or file transfer
The purpose of the notification is to communicate that a prohibited action has taken place, or was attempted, such as a virus being detected in an attempted HTTP file download.

NRS (Network Reputation Service) — Network Reputation Services (NRS) is a method of spam filtering that allows you to off-load the task from the MTA to the SCS SSM. The IP address of the originating MTA is checked against a database of IP addresses.

NTP — Network Time Protocol—A time-keeping protocol for synchronizing clocks of computer systems over a data network.

O

offensive content — Words or phrases in messages or attachments that are considered offensive to others, for example, profanity, sexual harassment, racial harassment, or hate mail.

online help — Documentation that is bundled with the GUI

open relay — An open mail relay is an SMTP (e-mail) server configured to allow anyone on the Internet to relay or send e-mail through it. Spammers can use an open relay to send spam messages.

outgoing — Email messages or other data *leaving* your network, routed out to the Internet.

P

parameter — A variable, such as a range of values (a number from 1 to 10).

password cracker — An application program that is used to recover a lost or forgotten password. These applications can also be used by an intruder to gain unauthorized access to a computer or network resources.

pattern file (also known as Official Pattern Release) The pattern file, as referred to as the Official Pattern Release (OPR), is the latest compilation of patterns for identified viruses. It is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. This pattern file is most effective when used with the latest scan engine.

payload Payload refers to an action that a virus performs on the infected computer. This can be something relatively harmless, such as displaying messages or ejecting the CD drive, or something destructive, such as deleting the entire hard drive.

phishing Phishing is a rapidly growing form of fraud that seeks to fool Web users into divulging private information by mimicking a legitimate Web site.

ping Pinging is a diagnostic tool used on TCP/IP networks that allows you to verify whether a connection from one host to another is working. See Ping IP, page A-14, for information about pinging from the command-line interface.

polymorphic virus A virus that is capable of taking different forms.

POP3 Post Office Protocol, version 3—A messaging protocol that allows a client computer to retrieve electronic mail from a server via a temporary connection, for example, a mobile computer without a permanent network connection.

POP3 server A server which hosts POP3 email, from which clients in your network retrieve POP3 messages.

port A logical channel or channel endpoint in a communications system, used to distinguish between different logical channels on the same network interface on the same computer. Each application program has a unique port number associated with it.

proxy A process providing a cache of items available on other servers which are presumably slower or more expensive to access.

proxy server A World Wide Web server which accepts URLs with a special prefix, used to fetch documents from either a local cache or a remote server, then returns the URL to the requester.

public-key encryption An encryption scheme where each person gets a pair of “keys,” called the public key and the private key. Each person's public key is published while the private key is kept secret. Messages are encrypted using the intended recipient's public key and can only be decrypted using his or her private key. *Also see* authentication *and* digital signature.

Q

queue A data structure used to sequence multiple demands for a resource when mail is being received faster than it can be processed. Messages are added at the end of the queue, and are taken from the beginning of the queue, using a FIFO (first-in, first-out) approach.

R

recipient The person or entity to whom an email message is addressed.

remote access tool Hardware and software that allow a legitimate system administrator to manage a network remotely. However, these same tools can also be used by intruders to attempt a breach of your system security.

replicate To self-reproduce. As used in this documentation, the term refers to viruses or worms that can self-reproduce.

ROMMON ROM monitor program. ROMMON is executed from ROM and is a single-threaded program that initializes a board and loads a higher-level operating system. ROMMON is for debugging or to manually boot the system.

rule-based spam detection Spam detection based on heuristic evaluation of message characteristics for determining whether an email message should be considered spam. When the anti-spam engine examines an email message, it searches for matches between the mail contents and the entries in the rules files. Rule-based spam detection has a higher catch rate than signature-based spam detection, but it also has a higher false positive rate as well.
Also see signature-based spam detection.
Also see false positive.

S

scan To examine items in a file in sequence to find those that meet a particular criteria.

scan engine The module that performs antivirus scanning and detection in the host product to which it is integrated.

script A set of programming commands that, once invoked, can be executed together. Other terms used synonymously with “script” are “macro” or “batch file.”

seat A license for one person to use Trend Micro InterScan for Cisco CSC SSM.

Secure Password Authentication An authentication process, by which communications can be protected, using for example, encryption and challenge/response mechanisms.

security Security refers to techniques for ensuring that data stored in or transferred via a computer cannot be accessed by unauthorized individuals. Methods for achieving system security are typically data encryption and passwords.

sender The person who is sending an email message to another person or entity.

server A program which provides some service to other (client) programs. The connection between client and server is normally by means of message passing, often over a network, and uses some protocol to encode the client's requests and the server's responses. The server may run continuously (as a daemon), waiting for requests to arrive, or it may be invoked by some higher-level daemon which controls a number of specific servers.

setup wizard The setup program used to install Trend Micro InterScan for Cisco CSC SSM. You can install using:
—A GUI setup wizard, launched from the ASDM (see the ASDM online help for details), or
—A command-line interface (see Reimaging and Configuring the CSC SSM Using the Command Line, page A-1, for more information)

signature-based spam detection — A method of determining whether an email message is spam by comparing the message contents to entries in a spam database. An exact match must be found for the message to be identified as spam. Signature-based spam detection has a nearly zero false positive rate, but does not detect "new" spam that isn't an exact match for text in the spam signature file.
Also see rule-based spam detection.
Also see false positive.

SMTP — Simple Mail Transfer Protocol—A protocol used to transfer electronic mail between computers, usually over Ethernet. It is a server-to-server protocol, so other protocols are used to access the messages.

SOCKS4 — A protocol that relays TCP (transmission control protocol) sessions at a firewall host to allow application users transparent access across the firewall.

spam — Unsolicited email messages meant to promote a product or service.

SSL — Secure Sockets Layer—A secure communications protocol on the Internet.

spyware — Advertising-supported software that typically installs tracking software on your system, capable of sending information about you to another party. The danger is that users cannot control what data is being collected, or how it is used.

stamp — To place an identifier, such as "Spam," in the subject field of an email message.

status bar — A feature of the user interface, that displays the status or progress of a particular activity, such as loading of files on your machine.

T

TAC — Technical Assistance Center

target (Also see action and notification) — The scope of activity to be monitored for a violating event, such as a virus being detected in an email message. For example, you could target virus scanning of all files passing into and out of your network, or just files with a certain file name extension.

TCP/IP — Transmission Control Protocol/Internet Protocol—TCP is a networking protocol, most commonly use in combination with IP (Internet Protocol), to govern connection of computer systems to the Internet.

TELNET — The Internet standard protocol for remote login that runs on top of TCP/IP (Transmission Control Protocol/Internet Protocol). This term can also refer to networking software that acts as a terminal emulator for a remote login session.

TFTP — Trivial File Transfer Protocol is a simple file transfer protocol used to read files from or write files to a remote server.

top-level domain (tld) — The last and most significant component of an Internet fully qualified domain name, the part after the last ".". For example, host *wombat.doc.ic.ac.uk* is in top-level domain "uk" (for United Kingdom).

traffic — Data flowing between the Internet and your network, both incoming and outgoing.

trigger An event that causes an action to take place. For example, Trend Micro InterScan for Cisco CSC SSM detects a virus in an email message. This *triggers* the message to be placed in quarantine, and a notification to be sent to the system administrator, message sender, and message recipient.

Trojan horse A malicious program that is disguised as something benign. A Trojan is an executable program that does not replicate, but instead, resides on a system to perform malicious acts, such as opening a port for an intruder.

true file type Used by IntelliScan, a virus scanning technology, to identify the type of information in a file by examining the file headers, regardless of the file name extension (which could be misleading).

trusted domain A domain from which Trend Micro InterScan for Cisco CSC SSM always accepts messages, without considering whether the message is spam. For example, a company called Example, Inc. has a subsidiary called Example-Japan, Inc. Messages from example-japan.com are always accepted into the example.com network, without checking for spam, since the messages are from a known and trusted source.

trusted host A server that is allowed to relay mail through your network because they are trusted to act appropriately and not, for example, relay spam through your network.

U

UDP A protocol in the TCP/IP protocol suite, the User Datagram Protocol or UDP allows an application program to send datagrams to other application programs on a remote machine. Basically UDP is a protocol that provides an unreliable and connectionless datagram service where delivery and duplicate detection are not guaranteed. It does not use acknowledgments, or control the order of arrival.

URL Uniform Resource Locator—A standard way of specifying the location of an object, typically a Web page, on the Internet, for example, *www.cisco.com*. The URL maps to an IP address using DNS.

V

VBscript virus VBscript (Microsoft Visual Basic scripting language) is a simple programming language that allows Web developers to add interactive functionality to HTML pages displayed in a browser. For example, developers might use VBscript to add a “Click Here for More Information” button on a Web page.

A VBscript virus is a virus that is targeted at these scripts in the HTML code. This enables the virus to reside in Web pages and download to a user’s desktop through the user’s browser.

Also see JavaScript virus.

virus A computer virus is a program – a piece of executable code – that has the unique ability to infect and replicate. Like biological viruses, computer viruses can spread quickly and are often difficult to eradicate.

In addition to replication, some computer viruses share another commonality: a damage routine that delivers the virus payload. While payloads may only display messages or images, they can also destroy files, reformat your hard drive, or cause other damage. Even if the virus does not contain a damage routine, it can cause trouble by consuming storage space and memory, and degrading the overall performance of your computer.

virus kit A template of source code for building and executing a virus, available from the Internet.

virus signature A virus signature is a unique string of bits that identifies a specific virus. Virus signatures are stored in the Trend Micro virus pattern file. The Trend Micro scan engine compares code in files, such as the body of an email message, or the content of an HTTP download, to the signatures in the pattern file. If a match is found, the virus is detected, and is acted upon (for example, cleaned, deleted, or quarantined) according to your security policy.

virus trap Software that helps you capture a sample of virus code for analysis.

virus writer Another name for a malicious computer hacker, someone who writes virus code.

W

Web The World Wide Web, also called the Web or the Internet.

Web server A server process running at a Web site which sends out Web pages in response to HTTP requests from remote browsers.

wildcard In Trend Micro InterScan for Cisco CSC SSM, the term is used in reference to content filtering, where an asterisk (*) represents any characters. For example, in the expression *ber, this expression can represent barber, number, plumber, timber, and so on. The term originates from card games, in which a specific card, identified as a “wildcard,” can be used for any number or suit in the card deck.

workstation (also known as client) A general-purpose computer designed to be used by one person at a time and which offers higher performance than normally found in a personal computer, especially with respect to graphics, processing power and the ability to carry out several tasks at the same time.

worm A self-contained program (or set of programs) that is able to spread functional copies of itself or its segments to other computer systems.

Z

zip file A compressed archive (in other words, “zip file”) from one or more files using an archiving program such as WinZip.

Zip of Death A zip (or archive) file of a type that when decompressed, expands enormously (for example 1000%) or a zip file with thousands of attachments. Compressed files must be decompressed during scanning. Huge files can slow or stop your network.