GLOSSARY

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 The operation to be performed when the following has occurred:
- A virus or other threat has been detected.
- File blocking has been triggered.

Actions usually include clean, delete, or pass (deliver or transfer anyway). Delivering or transferring anyway is not recommended; delivering a risk-infected message can compromise your network.

See also notification.

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. An example of an activation code is: 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 or 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 that runs automatically when the page is viewed. ActiveX controls allow web developers to create interactive, dynamic web pages with broad functionality, such as HouseCall, the Trend Micro free online scanner.

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

address Refers to a networking address or an e-mail address, which is the string of characters that specifies the source or destination of an e-mail message.

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

administrator account A username and password that has administrator-level privileges.

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

ADSP AppleTalk Data Stream Protocol, part of the AppleTalk protocol suite, which provides a TCP-style reliable connection-oriented transport. This protocol is full duplex.

adware Advertising-supported software in which advertising banners display while the program is running. Adware that installs a "backdoor" tracking mechanism on a computer without user 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.

audio or 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 username 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.

See also public-key encryption and digital signature.

B

binary A numerical representation consisting of zeros and ones used by most 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, certain viruses 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 that allows a person to read hypertext, such as Internet Explorer or Mozilla Firefox. The browser provides a way to view the contents of nodes (or "pages") and to move from one node to another. A browser acts as a client to a remote web server.

C

cache A small, yet fast portion of memory, holding recently accessed data, which is 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.

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. For more information, see Reimaging and Configuring the CSC SSM Using the CLI, page A-1.

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 responses. A client is part of a client-server software architecture.

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

compressed file A single file containing one or more separate files and 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 e-mail message.

content filtering Scanning e-mail messages for content (words or phrases) prohibited by 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 certain 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 a system to a pay-per-call location in which the unsuspecting user is unknowingly billed for the call.

digital signature Extra data appended to a message that identifies and authenticates the sender and message data using a technique called public-key encryption.

See also public-key encryption and authentication.

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

DNS Domain Name System. A general-purpose data query service used on the Internet to translate hostnames into IP addresses.

DNS resolution When a DNS client requests hostname 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 hostname 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 DNS.

Denial of Service (DoS) attack Group-addressed e-mail messages with large attachments that clog your network resources to the point that 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, which are files that have the these extensions. Unless they have overwritten or inadvertently destroyed part of the original program code, most DOS viruses try to replicate and spread by infecting other host programs.

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

E

ELF Executable and Linkable Format, a file format for UNIX and Linux platforms.

encryption 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 only by the person who created it has. With this method, anyone may send a message encrypted with the 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 common public-key encryption schemes.

end user license agreement (EULA) A legal contract between a software publisher and the software user, which outlines user restrictions.

Many users inadvertently agree to the installation of spyware and adware on their computers when they the EULA that appears during the installation of certain free software.

executable file A binary file containing a program in machine language that is ready to be executed.

EXE file infector An executable program with an .exe file extension.

See also DOS virus.

exploit Code that takes advantage of a software vulnerability or security hole. Exploits can propagate and run intricate routines on vulnerable computers.

F

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

file infecting virus File-infecting viruses infect executable programs (files that have extensions of .com or .exe). Most viruses 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. Some viruses are very destructive and try to format the hard drive at a predetermined time or perform other malicious actions.

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

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, message body, or attachment subject
- File type of the attachment

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

FTP A client-server protocol that 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; however, 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. The five group file types in the Trend Micro InterScan for Cisco CSS SSM interface are as follows:
- Audio/Video
- Compressed
- Executable
- Images
- Microsoft Office

GUI Graphical User Interface. The use of pictures rather than words alone to represent the input and output of a program.

H

hacker See virus writer.

hacking tool Tools such as hardware and software that enable penetration testing of a computer system or network to find 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, the authoring language used to create information that appears on a web page. The virus resides in a web page and downloads through a browser.

HTTP Hypertext Transfer Protocol. The client-server TCP/IP protocol used on the web through port 80 to render HTML documents.

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 central authority for research, intelligence, and certification testing of products for the security industry. 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, that is, a picture. Images are taken from the real world, for example, via a digital camera or by a computer using graphics software.

incoming E-mail 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, for university and many other research networks. The web is the most familiar aspect of the Internet.

in the wild Describes known viruses that are currently controlled by antivirus products.

in the zoo Describes known viruses that are actively circulating.

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

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

IP Internet Protocol.

IT Information technology, which includes 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 on the web. 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—often by 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-enabled browser to view a page that contains an applet, the applet code is transferred to your system and is executed by the Java Virtual Machine in the browser.

Java malicious code Virus code written or embedded in Java.

See also Java file.

JavaScript virus JavaScript is a 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 targets these scripts in the HTML code, which enables the virus to reside in web pages and download to a desktop computer through the browser.

See also VBscript virus.

K

keylogger Keyloggers are programs that catch and store all keyboard activity. Legitimate keylogging programs 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 log-on credentials and credit card numbers.

L

link (also called hyperlink) A reference from one point in one hypertext document to another 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 it with a mouse, the browser displays the target of the link.

listening port A port used in client connection requests for data exchange.

load balancing Mapping or remapping of work to processors to improve 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 usually 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 are not specific to an operating system and can spread via e-mail attachments, web downloads, file transfers, and cooperative applications.

malware (malicious software) Programming or files that are developed to do 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.

message An e-mail message, which includes the message subject in the message header and the message body.

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 that allows organizations to use unregistered IP network numbers internally and still communicate with the Internet. Use this device 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 e-mail 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 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 Services is a method of spam filtering that allows you to off-load the task from the MTA to the CSC 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.

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.

P

password cracker An 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. This file is guaranteed to have passed a series of critical tests to ensure that you get optimum protection from the latest virus threats. The file is most effective when used with the latest scan engine.

payload An action that a virus performs on the infected computer, which can be relatively harmless, such as displaying messages or ejecting the CD drive, or 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 website.

ping A diagnostic tool used on TCP/IP networks that allows you to verify whether a connection from one host to another is working. For more information, see Pinging an IP Address, page A-17.

polymorphic virus A virus that can take different forms.

POP3 Post Office Protocol, 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 that hosts POP3 e-mail, from which clients in your network retrieve POP3 messages.

proxy A service that provides a cache of items available on other servers that are slower or more expensive to access.

proxy server A web server that accepts URLs with a special prefix, which is used to retrieve 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 public key is published, while the private key is kept secret. Messages are encrypted using the recipient public key and can only be decrypted using the private key.

See also authentication and digital signature.

R

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 system security.

replicate To self-reproduce. 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 use to debug or to boot the system manually.

rule-based spam detection Spam detection based on heuristic evaluation of message characteristics to determine whether an e-mail message should be considered spam. When the anti-spam engine examines an e-mail message, the engine searches for matches between the mail content 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.

See also signature-based spam detection and false positive.

S

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

seat A license for a single user 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.

setup wizard The setup program used to install Trend Micro InterScan for Cisco CSC SSM, which can be one of the following:

- A GUI setup wizard, launched from the ASDM. For more information, see the ASDM online help.
- A CLI. For more information, see Reimaging and Configuring the CSC SSM Using the CLI, page A-1.

signature-based spam detection A method of determining whether an e-mail message is spam by comparing the message content 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 is not an exact match for text in the spam signature file.

See also rule-based spam detection and false positive.

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

SOCKS4 A protocol that relays TCP sessions to a firewall host to allow transparent access across the firewall to application users.

spam Unsolicited e-mail messages to promote a product or service.

SSL Secure Sockets Layer, a secure communications protocol on the Internet.

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

stamp To place an identifier, such as "Spam," in the subject field of an e-mail message.

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

T

TAC Technical Assistance Center, a support service that Cisco provides to users of Cisco products.

TCP/IP Transmission Control Protocol/Internet Protocol, a networking protocol commonly used in combination with the 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. 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 the top-level domain "uk" (for United Kingdom).

trigger An event that causes an action to take place. For example, Trend Micro InterScan for Cisco CSC SSM detects a virus in an e-mail message, which 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. 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, because the messages are from a known and trusted source.

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

U

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

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

V

VBscript virus Microsoft Visual Basic scripting language is a programming language that allows web developers to add interactive functionality to HTML pages displayed in a browser.

A VBscript virus targets these scripts in the HTML code, which enables the virus to reside in web pages and download to a desktop through the browser.

See also JavaScript virus.

virus 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 a 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 a computer.

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

virus signature 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 e-mail 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 the defined 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 website that distributes 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 character.

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 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 a network.