CompTIA Security+ SY0-701 Certification

Glossary of Malware Terms

Thank you for choosing this guide! This comprehensive resource has been designed to summarize and explain key terms from the glossary of malware, helping you better understand various threats and cybersecurity concepts for the CompTIA Security+ SY0-701 exam.

It provides detailed explanations of each term, referencing the official study materials and including tips for exam success.

While this resource is an excellent starting point and reference for your exam preparation, please note that it does not substitute the official book and other primary resources. Instead, it serves to clarify and reinforce key concepts, offering a deeper understanding of the exam objectives, backed by official sources and practical advice to help you succeed on your first attempt.

I aim to make these notes accessible to everyone. If you find them helpful, your support through tips/comments or contributions is always appreciated.
It enables me to continue creating high-quality study materials.

✓ Check this post for access to additional valuable resources, such as correct questions with explanations, a glossary, and study methods to help you pass the exam: linkedin.com/in/matteoschirinzi

Comment & like the post of Sec+ resource with your experience: linkedin.com/in/matteoschirinzi

Thank you for your support and good luck on your journey to earning the CompTIA Security+ certification!

Malware-related terms explicitly mentioned in the CompTIA Security+ SY0-701 exam objectives are marked in red.

ActiveX controls

A type of downloadable web browser plug-ins for Microsoft Internet Explorer providing additional interactive features to web pages. Malicious ActiveX controls pose a risk of unintended execution of malware.

Adware

Software that automatically plays, displays, or downloads advertisements to a computer.

Armored virus

A type of computer virus that takes advantage of various mechanisms specifically designed to make tracing, disassembling and reverse engineering its code more difficult.

Backdoor

An undocumented (and often legitimate) way of gaining access to a program, online service, or an entire computer system.

Bloatware

A type of pre-installed, typically unwanted software that consumes system resources and provides little to no value to the user.

Bot

A malware-infected networked host under remote control of a hacker.

Botnet

A group of compromised computers running malicious software under control of a hacker.

Buffer overflow

A technique used by certain types of malware to cause an error in a program and make it easier to run malicious code.

Command and Control (C2 or C&C) server

A computer controlled by an attacker used to send commands to systems compromised by malware.

Companion virus

An older type of computer virus which does not alter files and works by creating infected companion file with the exact same name as the legitimate program, but with different file extension. The virus takes advantage of the fact that in the old MS-DOS command-line interface executables can be run by providing only the file name which facilitates the execution of infected code by an unaware user.

Cross-site scripting

A computer security vulnerability allowing attackers to insert malicious code into a trusted website.

Cryptomalware

Malware that restricts access to a computer system by encrypting data.

Dialer

A rogue application designed to exploit dialup connections by making unauthorized telephone calls.

Downloader

A type of Trojan designed to transfer other malware onto a PC via Internet connection.

Drive-by download

An automatic download performed without the user's consent (and often without any notice) aimed at installing malware or potentially unwanted programs.

Dropper

A type of Trojan designed to install other malware files onto a PC without the need for an active Internet connection.

Executable file

A type of computer file that when opened runs a program or series of instructions contained in the file.

Exploit

Computer code or command that takes advantage of software design flaws.

Fileless Virus

A type of virus that resides only in Random-Access Memory (RAM).

Grayware

A category of applications which, despite not being classified as malware, can worsen the performance of a computer and pose security risk.

Heuristics

A method employed by many computer antivirus programs designed to detect previously unknown types of malware.

iframe

An HTML tag for embedding another web document within the current HTML web page. The downside of utilizing iframes relates to the fact that they can be used for the purpose of injecting malicious code (often in the form of JavaScript applet) into an otherwise trusted page.

Keylogger

An application collecting information about user keyboard activity. Typically, malicious keyloggers are installed and run on a system without the user's knowledge/consent to steal logon credentials, credit card numbers, and other sensitive data.

Logic bomb

Malicious code activated by a specific event.

Macro virus

A type of computer virus that exploits the capability for creating and embedding simple scripts in popular office and cooperative applications.

Malicious app

Mobile application designed to harm user devices or personal data acting in disguise of a legitimate program.

Malicious update

A type of malware that can be installed through a seemingly legitimate software update. The introduction of a malicious update into the application code can be enabled through various means, including unsigned application code, unencrypted update channel (HTTP vs HTTPS), fake update website, unauthorized access to update server, or compromised software development process.

Malicious USB cable

A deceptive hardware accessory that appears normal but contains hidden functionalities designed to compromise connected devices or steal data.

Malware

A generic term for various types of malicious software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. The category of malware encompasses all sorts of malicious applications, including Trojan horses, most rootkits and backdoors, computer viruses, worms, spyware, keyloggers, more intrusive forms of adware, and other malicious programs.

Payload

The part of malware performing malicious action.

Phage virus

A type of computer virus that deletes or corrupts the contents of the target host file instead of attaching itself to the file.

Polymorphic malware

A type of malicious software capable of changing its underlying code in order to avoid detection.

Pop-under

One of the ways of delivering online advertising content utilized by adware. Advertising pop-unders are usually displayed in a new browser window hidden beneath the current page and are not seen until the covering window is closed.

Pop-up

One of the ways of delivering online advertising content utilized by adware. Advertising pop-ups are usually displayed in a new web browser window and cover the contents of the current page.

Potentially Unwanted Program (PUP)

A computer program not explicitly classified as malware by an antivirus software. Although PUPs are legal apps typically downloaded and installed with the user's consent, they may adversely affect computer's security and performance, compromise user's privacy, or cause nuisance by displaying unsolicited ads.

Quarantine

The process of isolating files and applications suspected of containing malware to prevent further execution and potential harm to the user's system.

Ransomware

Malware that restricts access to a computer system by encrypting files or locking the entire system down until the user performs the requested action.

Remote Access Trojan (RAT)

A type of Trojan that enables unauthorized remote access to a compromised system.

Replication

The process by which a virus makes copies of itself to carry out subsequent infections.

Retrovirus

A computer virus that actively attacks an antivirus program in an effort to prevent detection.

Rootkit

A collection of software tools used by a hacker in order to mask intrusion and obtain administrator-level access to a computer or computer network.

Sandboxing

A mechanism for safe execution of untested code or untrusted applications.

Signature file

A file containing new malicious code patterns used by the antivirus application as a reference in the process of malware removal.

Spyware

Malicious software collecting information about users without their knowledge/consent.

SQL injection

Execution of SQL commands aimed at gaining unauthorized access to an online database. This type of attack occurs when, for example, entry fields of web forms designed to collect information from users allow passing unchecked user input to the database. The countermeasure against this type of code injection is input validation, which limits the scope of user input that can be passed through an online form.

Trojan horse

Malicious software performing unwanted and harmful actions in disguise of a legitimate and useful program.

Virus

A computer program containing malicious segment that attaches itself to an application program or other executable component.

Windows Defender

A built-in application tool for Microsoft operating systems providing protection against viruses, spyware, and other potentially unwanted programs.

Worm

A standalone malicious computer program that replicates itself over a computer network.

XSS

A shorthand term for cross-site scripting.

Zero-day attack

A type of attack exploiting vulnerabilities that are present in already released software but unknown to the software developer.

Zombie

A computer compromised by a virus or Trojan horse that puts it under the remote control of an online hijacker.