

Forum:[Hack Forums](#)

Thread: [\[MRT-X Academy\] Security & Anti-Malware Terminology](#)

Tha Sneak - January 30, 2025, 12:56 am

Security & Anti-Malware Terminology

Introduction

When analyzing antivirus or anti-malware logs, you may encounter various abbreviations and security-related terms. This guide provides a detailed reference for understanding these terms. While this is not an exhaustive list, it covers common security and malware-related terminology to enhance your understanding.

Anti-Malware Terminology

Common Malware Classifications & Abbreviations

Antivirus and anti-malware programs often use abbreviations to classify threats. Below are common threat types and their corresponding shorthand notations.

Trojan (Troj) – A type of malware disguised as legitimate software to trick users into executing it.

Virus (Vir) – A self-replicating program that spreads by infecting files.

Malware – Any software designed to cause harm to a system.

Rootkit – Malware that hides its presence and gains deep system access.

Worm – A self-replicating malware that spreads over networks.

Adware (Adw) – Software that displays unwanted advertisements.

Spyware – Malware designed to monitor user activity and steal information.

Keylogger – Malware that records keystrokes to steal credentials.

Bootkit – A type of rootkit that infects the boot sector.

Backdoor – Malware that allows remote access to a compromised system.

Ransomware – Encrypts user files and demands ransom for decryption.

Other Malware Categories

Banker Trojan – Malware designed to steal banking credentials.

Browser Helper Object Infection (BHO) – Malicious browser add-ons that alter browser settings.

Master Boot Record Infection (MBR) – Malware that infects the MBR to load before the OS.

Bot Trojan – Turns a computer into a botnet node for remote control.

Cookie Tracker – Tracks user activity for advertising or data collection.

Dialer Trojan – Hijacks modem connections to dial premium-rate numbers.

Dropper Trojan – Malware that installs additional infections.

EICAR Test File – A harmless file used to test antivirus detection.

Exploit Malware – Malware that exploits system vulnerabilities.

Hoax Malware – Fake security alerts designed to scare users into installing malware.

Hijacker – Malware that hijacks system settings (e.g., browser homepage).

Hack Tool – Unauthorized tools used for hacking or exploiting security flaws.

Heuristic Detection (Heur) – A detection method based on behavior analysis.

IRC Trojan – Malware that spies on IRC (Internet Relay Chat) conversations.

Macro Virus – Targets macro-based applications (e.g., Microsoft Office).

Password Stealing Trojan – Designed to steal user credentials.

Phishing Malware – Used to steal user data by impersonating trusted entities.

Polymorphic Virus – Changes code to evade detection. Examples: Virut or Sality

Process Killer – Malware that terminates security software processes.

Redirect Trojan – Hijacks browser traffic to malicious websites.

Remote Access Trojan (RAT) – Allows remote control over a compromised system.

Spamming Malware – Sends spam emails from infected machines.

Scamming Malware – Designed to defraud users through deception.

Rogue Malware (ROGUE) – Fake security software that extorts users.

Security Terminology

General Security & System Terms

ActiveX – A component of Internet Explorer that extends browser functionality.

Administrator – A user with system-wide access and control privileges.

Algorithm – A structured set of instructions for problem-solving.

Alias – An alternate name for a malware variant (e.g., Alureon = TDL4).

Anti-Malware – A tool designed to detect and remove all types of malware.

Anti-Spyware – A tool specifically for detecting spyware infections.

Antivirus – A security program that detects and removes viruses.

Application Programming Interface (API) – A set of routines that allow software to interact with an OS.

Armoring ("Crypting") – A technique used by malware to evade detection.

ASCII (American Standard Code for Information Interchange) – A character encoding system.

Attributes – Characteristics of files or folders (e.g., read-only, hidden).

BAT = Batch File -- A file designed to automate tasks.

BIOS (Basic Input/Output System) – Firmware that initializes system hardware.

Botnet – A network of compromised computers controlled by hackers.

Cache – A temporary storage mechanism used to improve system performance.

Cookie -- A text file that stores user information and preferences for websites to make your experience better on their site.

Debugger -- Used to run or halt a program by using breakpoints and has the ability to step through code line by line.

Decompiler -- Used to read the source code of a program.

Denial of Service (DoS) / Distributed DoS (DDoS) – An attack that overwhelms a server to disrupt service.

DNS (Domain Name System) – Translates domain names into IP addresses.

Driver – A program that allows the OS to communicate with hardware.

Dynamic Link Library (DLL) – A file that contains shared code modules.

Emergency Rescue Disk/Recovery - In older times a disk, but in modern times a USB drive loaded with portable recovery software to aid in scanning or recovering the computer.

Encryption / Decryption – The process of encoding/decoding data for security.

Exceptions – A security program's list of whitelisted files and programs.

FAT = File Allocation Table -- A section of a disk that defines the structure and/or organization of the disk. It contains addresses for where files/folders are stored on the disk.

Firewall – A security feature that monitors network traffic.

FTP = File Transfer Protocol -- A technique that transfers files over a TCP/IP connection.

Hacker – A person who gains unauthorized access to a computer system.

Header - A section of a file where information about the file are kept such as date, name, type, etc. usually located at the beginning of a file.

Host - A computer or system that acts as a source of information.

HTTP/HTTPS (Hypertext Transfer Protocol Secure) – The protocols for web browsing.

Identity Theft – The act of stealing someone's personal or financial data.

ISP (Internet Service Provider) – A company that provides internet access.

LAN (Local Area Network) – A private network connecting computers in a small area.

MIME = Multipurpose Internet Mail Extensions - A set of specifications for allowing text and files with different character sets and features be exchanged over the internet.

Mutex = Mutual Exclusion Object - An object or program use to control access to resources.

Partition - An area or division of a disk that identifies it as a separate disk. Each partition, for example, can be a separate/different operating system.

Payload – The malicious effects of malware execution.

PE = Portable Executable - A form of an executable file.

PUP (Potentially Unwanted Program) – Software that behaves suspiciously but is not malware.

P2P (Peer to Peer Software) - Software such as uTorrent.

Protocol – A set of rules for data transmission (e.g., FTP, TCP/IP).

Proxy - A controller of internet connection to help it be shared to multiple computers used to evade internet protocol address detection of the one using a proxy.

Quarantine - A technique used to disinfect a certain piece of malware, but keep information about the file stored.

Redirect -- A technique used to change navigation to a certain website to a different website.

Sector - A section or area of a disk.

Patch - A set of additional files meant to be added to a program to fix specific flaws or bugs.

String - A sequence of characters or codes.

Services - A specific program or driver that is meant to carry out specific tasks independently in the system. It can stop, pause, or be given certain instructions on its own. It can be controlled manually, automatically, or other options.

Signature – The unique identifier of a malware sample.

Variant - A modified version of the original virus or malware that is remade.

Volume - A partition, complete hard disk, or section of a disk described to be independent or shared.

UPX (Ultimate Packer for Executables) – A tool used to compress executable files.

WAN = Wide Area Network - A network of interconnected computers over a large region via network.

Windows Explorer - The program used to browse files and folders on the Windows Operating System.

Windows Registry – A database storing system settings and configurations.

Conclusion

This guide serves as a quick reference for security and anti-malware terminology. Understanding these terms will help you better analyze antivirus logs, research malware threats, and improve cybersecurity awareness.

Tha Sneak - March 1, 2025, 8:28 pm

Please do NOT reply to this thread in case information needs to be added or edited.

If you have a questions about the contents of the thread or other tutorials please go to this thread and post your question in this thread: <https://hackforums.net/showthread.php?tid=6293473>

Thanks,

Tha Sneak