ClamAV

https://cs.co/1page

ClamAV® is an open-source (GPL) anti-virus engine used for email attachment scanning, web scanning and endpoint security. It can detect, quarantine, and remove all types of malware, including trojans, worms, rootkits, and others. Initially created for UNIX but is currently also available for versions of Linux, Windows and macOS.

Benefits:

- Compatible with major operating systems like Windows, Linux and macOS
- ClamAV can detect millions of viruses, worms, trojans, mobile malware, and even Microsoft Office macro viruses
- ClamAV is an open-source virus database and can be used for research or improvement purposes
- ClamAV can scan archives and compressed files
- Mail gateway scan is possible
- Multi-threaded virtual scanner against malware
- The utility command line allows easy navigation
- This antivirus is free and any custom GUI front-end can connect to it
- Signature databases will ensure that only trusted databases will be used by ClamAV

Features:

- Command-line scanner.
- Milter interface for sendmail.
- Advanced database updater with support for scripted updates & digital signatures.
- Virus database updated multiple times per day.
- Built-in support for all standard mail file formats.
- Built-in support for various archive formats, including ZIP, RAR, Dmg, Tar, GZIP, BZIP2, OLE2, Cabinet, CHM, BinHex, SIS and others.
- Built-in support for ELF and Portable Executable files packed with UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack and obfuscated with SUE, Y0da Cryptor & others.
- Built-in support for popular document formats, including MS Office and MacOffice files, HTML, Flash, RTF and PDF.

Architecture:

- **ClamAV engine:** The core component of the ClamAV antivirus that is responsible for performing malware detection.
- **ClamAV database:** The component that is most frequently updated, and it contains the virus signatures used to detect malware.
- **ClamAV frontend:** Frontends are the applications that provide a user interface for ClamAV. Several frontends are available for ClamAV such as ClamTK.

ClamAV Options:

--verbose: shows the version of the tool

--infected: displays only infected files

--quiet: only lists error messages

--remove: removes infected files

--recursive: ensures that all subdirectories in the directory will be scanned

--move: moves infected files into the specified directory

 # sudo apt-get install clamav: install ClamAV (e.g. Ubuntu)

 # freshclam: Run command to update the signatures database

 # sudo apt-get remove clamav clamav-daemon: To remove ClamAV

 # clamscan -r /: To check all files on the computer

Types of Malware:

Computer Virus: Malware that infects a computer file system from any infected file downloaded

Worms: A worm doesn't infect any file, but spreads by copying itself from one computer to another

Trojan Horse: Malware that can deceive the user to install a software package thinking it is reliable

Ransomware: Causes denial of access to data and threatens the user by demanding a ransom

Spyware: Gathers information about user and data stored in computer

Adware: Doesn't do any harm to data, but it displays advertisements

Wiper: Intended to wipe the hard drive of the user's computer

Scareware: Malware is intended to scare user by displaying false alerts

Resources:

		3rd party tools:	Public pages:
ClamAV Downloads	Signature Writing	ClamWin.com	Talos Intelligence
ClamAV Docs	ClamAV News	MacPorts.org	Wikipedia
ClamAV Blog	Repository	FreshClam	ClamAV.net