Clam AntiVirus

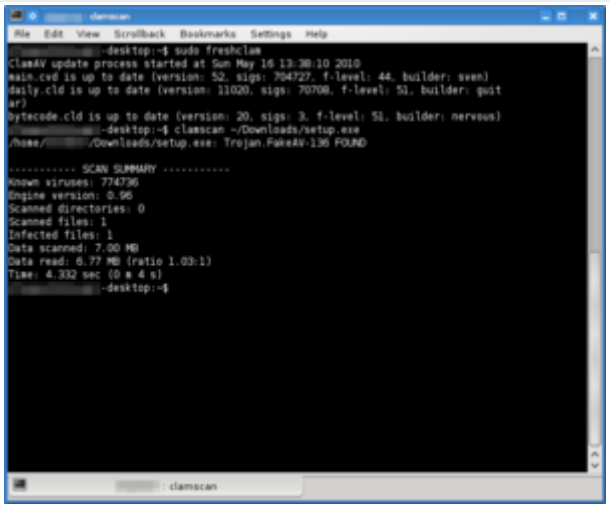
Clam AntiVirus (**ClamAV**) is a free software, cross-platform and open-source antivirus software toolkit able to detect many types of malicious software, including viruses. One of its main uses is on mail servers as a server-side email virus scanner. The application was developed for Unix and has third party versions available for AIX, BSD, HP-UX, Linux, macOS, OpenVMS, OSF (Tru64) and Solaris. As of version 0.97.5, ClamAV builds and runs on Microsoft Windows.[1][2] Both ClamAV and its updates are made available free of charge.

Sourcefire, a maker of intrusion detection products and the owner of Snort, announced on 17 August 2007 that it had acquired the trademarks and copyrights to ClamAV from five key developers.[3] Upon joining Sourcefire, the ClamAV team joined the Sourcefire Vulnerability Research Team (VRT). In turn, Sourcefire was acquired by Cisco in 2013.[4] The Sourcefire VRT became Cisco Talos,[5] and ClamAV development remains there.

Contents

- Features
- Effectiveness
- Unofficial databases
- Platforms
  - Linux, BSD
  - macOS
  - OpenVMS
  - Windows
  - OS/2
- Graphical interfaces
  - ClamWin
  - Clam Sentinel
- Real-time file scanning
- Patent lawsuit
- See also
- References
- Further reading
- External links

Clam AntiVirus



Clam AV 0.96, running a definition update, scanning a file and identifying a Trojan from the command-line.

Developer(s)	Cisco Systems
Stable release	0.103.0 / September 14, 2020
Repository	github.com/Cisco-Talos/clamav-devel (https://github.com/Cisco-Talos/clamav-devel)
Written in	C, C++
Operating system	Cross-platform
Type	Antivirus software
License	GNU General Public License
Website	www.clamav.net (https://www.clamav.net)

Features

ClamAV includes a number of utilities: a command-line scanner, automatic database updater and a scalable multi-threaded daemon, running on an anti-virus engine from a shared library.[1]

The application also features a Milter interface for sendmail and on-demand scanning. It has support for Zip, RAR, Tar, Gzip, Bzip2, OLE2, Cabinet, CHM, BinHex, SIS formats, most mail file formats, ELF executables and Portable Executable (PE) files compressed with UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack and obfuscated with SUE, Y0da Cryptor. It also supports many document formats, including Microsoft Office, HTML, Rich Text Format (RTF) and Portable Document Format (PDF).[1]

The ClamAV virus database is updated at least every four hours and as of 10 February 2017 contained over 5,760,000 virus signatures with the daily update Virus DB number at 23040.[6][7]

Effectiveness

ClamAV is currently tested daily in comparative tests against other antivirus products on *Shadowserver*. In 2011, Shadowserver tested over 25 million samples against ClamAV and numerous other antivirus products. Out of the 25 million samples tested, ClamAV scored 76.60% ranking 12 out of 19, a higher rating than some much more established competitors.[8]

In the 2008 AV-Test, which compared ClamAV to other antivirus software, it rated: on-demand: very poor; false positives: poor; response time: very good; rootkits: very poor.[9]

In a Shadowserver six-month test between June and December 2011, ClamAV detected over 75.45% of all viruses tested, putting it in fifth place behind AhnLab, Avira, BitDefender and Avast. AhnLab, the top antivirus, detected 80.28%.[10]

Unofficial databases

The ClamAV engine can be reliably used to detect several kinds of files. In particular, some phishing emails can be detected using antivirus techniques. However, false positive rates are inherently higher than those of traditional malware detection.[11]

There are several unofficial databases for ClamAV:

- Sanesecurity is an organization that maintains a number of such databases; in addition they distribute and classify a number of similar databases from other parties, such as Porcupine, Julian Field, MalwarePatrol.[12]
- SecuriteInfo.com also provides additional signatures for ClamAV.[13]

ClamAV Unofficial Signatures are mainly used by system administrators to filter email messages.[14] Detections of these groups should be scored, rather than causing an outright block of the "infected" message.[12]

Platforms

Linux, BSD

ClamAV is available for Linux and BSD-based operating systems.[1] In most cases it is available through the distribution's repositories for installation.

On Linux servers ClamAV can be run in daemon mode, servicing requests to scan files sent from other processes. These can include mail exchange programs, files on Samba shares, or packets of data passing through a proxy server.

On Linux and BSD desktops ClamAV provides on-demand scanning of individual files, directories or the whole PC.[1]

macOS

Apple macOS Server has included ClamAV since version 10.4. It is used within the operating system's email service. A paid-for graphical user interface is available from Canimaan Software Ltd[15] in the form of *ClamXav*.[16] Additionally, Fink, Homebrew and MacPorts have ported ClamAV.

Another program which uses the ClamAV engine, on macOS, is Counteragent. Working alongside the Eudora Internet Mail Server program, Counteragent scans emails for viruses using ClamAV and also optionally provides spam filtering through SpamAssassin.

OpenVMS

ClamAV for OpenVMS is available for DEC Alpha and Itanium platforms. The build process is simple and provides basic functionality, including: library, clamscan utility, clamd daemon and freshclam for update.[17]

Windows

ClamAV for Windows is now a part of the Immunet client produced by Cisco. Immunet is a real-time cloud based detection software, maintained by Cisco, which owns both ClamAV and Immunet.[18]

OS/2

A port of ClamAV is available for OS/2 (including eComStation and ArcaOS) with a native UI written in REXX.[19][20]

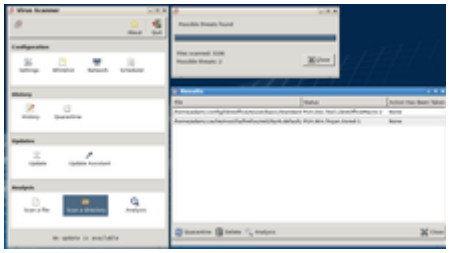
Graphical interfaces

Since ClamAV does not include a graphical user interface (GUI) but instead is run from the command line, a number of third-party developers have written GUIs for the application for various platforms and uses.

These include:

- Linux
  - ClamTk using gtk2-perl; project is named for the Tk libraries that were used when it began[21][22]
  - KlamAV for KDE, discontinued development in 2009[23]
  - wbmclamav is a webmin module to manage Clam AntiVirus[24]

- macOS
  - ClamXav is a port which includes a graphical user interfaces and has a "sentry" service which can watch for changes or new files in many cases. There is also an update and scanning scheduler through a cron job facilitated by the graphical interface. ClamXav can detect malware specific to macOS, Unix, or Windows. The ClamXav application and the ClamAV engine are updated regularly.[25] ClamXav is written and sold by Canimaan Software Ltd.[15]
  - Tiger Cache Cleaner is shareware software which installs and presents a graphic interface for using ClamAV to scan for viruses, and provides other unrelated functions.
- Microsoft Windows
  - Immunet
  - ClamWin
  - CS Antivirus[26]
  - Graugon AntiVirus[26]
  - Clam Sentinel
- OS/2
  - ClamAV-GUI[19]

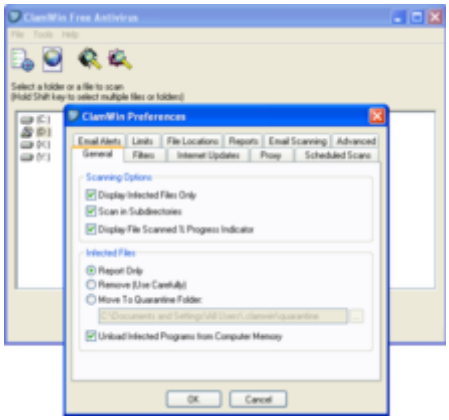


ClamTk 5.27 running on Lubuntu 19.04

ClamWin

ClamWin is a graphical user interface front end for ClamAV for Microsoft Windows built by ClamWin Pty Ltd. Features include *on-demand* (user started) scanning, automatic updates, scan scheduling, context menu integration to Explorer, and an add-in for Microsoft Outlook. ClamWin does not provide on-access scanning, additional software must be used.

Plugins for Mozilla Firefox which use ClamWin to scan downloaded files are also available.[27][28] Several other extensions allow users to process downloaded files with any software and scan the files with ClamWin.[29][30][31][32]



ClamWin running on Windows XP

Clam Sentinel

Clam Sentinel[33] is a free software system tray application that detects file system changes and scans the files modified using ClamWin in real-time.[34] It works with Windows 98/98SE/ME/XP/Vista/7/8. It features a real-time scanner for ClamWin, optional system change messages and proactive heuristic protection.

Real-time file scanning

Since Version 0.99, ClamAV supports on-access (real-time) scanning via the Linux kernel (version >= 3.8) module fanotify.[35] Alternatively, ClamAV can be used with other applications such as ClamFS (for any Unix-like operating system supporting FUSE) and Clam Sentinel (for Windows) to provide real-time

checks.[36]

Patent lawsuit

In 2008, Barracuda Networks was sued by Trend Micro for its distribution of ClamAV as part of a security package.[37] Trend Micro claimed that Barracuda's utilization of ClamAV infringes on a software patent for filtering viruses on an Internet gateway. The free software community responded in part by calling for a boycott against Trend Micro. The boycott was also endorsed by the Free Software Foundation.[38] Barracuda Networks counter-sued with IBM-obtained patents in July 2008.[39] On May 19, 2011, the U.S. Patent and Trademark Office issued a Final Rejection[40] in the reexamination of Trend Micro's U.S. patent 5,623,600.[41]

See also

- List of antivirus software
- List of free and open-source software packages
- Software patents and free software

References

1. ClamAV (2007). "About ClamAV" (http://www.clamav.net/about). Retrieved 2008-12-25.
2. ClamAV (2007). "ClamAV Packages and Ports" (https://web.archive.org/web/20080720205113/http://www.clamav.net/download/packages/). Archived from the original (http://www.clamav.net/download/packages/) on 2008-07-20. Retrieved 2008-12-31.
3. "Sourcefire acquires ClamAV" (https://web.archive.org/web/20071215031743/http://www.clamav.org/2007/08/17/sourcefire-acquires-clamav/). ClamAV. 2007-09-17. Archived from the original (http://www.clamav.org/2007/08/17/sourcefire-acquires-clamav/) on 2007-12-15. Retrieved 2008-02-12.
4. "Cisco Completes Acquisition of Sourcefire" (http://www.cisco.com/web/about/ac49/ac0/ac1/ac259/sourcefire.html). *cisco.com*. 2013-10-07. Retrieved 2014-06-18.
5. "Cisco Talos" (https://talosintelligence.com). 2018-01-19.
6. "About ClamAV" (https://web.archive.org/web/20081120213532/http://www.clamav.net./about). Archived from the original (http://www.clamav.net/about/) on 2008-11-20. Retrieved 2008-12-25.
7. "Latest Stable Release" (https://web.archive.org/web/20100918141732/http://www.clamav.net/lang/en/about/). Archived from the original (http://www.clamav.net/lang/en/about/) on 2010-09-18. Retrieved 2010-08-21.
8. "ShadowServer Yearly Stats" (https://web.archive.org/web/20110625201600/http://www.shadowserver.org/wiki/pmwiki.php/Stats/VirusYearlyStats). shadowserver.org. 2012-01-05. Archived from the original (http://www.shadowserver.org/wiki/pmwiki.php/Stats/VirusYearlyStats) on 2011-06-25. Retrieved 2012-01-05.
9. "Anti-virus comparison test of current anti-malware products, Q1/2008" (https://web.archive.org/web/20110715060200/http://blogs.pcmag.com/securitywatch/Results-2008q1.htm). AV-Test GmbH. 22 January 2008. Archived from the original (http://blogs.pcmag.com/securitywatch/Results-2008q1.htm) on 15 July 2011. Retrieved 12 February 2008.
10. "ShadowServer 180 Day Stats" (https://web.archive.org/web/20111127145417/http://www.shadowserver.org/wiki/pmwiki.php/AV/Virus180-DayStats). shadowserver.org. 2011-08-16. Archived from the original (http://www.shadowserver.org/wiki/pmwiki.php/AV/Virus180-DayStats) on 2011-11-27. Retrieved 2011-12-16.

11. Brad Wardman; Tommy Stallings; Gary Warner; Anthony Skjellum (5 August 2011). "High-Performance Content-Based Phishing Attack Detection" (https://uab.edu/cas/thecenter/images/Documents/High-Performance-Content-Based-Phishing-Attack-Detection.pdf) (PDF). *uab.edu*. Retrieved 19 March 2018.
12. Sanesecurity Phishing, Scam and Malware signatures for ClamAV (http://www.sanesecurity.com/clamav/databases.htm) Archived (https://web.archive.org/web/20150910185428/http://www.sanesecurity.com/clamav/databases.htm) 2015-09-10 at the Wayback Machine
13. SecuriteInfo.com Add 4.000.000 signatures to ClamAV Antivirus (https://www.securiteinfo.com/services/improve-detection-rate-of-zero-day-malwares-for-clamav.shtml)
14. "ClamAV Unofficial Signatures Updater" (http://sourceforge.net/projects/unofficial-sigs/). *sourceforge.net*. 24 May 2009. Retrieved 2 September 2014.
15. "About us" (https://www.clamxav.com/about-us/). *ClamXAV*. Retrieved 2017-07-15.
16. ClamXav.com (n.d.). "ClamXAV.com" (http://www.clamxav.com/). Retrieved 2009-01-24.
17. Chupahin, Alexey (December 2008). "Clam AntiVirus OpenVMS Project News" (https://web.archive.org/web/20111006011551/http://clamav.dyndns.org/clamav/). Archived from the original (http://clamav.dyndns.org/clamav/) on 2011-10-06. Retrieved 2008-12-25.
18. "Immunet Online Protection" (https://web.archive.org/web/20150524121927/http://www.immunet.com/free/index.html). Archived from the original (http://www.immunet.com/free/index.html) on 2015-05-24. Retrieved 2015-05-23.
19. "My graphical user interface for "ClamAV" " (http://remydodin.levillage.org/en/realisations.php?item=5900&id=realisations). Retrieved 2020-09-03.
20. "Clamav, ClamAV-GUI (Rexx & QT4) & eCSClamav" (https://ecsoft2.org/clamav-clamav-gui-rexx-qt4-ecsclamav). Retrieved 2020-09-03.
21. Mauroni, Dave (December 2008). "ClamTk Virus Scanner" (http://clamtk.sourceforge.net/). Retrieved 2008-12-25.
22. Mauroni, Dave (October 2008). "ClamTk README" (http://clamtk.sourceforge.net/README). Retrieved 2008-12-26.
23. KlamAV F. (May 2006). "KlamAV - Main Page" (http://sourceforge.net/projects/klamav/). Retrieved 2013-03-04.
24. "wbmclamav project" (http://wbmclamav.labs.libre-entreprise.org/).
25. ClamXav.com (November 2008). "ClamXav.com" (http://www.clamxav.com/). Retrieved 2008-12-25.
26. "CS Anti-Virus description" (http://www.softpedia.com/get/Antivirus/CS-Anti-Virus.shtml). Softpedia.com. 2009-03-23. Retrieved 2010-11-09.
27. "FireClam: Use ClamAV to scan Firefox downloads for viruses" (https://addons.mozilla.org/en-US/firefox/addon/fireclam/). Firefox Addons. Retrieved 2009-11-02.
28. "ClamWin Antivirus Glue for Firefox" (https://archive.today/20121220214917/https://addons.mozilla.org/en-US/firefox/addon/clamwin-antivirus-glue-for-fir/). Firefox Addons. Archived from the original (https://addons.mozilla.org/en-US/firefox/addon/clamwin-antivirus-glue-for-fir/) on 2012-12-20. Retrieved 2008-04-15.
29. "Download Scan" (http://downloadstatusbar.mozdev.org/downscan/). Downloadstatusbar.mozdev.org. 2005-08-19. Retrieved 2010-11-09.
30. Download Statusbar (https://addons.mozilla.org/en-US/firefox/addon/download-statusbar/)
31. "Safe Download" (http://extensions.geckozone.org/SafeDownload). Extensions.geckozone.org. Retrieved 2010-11-09.
32. ClamWin Pty Ltd (2009). "About ClamWin Free Antivirus" (https://web.archive.org/web/20100125005824/http://www.clamwin.com/content/view/71/1/). Archived from the original (http://www.clamwin.com/content/view/71/1/) on 2010-01-25. Retrieved 2009-03-13.
33. Clam Sentinel (2014-09-01). "Clam Sentinel - Free Realtime Antivirus" (http://clamsentinel.sourceforge.net/index.php?Lang=en).

34. Cyber Pillar. "Clam Sentinel - Making ClamWin Be Used In Real-Time" (http://cyberpillar.com/dirsver/1/mainsite/techns/bhndscen/protsoft/antimalw/antivir/avmswin/clamwin/mkclmwrt/mkclmwrt.htm). Retrieved 2014-09-01.
35. https://blog.clamav.net/2016/03/configuring-on-access-scanning-in-clamav.html
36. "Clam Sentinel" (http://sourceforge.net/projects/clamsentinel/). Retrieved 2014-06-19.
37. "Trend Micro patent claim provokes FOSS community, leads to boycott" (http://www.linux.com/feature/126851). Linux.com. 2008-02-11. Retrieved 2008-02-12.
38. "Boycott Trend Micro" (http://www.fsf.org/blogs/community/boycottTrendMicro.html). Free Software Foundation. 2008-02-11. Retrieved 2008-02-12.
39. Paul, Ryan (2008-07-02). "Barracuda bites back at Trend Micro in ClamAV patent lawsuit" (https://arstechnica.com/open-source/news/2008/07/barracuda-bites-back-at-trend-micro-in-clamav-patent-lawsuit.ars). Arstechnica.com. Retrieved 2012-02-14.
40. "Ex Parte Reexamination" (http://www.groklaw.net/pdf3/90011022-18.pdf) (PDF). U.S. Patent and Trademark Office. 2011-05-19. Retrieved 2015-10-04.
41. "Anatomy of a Dying Patent - The Reexamination of Trend Micro's '600 Patent" (http://www.groklaw.net/article.php?story=20110613091958268). Groklaw.net. 2011-06-13. Retrieved 2015-10-04.

Further reading

- An interview with ClamAV founder Tomasz Kojm archived version (https://web.archive.org/web/20120206053729/http://www.emailbattles.com/2005/08/31/virus_aabejfhaib_ag/)

External links

- Official website (https://www.clamav.net)