



Introduction to ClamAV

Tomasz Kojm

SOURCE*fire*

ENTERPRISE THREAT MANAGEMENT

General information



- Clam AntiVirus (ClamAV) is an anti-virus toolkit for UNIX
- Designed for integration with mail servers
- Developed by international team of developers and distributed under the GPL v2 license
- Since August 2007 developed under Sourcefire wings

ClamAV in numbers



- ClamAV is six years old
- Database includes over 315 000 signatures
- 2M+ unique IP addresses download the virus database every day
- There are more than 120 database mirrors in 44 countries
- Each mirror serves ~1TB of data per day

Main advantages of ClamAV



- Portable code, written entirely in C
- Large and regularly updated (usually 5 or more times per day) virus database
- Very good reaction times to new threats
- Solid network infrastructure
- Widely supported by third party software (more than 100 related projects) which allow for integration with MTA, MUA, POP3, FTP...

Software package



- The ClamAV software package provides:
 - *libclamav* – anti-virus engine
 - *clamd* – scanning daemon
 - *clamscan* – command line scanner
 - *clamdscan* – clamscan-like clamd client
 - *freshclam* – virus database updater
 - *main.cvd*, *daily.cvd* – virus signature databases
 - *clamconf* – configuration tool



Compilation and installation

SOURCE*fire*

ENTERPRISE THREAT MANAGEMENT



- *libclamav* is the core part of ClamAV:
 - Includes virus detection algorithms
 - Provides a virus detection API
 - Available as a shared library
 - Thread safe
 - Allows for easy integration of AV scanning in 3rd party products

libclamav: virus detection



- Virus detection primarily relies on pattern (signature) matching
- Anti-virus software must be able to match dozens of thousands signatures effectively
- ClamAV relies on two pattern matching algorithms:
 - Aho-Corasick
 - Multi-pattern version of Boyer-Moore

libclamav: virus detection



- ❏ ClamAV can use various signature formats:
 - Based on fragment of virus body
 - MD5 checksum of entire file or specific PE section
 - Based on archive metadata
- ❏ Some malware cannot be detected with signatures and requires algorithmic approach
- ❏ Algorithmic detection and signature scanning are complementary, dedicated algorithms help to detect complex viruses more reliably



libclamav: supported formats

- ❏ ClamAV can scan within many file formats:
 - Executables: PE (win32/64), ELF (unix)
 - PE packers supported: AsPack, UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack, Y0da Crypter...
 - Archives and compressors: zip, rar, arj, chm, cabinet, ole2, tar, sis, nsis, szdd, gzip, bzip2,...
 - Documents: MS Office, HTML, RTF, PDF
 - All popular mail formats
 - Other: BinHex, uuencode, ScrEnc, CryptFF...

libclamav: phishing detection



- ❏ ClamAV provides a double layer protection against phishing:
 - the first approach uses regular signatures to reliably detect common phishing attacks
 - the other uses heuristics and special signatures to proactively detect new threats

Libclamav: detection of Potentially Unwanted Applications



- ❖ ClamAV can detect applications which are not malicious by itself but can be used in malicious or unwanted context
- ❖ PUA includes password crackers, runtime packers, various specialized network tools, etc.
- ❖ PUA detection is not enabled by default

clamscan



- ❏ Command line file scanner
- ❏ Easy scanning of files and directories
- ❏ Needs to load virus databases each time when started



clamscan in practice

SOURCE*fire*

ENTERPRISE THREAT MANAGEMENT

clamd



- ❏ Multi-threaded daemon
- ❏ Can take advantage of SMP systems
- ❏ Operates in TCP and UNIX socket mode
- ❏ Command driven: SCAN, PING, RELOAD, STREAM,...
- ❏ Fast scanning: clamd loads the database once and then shares it with all threads
- ❏ On-access scanning on Linux and FreeBSD



clamd - configuration

- The most important options include:
 - LogFile
 - PidFile
 - DatabaseDirectory
 - LocalSocket
 - TCPSocket
 - MaxScanSize, MaxFileSize, MaxFiles, MaxRecursion



clamdscan

- ❏ Command line clamd client
- ❏ Can be used as a basic replacement for clamscan
- ❏ Fast scanning of small files
- ❏ Passes files, directories and data streams directly to clamd
- ❏ Can only scan files accessible by clamd instance it connects to



clamd and clamdscan in practice

SOURCE*fire*

ENTERPRISE THREAT MANAGEMENT



- ❏ Signature database update tool
- ❏ Works in interactive and daemon modes
- ❏ Verifies database integrity
- ❏ Tries to minimize download size by picking up small diff files
- ❏ Can call external applications on special events (update, error, new software available...)
- ❏ Supports proxy and uses DNS (a special TXT record) to check for new database and software releases



freshclam - configuration

- ❏ freshclam.conf uses the same format as clamd.conf
- ❏ Provides about 30 configuration options
- ❏ freshclam.conf should always include two DatabaseMirror entries:
 - DatabaseMirror db.XY.clamav.net
 - DatabaseMirror database.clamav.net
- ❏ XY is the country code, see <http://www.iana.org/cctld/cctld-whois.htm>

Database Mirrors



- ❏ Signature databases are distributed through more than 120 official mirrors in 44 countries
- ❏ `db.XY.clamav.net` points to mirrors available in country XY
- ❏ `db.local.clamav.net` attempts to redirect `freshclam` to closest pool of mirrors by checking its IP in the GeoIP database
- ❏ `database.clamav.net` is a round robin record which points to the largest and most reliable mirrors



freshclam and database handling in practice

SOURCE*fire*

ENTERPRISE THREAT MANAGEMENT

Troubleshooting



- ❖ Mac OS X: ./configure refuses to continue and suggests to use a different compiler
- ❖ Clamd/clamscan and freshclam show a different number of signatures
- ❖ Scanning RAR archives results in a warning (“RAR code not compiled-in”)
- ❖ freshclam cannot update signature databases



How to report bugs

- ❏ If you find a bug, please check if it still exists in the development (SVN) version
- ❏ Visit our bugzilla and check if the problem has been already reported
- ❏ Please open a bug report and provide all required information as listed on <http://www.clamav.org/bugs/>
- ❏ Please do not report bugs which only exist in software derived from ClamAV (including unofficial binary ports)



Questions?

SOURCE*fire*

ENTERPRISE THREAT MANAGEMENT