Clam AntiVirus 0.81rc1

User Manual

Contents

1 Introduction

Clam AntiVirus is an anti-virus toolkit for UNIX, designed for e-mail scanning on mail gateways. It provides a flexible and scalable multi-threaded daemon, a command line scanner, and an advanced tool for automatic database updating via Internet. The package also includes a virus scanner shared library.

1.1 Features

- Licensed under the GNU General Public License, Version 2
- POSIX compliant, portable
- Fast scanning
- Supports on-access scanning (Linux and FreeBSD only)
- Detects over 29000 viruses, worms, and trojans, including Microsoft Office and MacOffice macro viruses
- Scans within archives and compressed files (also protects against archive bombs), built-in support includes:
  - Zip
  - RAR (2.0)
  - Tar
  - Gzip
  - Bzip2
  - MS OLE2
  - MS Cabinet Files
  - MS CHM (Compiled HTML)
  - MS SZDD compression format
- Supports Portable Executable files compressed with:
  - UPX
  - FSG
  - Petite
- Powerful mail scanner
- Advanced database updater with support for digital signatures and DNS based database version queries

1.2 Mailing lists

If you have a trouble installing or using ClamAV try to ask on our mailing lists. There are four lists available:

- **clamav-announce*lists.clamav.net** - info about new versions, moderated[1].
- **clamav-users*lists.clamav.net** - user questions
- **clamav-devel*lists.clamav.net** - technical discussions
- **clamav-virusdb*lists.clamav.net** - database update announcements, moderated

You can subscribe and search the mailing list archives at: `http://www.clamav.net/ml.html`

1.3 Virus submitting

If you have got a virus which is not detected by your ClamAV with the latest databases, please check it with the *ClamAV Online Specimen Scanner*:

`http://test-clamav.power-netz.de/`

and then submit it on our website:

`http://www.clamav.net/sendvirus.html`

2 Base package

2.1 Supported platforms

All popular operating systems are supported. Clam AntiVirus was tested on:

- GNU/Linux
- Solaris
- FreeBSD
- OpenBSD [2]
- AIX 4.1/4.2/4.3/5.1

[1] Subscribers are not allowed to post to the mailing list
[2] Installation from a port is recommended.

- HPUX 11.0
- SCO UNIX
- IRIX 6.5.20f
- Mac OS X
- BeOS
- Cobalt MIPS boxes
- Cygwin
- Windows Services for Unix 3.5 (Interix)

Some features may not be available on your operating system. If you are successfully running Clam AntiVirus on a system not listed above please let us know.

2.2 Binary packages

- **Debian**
  The package is maintained by Stephen Gran and Thomas Lamy. ClamAV has been officially included in the Debian distribution starting from the Sarge release. Run `apt-cache search clamav` to find the names of the packages available for installation. Unofficial packages for Woody and Sarge are available and they are usually more recent than official ones. Add the following lines to your /etc/apt/sources.list:

  ```
  for stable/woody (i386):
  deb http://people.debian.org/~sgran/debian woody main
  deb-src http://people.debian.org/~sgran/debian woody main
  for testing/sarge (i386):
  deb http://people.debian.org/~sgran/debian sarge main
  deb-src http://people.debian.org/~sgran/debian sarge main
  ```

  Feel free to search for clamav on `http://www.apt-get.org/` too.

- **RedHat - Fedora**
  The packages are maintained by Petr Kristof.
  Fedora1: `http://crash.fce.vutbr.cz/crash-hat/1/clamav/`
  Fedora2: `http://crash.fce.vutbr.cz/crash-hat/2/clamav/`
  Devel snapshots: `http://crash.fce.vutbr.cz/crash-hat/testing/2/`
  Please follow the instructions at `http://crash.fce.vutbr.cz/yum-repository.html` and then run:

```
yum update clamav
or
up2date -u clamav
```

Another very good repository is maintained by Dag Wieers: http://dag.wieers.com/packages/clamav/

- **PLD Linux Distribution**
  The RPM packages for the Polish(ed) Linux Distribution are maintained by Arkadiusz Miskiewicz (visit http://www.pld-linux.org/).

- **Mandrake**
  A RPM package for Mandrake is available on Mandrake's mirrors and is maintained by Oden Eriksson. Another set of RPM packages (maintained by Bill Randle) is available at ftp://ftp.neocat.org/pub/.

- **Slackware**
  Slackware packages without milter support are maintained by Jay Scott Raymond. You can find them at http://webpages.charter.net/jay_scott_raymond/linux/slackages/ If you need milter enabled ClamAV, try Peter Kaagman's packages available at http://bilbos-stekkie.com/clamav/
  Both of them are also available at http://www.linuxpackages.net/

- **SuSE** SuSE 8.2 and 9.1 RPMs are maintained by Joe Benden. You can download them at http://www.ispservices.com/clamav.html. Official ClamAV packages for SuSE are maintained by Reinhard Max.

- **FreeBSD**
  The official FreeBSD port is maintained by Masahiro Teramoto. There are two version available: clamav and clamav-devel. You can find both of them under /usr/ports/security/

- **OpenBSD**
  ClamAV will become part of the official ports tree in the upcoming 3.7 release of OpenBSD. The new port is maintained by Marc Balmer. The old unofficial port for OpenBSD (maintained by Jerome Loyet) is available at: http://www.fatbsd.com/openbsd/clamav/

- **NetBSD**
  The official port is available.

- **Solaris**
  Stable packages and daily snapshots for Solaris 8 SPARC are available at http:

//clamav.or.id/snapshot/. Latest stable packages for Solaris 9 SPARC 64bit are available at http://clamav.citrus-it.net

- **AIX**
  The binary packages for AIX are available in AIX PDSLIB, UCLA
  http://aixpdslib.seas.ucla.edu/packages/clamav.html
- **Mac OS X**
  There's a binary package available at http://clamav.darwinports.com/
  clamXav (see 8.6.6), a GUI for ClamAV running on MacOS X, is available at http://www.markallan.co.uk/clamXav
- **BeOS**
  BeClam is a port of ClamAV for the BeOS operating system. It includes a very simple GUI. Get it at http://www.bebits.com/app/3930/
- **MS Windows - Cygwin**
  All major features of ClamAV are implemented under Win32 using the Cygwin compatibility layer. You can download a self-installing package at
  http://www.sosdg.org/clamav-win32/index.php
- **MS Windows - Interix**
  A binary package of ClamAV for Interix is maintained at
  http://www.interopsystems.com/tools/warehouse.htm
- **MS Windows - graphical version**
  A standalone GUI version is also available. See ClamWin in the *Third Party Software* section (8.6.7).

2.3 Daily built snapshots

Thanks to Fajar A. Nugraha you can download daily builds (from daily snapshots) for the following operating systems:

- SPARC Solaris 8/9
- DEC OSF (built on Tru64 UNIX V5.0A)
- AIX (built on AIX Version 5.1)
- Linux i386 with glibc 2.3 (compiled on Fedora Core 1, works on RH $\geq$ 8)
- Win32/Cygwin (compiled on XP)

They're available at http://clamav.or.id/

3 Installation

3.1 Requirements

The following elements are required to compile ClamAV:

- zlib and zlib-devel packages
- gcc compiler suite (both 2.9x and 3.x are supported)

The following packages are optional but **highly recommended**:

- bzip2 and bzip2-devel library
- GNU MP 3
  It's very important to install the GMP package because it allows `freshclam` to verify the digital signatures of the virus databases. If freshclam was compiled without GMP support it will display "SECURITY WARNING: NO SUPPORT FOR DIGITAL SIGNATURES" on every update. You can download GNU MP at `http://www.swox.com/gmp/`
  A note for Solaris/SPARC users: you must set the *ABI* system variable to 32 (e.g. `setenv ABI 32`) before running the configuration script of GMP.

3.2 Installing on a shell account

To install ClamAV on a shell account (e.g. on some shared host) you need not create any additional users or groups. Assuming your home directory is `/home/gary` you should build it as follows:

```
$ ./configure --prefix=/home/gary/clamav --disable-clamav
$ make; make install
```

To test your installation execute:

```
$ ~/clamav/bin/freshclam
$ ~/clamav/bin/clamscan ~
```

The `--disable-clamav` switch disables testing for the existence of the *clamav* user and group but `clamscan` would still require an unprivileged account to work in a superuser mode.

3.3 Adding new system user and group

If you are installing ClamAV for the first time, you have to add a new user and group to your system: [3]

```
# groupadd clamav
# useradd -g clamav -s /bin/false -c "Clam AntiVirus" clamav
```

Consult a system manual if your OS has not *groupadd* and *useradd* utilities. The account should be locked in */etc/passwd* or */etc/shadow*.

3.4 Compilation of base package

Once you have created the clamav user and group, please extract the archive:

```
$ zcat clamav-x.yz.tar.gz | tar xvf -
$ cd clamav-x.yz
```

Assuming you want to install the configuration files in /etc, configure the package as follows:

```
$ ./configure --sysconfdir=/etc
```

Currently *gcc* is required to compile ClamAV.

```
$ make
$ su -c "make install"
```

In the last step the software is installed in the /usr/local directory and the config file goes to /etc. **WARNING: Never enable the SUID or SGID bits in Clam AntiVirus binaries.**

3.5 Compilation with clamav-milter enabled

libmilter and its development files are required. To enable clamav-milter, configure ClamAV with

```
$ ./configure --enable-milter
```

[3] Cygwin note: If you have not /etc/passwd you can skip this procedure

4 Configuration

4.1 clamd

If you are going to use the daemon, you have to edit the configuration file (in other case `clamd` won't run):

```
$ clamd
ERROR: Please edit the example config file /etc/clamd.conf.
```

This shows the location of the default configuration file. The format and options of this file are fully described in the *clamd.conf(5)* manual. The config file is well commented and configuration should be straightforward.

4.1.1 On-access scanning

An interesting feature of `clamd` is on-access scanning based on the Dazuko module, available from `http://dazuko.org/`. **It is not required to run clamd - furthermore, you shouldn't run Dazuko on production systems**. The special thread in `clamd` responsible for the communication with Dazuko is called "Clamuko" (due to the funny name of Dazuko) and it's only supported on Linux and FreeBSD. To compile dazuko execute:

```
$ tar zxpvf dazuko-a.b.c.tar.gz
$ cd dazuko-a.b.c
$ make dazuko
or
$ make dazuko-smp (for smp kernels)
$ su
# insmod dazuko.o
# cp dazuko.o /lib/modules/‘uname -r‘/misc
# depmod -a
```

Depending on your Linux distribution you have to add a "dazuko" entry to */etc/modules* or run the module during system's startup by adding

```
modprobe dazuko
```

to some startup file. You must also create a new device:

```
$ cat /proc/devices | grep dazuko
254 dazuko
$ su -c "mknod -m 600 /dev/dazuko c 254 0"
```

Now configure Clamuko in `clamd.conf` and read the 5.3 section.

4.2 clamav-milter

Nigel Horne's `clamav-milter` is a very fast email scanner designed for Sendmail. It's written entirely in C and only depends on `clamd`. You can find detailed installation instructions in the `INSTALL` file that comes with the clamav-milter sources. Basically, to connect it with Sendmail add the following lines to `/etc/mail/sendmail.mc`:

```
INPUT_MAIL_FILTER('clmilter','S=local:/var/run/clmilter.sock,
F=, T=S:4m;R:4m')dnl
define('confINPUT_MAIL_FILTERS', 'clmilter')
```

Check entry in `clamd.conf` of the form:

```
LocalSocket /var/run/clamd.sock
```

Start clamav-milter

```
/usr/local/sbin/clamav-milter -lo /var/run/clmilter.sock
```

and restart sendmail.

4.3 Testing

Try to scan recursively the source directory:

```
$ clamscan -r -l scan.txt clamav-x.yz
```

It should find some test files in the clamav-x.yz/test directory. The scan result will be saved in the `scan.txt` log file [4]. To test `clamd`, start it and use `clamdscan` (or connect directly to its socket and run the SCAN command instead):

```
$ clamdscan -l scan.txt clamav-x.yz
```

Please note that the scanned files must be accessible by the user running `clamd` or you get an error.

[4] To get more info on clamscan options execute 'man clamscan'

4.4 Setting up auto-updating

`freshclam` is the default database updater for Clam AntiVirus. It can work in two modes:

- interactive - from command line, verbosely
- daemon - alone, silently

When started by a superuser it drops privileges and switches to the *clamav* user. `freshclam` uses the `database.clamav.net` round-robin DNS which automatically selects a database mirror9.1. `freshclam` is an advanced tool: it supports database version verification through DNS, proxy servers (with authentication), digital signatures and various error scenarios. **Quick test: run freshclam (as superuser) with no parameters and check the output.** If everything is OK you may create the log file in /var/log (owned by *clamav* or another user `freshclam` will be running as (`--user`):

```
# touch /var/log/clam-update.log
# chmod 600 /var/log/clam-update.log
# chown clamav /var/log/clam-update.log
```

Now you *should* edit the configuration file (`freshclam.conf` or `clamd.conf` if they're merged) and configure the *UpdateLogFile* directive to point to the created log file. Finally, to run `freshclam` in the daemon mode, execute:

```
# freshclam -d
```

The other method is to use the *cron* daemon. You have to add the following line to the crontab of the **root** or **clamav** users:

```
N * * * * /usr/local/bin/freshclam --quiet
```

to check for a new database every hour. **N should be a number between 3 and 57 of your choice. Please don't choose any multiple of 10, because there are already too many clients using those time slots.** Proxy settings are only configurable via the configuration file and `freshclam` will require strict permissions on the config file when `HTTPProxyPassword` is enabled.

```
HTTPProxyServer myproxyserver.com
HTTPProxyPort 1234
HTTPProxyUsername myusername
HTTPProxyPassword mypass
```

4.5 Closest mirrors

The `DatabaseMirror` directive in the config file specifies the database server `freshclam` will attempt (up to `MaxAttempts` times) to download the database from. The default database mirror is `database.clamav.net` but multiple directives are allowed. In order to download the database from the closest mirror you should configure `freshclam` to use `db.xx.clamav.net` where xx represents your country code. For example, if your server is in "Ascension Island" you should add the following lines to `freshclam.conf`:

```
DNSDatabaseInfo current.cvd.clamav.net
DatabaseMirror db.ac.clamav.net
DatabaseMirror database.clamav.net
```

The second entry acts as a fallback in case a connection to the first mirror fails for some reason. The full list of two-letters country codes is available at `http://www.iana.org/cctld/cctld-whois.htm`

5 Usage

5.1 Clam daemon

`clamd` is a multi-threaded daemon that uses *libclamav* to scan files against viruses. It may work in one of the two network modes, listening on a:

- Unix (local) socket
- TCP socket

The daemon is fully configurable via the `clamd.conf` file [5]. `clamd` recognizes the following commands:

- **PING**
  Check daemon state (should reply with "PONG").
- **VERSION**
  Print program and database versions.
- **RELOAD**
  Reload databases.
- **SHUTDOWN**
  Perform a clean exit.

[5] man 5 clamd.conf

- **SCAN file/directory** Scan file or directory (recursively) with archive support enabled (a full path is required).
- **RAWSCAN file/directory** Scan file or directory (recursively) with archive support disabled (a full path is required).
- **CONTSCAN file/directory** Scan file or directory (recursively) with archive support enabled and do not stop scanning if virus is found.
- **STREAM** Scan stream: `clamd` will return a new port number you should connect to and send data to scan.
- **SESSION, END** Start/end a `clamd` session - you can do multiple commands per TCP session (WARNING: due to the `clamd` implementation the **RELOAD** command will break the session).

and reacts to the special signals:

- **SIGTERM** - perform a clean exit
- **SIGHUP** - reopen a log file
- **SIGUSR2** - reload the database

5.2 Clamdscan

`clamdscan` is a simple `clamd` client. In many cases you can use it as a `clamscan` replacement but you must remember that:

- it only depends on `clamd`
- although it accepts the same command line options as `clamscan` most of them are ignored because they must be enabled directly in `clamd`, i.e. `clamd.conf`
- scanned files must be accessible for `clamd`
- it can't use external unpackers

5.3 Clamuko

Clamuko is a special thread in `clamd` that performs on-access scanning under Linux and FreeBSD and shares internal virus database with the daemon. **You must follow some important rules when using it:**

- Always stop the daemon cleanly - using the SHUTDOWN command or the SIGTERM signal. In other case you can lose an access to protected files until the system is restarted.
- Never protect a directory your mail-scanner software uses for attachment unpacking. Access to all infected files will be automatically blocked and the scanner (even `clamd`) won't be able to detect any virus. In the result **all infected mails will be delivered.**

For example, to protect a whole system add the following lines to `clamd.conf`:

```
ClamukoScanOnAccess
ClamukoIncludePath /
ClamukoExcludePath /proc
ClamukoExcludePath /temporary/dir/of/your/mail/scanning/software
```

You can also use clamuko to protect files on Samba/Netatalk but far more better and safe idea is to use the **samba-vscan** module 8.4.3. NFS is not supported because Dazuko doesn't intercept NFS access calls.

5.4 Output format

5.4.1 clamscan

`clamscan` by default writes all messages to **stderr**. Run it with `--stdout` enabled to redirect them to the standard output. An example of the `clamscan` output is:

```
/tmp/test/removal-tool.exe: Worm.Sober FOUND
/tmp/test/md5.o: OK
/tmp/test/blob.c: OK
/tmp/test/message.c: OK
/tmp/test/error.hta: VBS.Inor.D FOUND
```

When a virus is found its name is printed between the `filename:` and `FOUND` strings. In case of archives the scanner depends on libclamav and only prints the first virus found within an archive:

```
zolw@localhost:/tmp$ clamscan malware.zip
malware.zip: Worm.Mydoom.U FOUND
```

TIP: *You can force clamscan to list all infected files in an archive using –no-archive (that disables transparent decompressors built into libclamav) and external decompressors: –unzip –unrar....*

```
zolw@localhost:/tmp$ clamscan --no-archive --unzip malware.zip
Archive:  /tmp/malware.zip
  inflating: test1.exe
  inflating: test2.exe
  inflating: test3.exe
/tmp/clamav-77e7bfdbb2d3872b/test1.exe: Worm.Mydoom.U FOUND
/tmp/clamav-77e7bfdbb2d3872b/test2.exe: Trojan.Taskkill.A FOUND
/tmp/clamav-77e7bfdbb2d3872b/test3.exe: Worm.Nyxem.D FOUND
/tmp/malware.zip: Infected Archive FOUND
```

5.4.2 clamd

`clamd` uses a `clamscan` compatible output format:

```
zolw@localhost:~$ telnet localhost 3310
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
SCAN /home/zolw/test
/home/zolw/test/clam.exe: ClamAV-Test-File FOUND
Connection closed by foreign host.
```

In the **SCAN** mode it closes the connection when the first virus is found.

```
SCAN /home/zolw/test/clam.zip
/home/zolw/test/clam.zip: ClamAV-Test-File FOUND
```

CONTSCAN continues scanning even if virus was already found.
Error messages are printed in the following format:

```
SCAN /no/such/file
/no/such/file: Can't stat() the file. ERROR
```

6 LibClamAV

libclamav is a simple and easy way to add a virus protection to your software. The library is thread-safe and transparently recognizes and scans within archives, mail files, MS Office document files, executables and other file formats.

6.1 Licence

libclamav is licensed under the GNU GPL licence. That means you are **not allowed** to link commercial, close-source applications against it[6]. All software using libclamav must be GPL compliant.

6.2 Features

6.2.1 Archives and compressed files

The library has a built-in support for the following formats:

- Zip
- RAR (2.0)
- Tar
- Gzip
- Bzip2
- MS OLE2
- MS Cabinet Files
- MS CHM (Compiled HTML)
- MS SZDD compression format
- UPX (all versions)
- FSG (1.3, 1.31, 1.33, 2.0)
- Petite (2.x)

[6] You can still use clamd or clamscan instead

Due to license issues, support for RAR 3.0 archives is currently not available in libclamav (they will cause `RAR module failure.` error message). You can scan them with help of external unpackers in `clamscan`, though.

```
$ clamscan --unrar clam-error.rar
/home/zolw/test/clam-error.rar: RAR module failure.

UNRAR 3.00 freeware      Copyright (c) 1993-2002 Eugene Roshal


Extracting from /home/zolw/test/clam-error.rar

Extracting  clam.exe                                          OK
All OK
/tmp/44694f5b2665d2f4/clam.exe: ClamAV-Test-File FOUND
/home/zolw/test/clam-error.rar: Infected Archive FOUND
```

6.2.2 Mail files

Advanced mail scanner built into libclamav transparently scans e-mails for infected attachments. All popular UNIX mail formats are supported.

6.3 API

6.3.1 Header file

Every program using libclamav must include the `clamav.h` header file:

```
#include <clamav.h>
```

6.3.2 Database loading

The following set of functions provides an interface to database initialisation mechanisms:

```
int cl_loaddb(const char *filename, struct cl_node **root,
unsigned int *signo);

int cl_loaddbdir(const char *dirname, struct cl_node **root,
unsigned int *signo);
```

```
const char *cl_retdbdir(void);
```

`cl_loaddb` loads selected database while `cl_loaddbdir` loads all databases from a `dirname` directory. `cl_retdbdir` returns a default (hardcoded) database directory path. After an initialisation an internal database representation will be saved under `root` (which must initially point to NULL) and a number of loaded signatures will be **added** [7] to `virnum`. You can eventually pass NULL if you don't care about a signature counter. Both `cl_loaddb` and `cl_loaddbdir` functions return 0 on success and a non-negative value on failure.

```
    ...
    struct cl_node *root = NULL;
    int ret, signo = 0;

ret = cl_loaddbdir(cl_retdbdir(), &root, &signo);
```

6.3.3 Error handling

Use `cl_strerror` to convert error codes into human readable messages. The function returns a statically allocated string:

```
if(ret) {
    printf("cl_loaddbdir() error: %s\n", cl_strerror(ret));
    exit(1);
}
```

6.3.4 Database structure

Now initialise internal transitions with `cl_build`.

```
int cl_build(struct cl_node *root);
```

In our example:

```
if((ret = cl_build(root)))
    printf("cl_build() error: %s\n", cl_strerror(ret));
```

[7] Remember to initialize the virus counter variable with 0.

6.4 Database reloading

The most important thing is to keep the internal instance of the database up to date. You can watch database changes with the `cl_stat` functions family.

```
int cl_statinidir(const char *dirname, struct cl_stat *dbstat);
int cl_statchkdir(const struct cl_stat *dbstat);
int cl_statfree(struct cl_stat *dbstat);
```

Initialization:

```
    ...
    struct cl_stat dbstat;

memset(&dbstat, 0, sizeof(struct cl_stat));
cl_statinidir(dbdir, &dbstat);
```

To check for a change you only need to call `cl_statchkdir`:

```
if(cl_statchkdir(&dbstat) == 1) {
    reload_database...;
    cl_statfree(&dbstat);
    cl_statinidir(cl_retdbdir(), &dbstat);
}
```

Remember to reinitialize the structure after reload.

6.4.1 Data scan functions

It’s possible to scan a buffer, a descriptor, or a file with:

```
int cl_scanbuff(const char *buffer, unsigned int length,
const char **virname, const struct cl_node *root);

int cl_scandesc(int desc, const char **virname, unsigned
long int *scanned, const struct cl_node *root, const
struct cl_limits *limits, unsigned int options);

int cl_scanfile(const char *filename, const char **virname,
unsigned long int *scanned, const struct cl_node *root,
const struct cl_limits *limits, unsigned int options);
```

All the functions save a virus name under `virname` pointer. It points to a field in the internal database structure and must not be released directly. If the `scanned` pointer is not NULL the functions will increase a value represented by this pointer by a size of scanned data in `CL_COUNT_PRECISION` units. The last two functions also support archive limits required to protect against Denial of Service attacks.

```
struct cl_limits {
    int maxreclevel; /* maximal recursion level */
    int maxfiles; /* maximal number of files to be
                   * scanned within archive
                   */
    int maxratio; /* maximal compression ratio */
    short archivememlim; /* limit memory usage for bzip2 (0/1) */
    long int maxfilesize; /* archived files larger than this
                           * value will not be scanned
                           */
};
```

The `options` argument configures the scan engine and supports the following flags (that can be combined using bit operators):

- **CL_SCAN_STDOPT**
  This is an alias for a recommended set of scan options. You should use it to make your software ready for new features in future versions of libclamav.
- **CL_SCAN_RAW**
  It does nothing. Please use it (alone) if you don't want to scan any special files.
- **CL_SCAN_ARCHIVE**
  This flag enables transparent scanning of various archive formats.
- **CL_SCAN_BLOCKENCRYPTED**
  With this flag the library marks encrypted archives as viruses (Encrypted.Zip, Encrypted.RAR).
- **CL_SCAN_BLOCKMAX**
  Mark archives as viruses if `maxfiles`, `maxfilesize`, or `maxreclevel` limit is reached.
- **CL_SCAN_MAIL**
  It enables support for mail files.

- **CL_SCAN_MAILURL**
  The mail scanner will download and scan URLs listed in a mail body. This flag should not be used on loaded servers. Due to potential problems please do not enable it by default but make it optional.

- **CL_SCAN_OLE2**
  Enables support for Microsoft Office document files.

- **CL_SCAN_PE**
  This flag enables scanning withing Portable Executable files and allows libclamav to unpack UPX, Petite, and FSG compressed executables.

- **CL_SCAN_BLOCKBROKEN**
  libclamav will try to detect broken executables and mark them as Broken.Executable.

- **CL_SCAN_HTML**
  This flag enables HTML normalisation (including JScript decryption).

All functions return 0 (`CL_CLEAN`) if the file is clean, `CL_VIRUS` when virus is detected and an another value on failure.

```
    ...
    struct cl_limits limits;
    const char *virname;

memset(&limits, 0, sizeof(struct cl_limits));
/* maximal number of files in archive */;
limits.maxfiles = 1000
/* maximal archived file size */
limits.maxfilesize = 10 * 1048576; /* 10 MB */
/* maximal recursion level */
limits.maxreclevel = 5;
/* maximal compression ratio */
limits.maxratio = 200;
/* disable memory limit for bzip2 scanner */
limits.archivememlim = 0;

if((ret = cl_scanfile("/home/zolw/test", &virname, NULL, root,
&limits, CL_STDOPT)) == CL_VIRUS) {
    printf("Detected %s virus.\n", virname);
} else {
    printf("No virus detected.\n");
    if(ret != CL_CLEAN)
```

```
        printf("Error: %s\n", cl_strerror(ret));
}
```

6.4.2 Memory

Because the internal database uses a few megabytes of memory, you should release it if you no longer need to scan files.

```
void cl_free(struct cl_node *root);
```

6.4.3 clamav-config

Use `clamav-config` to check libclamav compilation information.

```
zolw@localhost:~$ clamav-config --libs
-L/usr/local/lib -lz -lbz2 -lgmp -lpthread
zolw@localhost:~$ clamav-config --cflags
-I/usr/local/include -g -O2
```

6.4.4 Example

You will find an example scanner application in the clamav sources (/example). Remember that all programs based on libclamav must be linked against it:

```
gcc -Wall ex1.c -o ex1 -lclamav
```

6.5 CVD format

CVD (ClamAV Virus Database) is a digitally signed tarball file that contains one or more databases. The header is a 512 bytes long string with colon separated fields:

```
ClamAV-VDB:build time:version:number of signatures:functionality
level required:MD5 checksum:digital signature:builder name:build time (sec)
```

`sigtool --info` displays detailed information on CVD files:

```
zolw@localhost:/usr/local/share/clamav$ sigtool -i daily.cvd
Build time: 11 Sep 2004 21-07 +0200
Version: 487
# of signatures: 1189
Functionality level: 2
Builder: ccordes
MD5: a3f4f98694229e461f17d2aa254e9a43
Digital signature: uwJS6d+y/9g5SXGE0Hh1rXyjZW/PGK/zqVtWWVL3/tfHEn
A17z6VB2IBR2I/OitKRYzmVo3ibU7bPCJNgi6fPcW1PQwvCunwAswvR0ehrvY/4ks
UjUOXo1VwQlW7l86HZmiMUSyAjnF/gciOSsOQa9Hli8D5uET1RDzVpoWu/id
Verification OK.
```

7 Frequently Asked Questions

The FAQ section is maintained by Luca Gibelli.

- **What does *WARNING: Current functionality level = 1, required = 2* mean?**
  The functionality level of the database determines which scanner engine version is required to use all of its signatures. If you don't upgrade immediately you will be in big trouble.

- **What does *Your ClamAV installation is OUTDATED* mean?**
  You'll get this message whenever a new version of ClamAV is released. In order to detect all the latest viruses, it's not enough to keep your database up to date. You also need to run the latest version of the scanner. You can find the latest release at `http://www.clamav.net` under the `stable` link. Running the latest stable release also improves stability.

- **What does *WARNING: DNS record is older than 3 hours* mean?**
  freshclam attempts to detect potential problems with DNS caches and switches to the old mode if something looks suspicious. If this message appears seldomly, you can safely ignore it. If you get the error everytime you run freshclam, you should check your dns settings.

- **What does *SECURITY WARNING: NO SUPPORT FOR DIGITAL SIGNATURES* mean?**
  The ClamAV package requires the GMP library to verify the digital signature of the virus database. When building ClamAV you need the GMP library and its headers: if you are using Debian just run `apt-get install libgmp3-dev`, if you are using an RPM based distribution install the gmp-devel package.

- **How often is the virus database updated?**
  The virus database is usually updated many times per week. Check out `http://news.gmane.org/gmane.comp.security.virus.clamav.virusdb/` to see our response times to new threats. The virusdb team tries to keep up with the latest worm in the wild. When a new worm spreads out, often it is less than one hour before we release a database update. You can contribute to make the virusdb updating process more efficient by submitting samples of viruses via our web interface.

- **I tried to submit a sample through the web interface, but it said the sample is already recognized by ClamAV. My clamscan tells me it's not. I already updated my database, what's wrong with my setup?**
  Please run clamscan with the –mbox option. Also check that freshclam and clamscan are using the same path for storing/reading the database.

- **ClamAV crashes/hangs/doesn't compile/doesn't start. Did I find a bug?**
  Before reporting a bug, please download the latest CVS code and try to reproduce the bug with it. Chances are the bug you encountered has already been fixed. If you really feel like you found a bug, please send a message `bugs*clamav.net`.

- **How do I automatically restart clamd when it dies?**
  Set up a cronjob which checks that clamd is up and running, every XX minutes. You can find an example script in the `contrib/clamdwatch/` directory.

- **How do I keep my virus database up to date?**
  ClamAV comes with freshclam, a tool which periodically checks for new database releases and keeps your database up to date.

- **I'm running ClamAV on a lot of clients on my local network. Can I mirror the database locally so that each client doesn't have to download it from your servers?**
  Sure, install a proxy server and then configure your freshclam clients to use it (watch for the `HTTPProxyServer` parameter in `man freshclam.conf`). Alternatively, you can configure a local webserver on one of your machines (say machine1.mylan) and let freshclam download the *.cvd files from `http://database.clamav.net/` to the webserver's `DocumentRoot`. Finally, change `freshclam.conf` on your clients so that it reads: `DatabaseMirror machine1.mylan` First the database will be downloaded to the local webserver and then the other clients on the network will update their copy of the database from it.

- **How can I list the virus signature names contained in the database?**
  If you are using a recent version of ClamAV just run: `$sigtool --list-sigs`

- **I found an infected file in my HD/floppy/mailbox, but ClamAV doesn't recognize it yet. Can you help me?**
  Our virus database is kept up to date with the help of the community. Whenever you find a new virus which is not detected by ClamAV you should submit it on our website (go to `www.clamav.net` and click on *submit sample*). The virusdb team will review your submission and update the database if necessary. Before submitting a new sample:
  - check that the value of `DatabaseDirectory`, in both `clamd.conf` and `freshclam.conf`, is the same
  - update your database by running freshclam
- **Why is ClamAV calling the XXX virus with another name?**
  This usually happens when we add a signature before other AV vendors. No well-known name is available at that moment so we have to invent one. Renaming the virus after a few days would just confuse people more, so we usually keep on using our name for that virus. The only exception is when a new name is established soon after the signature addition. You can find more info about this in the virus naming page at `http://www.clamav.net/cvdinfo.html`
- **How do I know when database updates are released?**
  Subscribe to the *clamav-virusdb* mailing-list.
- **How can I scan a file on my hard disk for viruses without installing ClamAV?**
  Use the online scanning tool available at `http://test-clamav.power-netz.de/`
- **I found a false positive in ClamAV virus database. What shall I do?**
  Fill the form at `http://www.clamav.net/sendvirus.html` Be sure to select *The file attached is... a false positive*
- **How do I verify the integrity of ClamAV sources?**
  Using GnuPG (`http://www.gnupg.org/`) you can easily verify the authenticity of your stable release downloads by using the following method:
  - Download Tomasz Kojm's key from the clamav.net site:
    `$ wget http://www.clamav.net/gpg/tkojm.gpg`
  - Import the key into your local public keyring:
    `\$ gpg --import tkojm.gpg`
  - Download the stable release AND the corresponding .sig file to the same directory.

```
$ wget http://prdownloads.sourceforge.net/clamav/clamav-X.XX.tar.gz
$ wget http://prdownloads.sourceforge.net/clamav/clamav-X.XX.tar.gz.sig
```

  - Verify that the stable release download is signed with the proper key:
    `$ gpg --verify clamav-X.XX.tar.gz.sig`
  - Make sure the resulting output contain the following information:
    `Good signature from Tomasz Kojm (tk*lodz.tpnet.pl)`

- **Can ClamAV disinfect files?**
  No, it can't. We will add support for disinfecting OLE2 files in one of the next stable releases. There are no plans for disinfecting other types of files. There are many reasons for it: cleaning viruses from files is virtually pointless these days. It is very seldom that there is anything useful left after cleaning, and even if there is, would you trust it?

- **When using clamscan, is there a way to know which message within an mbox is infected?**
  No, clamscan stops at the first infected message. You can convert the mbox to Maildir format, run clamscan on it and then convert it back to mbox format. There are many tools available which can convert to and from Maildir format, e.g: formail, mbox2maildir, and maildir2mbox.

- **I'm running qmail+Qmail-Scanner+ClamAV and get the following error in my mail logs: *clamdscan: corrupt or unknown clamd scanner error or memory/resource/perms problem*. What's wrong with it?**
  Most likely clamd is not running at all, or you are running Qmail-Scanner and clamd under a different uid. If you are running Qmail-Scanner as qscand (default setting) you could put `User qscand` inside your clamd.conf file and restart clamd. Remember to check that qscand can create clamd.ctl (usually located at `/var/run/clamav/clamd.ctl`). The same applies to the log file.

- **How do I use ClamAV with p3scan?**
  Add the following lines to your pop3vscan configuration file:

```
virusregexp = .*: (.*) FOUND
scanner = /usr/bin/clamdscan --no-summary -i
scannertype = basic
```

- **Where can I ask questions about using ClamAV?**
  Subscribe to our *clamav-users* mailing-list at `http://www.clamav.net/ml.html`

- **Where can I get the latest CVS snapshot of ClamAV?**
  Basically, there are two ways:

  - Run
    `cvs -d:pserver:anonymous @ cvs.sourceforge.net:/cvsroot/clamav co clamav-deve`
  - Visit `http://www.clamav.net/snapshot/`

- **I'm a MS Windows user. Can I take advantage of ClamAV virus protection?**
  Yes, you can use ClamWin, a port of ClamAV for win32 systems with a very nice graphic interface. Download it at `http://www.clamwin.net`

- **Where can I find more information about ClamAV?**
  Please read this documentation. You can also try searching the mailing list archives. If you can't find the answer, you can ask for support on the clamav-users mailing-list, but please before doing it, search the archives! Also, make sure that you don't send HTML-ized email messages and that you don't top-post (these violate the netiquette and lessen your chances of being answered).

- **How can I contribute to the ClamAV project?**
  There are many ways to contribute to the ClamAV project. See the donations page (`http://www.clamav.net/donate.html` for more info.

8 Third party software

The following software supports ClamAV. It's specified which elements are supported, please note that if a program doesn't support clamd you can use clamdscan instead of clamscan.

8.1 *MTA + ClamAV*

8.1.1 amavisd-new

Homepage: `http://www.ijs.si/software/amavisd/`
Supports: clamd, clamscan

amavisd-new is a rewritten version of amavis maintained by Mark Martinec.

Installation:
clamscan is enabled automatically if clamscan binary is found at amavisd-new startup time. clamd is activated by uncommenting its entry in the @av_scanners list, file /etc/amavisd.conf.

8.1.2 AMaViS - "Next Generation"

Homepage: `http://sourceforge.net/projects/amavis/`
Supports: clamscan

AMaViS-ng is a rewritten, more modular version of amavis-perl/amavisd, developed by Hilko Bengen. **Installation:**

Please download the newest version (at least 0.1.4). After installation (which is quite easy), please uncomment the following line in amavis.conf:

```
virus-scanner = CLAM
```

and if it's needed change the path to clamscan in the `[CLAM]` section:

```
[CLAM]

clamscan = /usr/local/bin/clamscan
```

8.1.3 ClamdMail

Homepage: `http://clamdmail.sf.net/`
Supports: clamd

A mail processing client for ClamAV. Small, fast and easy to install.

8.1.4 cgpav

Homepage: `http://program.farit.ru/`
Supports: clamd

This is a fast (written in C) CommuniGate Pro anti-virus plugin with support for clamd.

8.1.5 ClamCour

Homepage: `http://sourceforge.net/projects/clamcour/`
Supports: clamd

ClamCour is a Courier-MTA multithread filter that allows Courier to scan mail for viruses using Clam AntiVirus package.

8.1.6 clamfilter

Homepage: `http://www.ensita.net/products/clamfilter/`
Supports: clamd

Clamfilter is a small, secure, and efficient content filter for Postfix designed for filtering messages efficiently through the clamd daemon.

8.1.7 ClamSMTP

Homepage: http://memberwebs.com/nielsen/software/clamsmtp/
Supports: clamd

ClamSMTP is an SMTP filter for Postfix and other mail servers that checks for viruses using the ClamAV anti-virus software. It aims to be lightweight, reliable, and simple rather than have a myriad of options. Written in C without major dependencies.

8.1.8 clapf

Homepage: http://thorium.ath.cx/clapf/
Supports: libclamav

Clapf is a clamav based virus scanning and anti-spam content filter for Postfix.

8.1.9 DSpamPD

Homepage: http://caspian.dotconf.net/menu/Software/DspamPD/
Supports: clamd

DspamPD is a transparent SMTP proxy daemon that passes email through DSPAM. It can also pass mail through ClamAV as well, providing you with a one-stop anti-spam / anti-virus smtp proxy with no extra perl modules!

8.1.10 exiscan

Homepage: http://duncanthrax.net/exiscan-acl/
Supports: clamscan, clamd

exiscan is a patch against exim version 4, providing support for content scanning in email messages received by exim. Four different scanning facilities are supported: antivirus, antispam, regular expressions, and file extensions.

8.1.11 Gadoyanvirus

Homepage: http://oss.mdamt.net/gadoyanvirus/
Supports: libclamav

gadoyanvirus is a (yet another) virus stopper for qmail. It replaces the original qmail-queue program. It scans incoming messages using the ClamAV anti-virus library. Suspected message will be quarantined and (optionally) a notification message will be sent to the recipients. By default, gadoyanvirus needs QMAILQUEUE patched qmail installation.

8.1.12 IVS Milter

Homepage: `http://ivs-milter.lbsd.net/`
Supports: clamd

IVS Milter is a virus and spam scanning milter. The name stands for Industrial Virus + Spam milter. It's designed to be used by anything from home users to large ISPs.

8.1.13 j-chkmail

Homepage: `http://j-chkmail.ensmp.fr/`
Supports: libclamav, clamd

j-chkmail is a fast (written in C) filter for sendmail. It does spam and dangerous content (virus) filtering with help of ClamAV. The program supports many modes of monitoring and run time controlling and was designed to work on highly loaded servers. It's an open source software available for free to registered users (for non-commercial usage).

8.1.14 Mail Avenger

Homepage: `http://www.mailavenger.org/`
Supports: clamscan

Mail avenger is a highly-configurable SMTP server. It allows you to reject spam during mail transactions, before spooling messages in your local mail queue. You can specify site-wide default policies for filtering mail, but individual users can also craft their own policies by creating avenger scripts in their home directories.

8.1.15 Mailnees

Homepage: `http://mailnees.kicks-ass.org/`
Supports: clamdscan

Mailnees is an open source mail content filter for Sendmail and Postfix.

8.1.16 MailScanner

Homepage: `http://www.mailscanner.info/`
Supports: clamscan

MailScanner scans all e-mail for viruses, spam and attacks against security vulnerabilities. It is not tied to any particular virus scanner, but can be used with any combination of 14 different virus scanners, allowing sites to choose the ”best of breed” virus scanner.

8.1.17 Maverix

Homepage: http://www.crystalballinc.com/vlad/software/maverix/
Supports: clamscan

Maverix is AOLserver module that implements SMTP protocol and acts as a SMTP proxy with anti-spam and anti-virus capabilities.

8.1.18 MIMEDefang

Homepage: http://www.roaringpenguin.com/mimedefang
Supports: clamscan, clamd

This is an efficient mail scanner for Sendmail/milter.

8.1.19 mxGuard for IMail

Homepage: http://www.mxguard.com/postmaster/
Supports: clamscan

mxGuard is a spam filter for Ipswitch IMail mail server running on Windows platforms. It also includes free hooks to major anti-virus engines including ClamAV.

8.1.20 OdeiaVir

Homepage: http://odeiavir.sourceforge.net/
Supports: clamdscan

OdeiaVir is an e-mail filter for qmail or Exim.

8.1.21 OpenProtect

Homepage: http://opencompt.com/
Supports: ClamAV via MailScanner

OpenProtect is a server side e-mail protection solution consisting of MailScanner, Spamassassin, ClamAV with support for Sendmail, Postfix, Exim and qmail. It also consists of a fully automatic installer and uninstaller, which configures everything automatically including setting up perl modules and virus scanner settings.

8.1.22 Protea AntiVirus Tools

Homepage: http://www.proteatools.com/
Supports: clamd

Protea AntiVirus Tools for Lotus Domino scans and cleans automatically attached files

and other objects in Domino mail. Clam AntiVirus scanner is used for virus detection. Fully configurable scheduled database scanning offers an additional layer of protection.

8.1.23 PTSMail Utilities

Homepage: `http://www.scanmail-software.com/`
Supports: clamscan

PTSMail uses clamscan as part of the ptsfilter (a sendmail milter).

8.1.24 pymavis

Homepage: `http://mplayerhq.hu/~arpi/pymavis/`
Supports: clamscan

pymavis is an email parser, similar to the old amavis (or amavis-perl). The primary goal is to retrieve all attachments from an email, and then run various virus scanners over them. The parser can deal with damaged and truncated messages, non-RFC compliant or broken MIME syntax headers, inline (non-MIME) attachments, can decode base64, quoted-printable, uuencoded and binhex 4.0 (hqx) encodings.

8.1.25 Qmail-Scanner

Homepage: `http://qmail-scanner.sf.net/`
Supports: clamscan

Please increase the softlimit value if you are going to use it with clamscan.

8.1.26 qscanq

Homepage: `http://budney.homeunix.net:8080/users/budney/software/qscanq/index.html`
Supports: clamscan

qscanq replaces qmail-queue. It initiates a scan (using clamscan or clamdscan) on an incoming email, and returns the exit status of the scanner or of qmail-queue to the caller.

8.1.27 qSheff

Homepage: `http://www.enderunix.org/qsheff`
Supports: clamdscan, clamd

The tool allows running anti-virus and content filtering software simultaneously. Supports ClamAV for virus checking and Zabit for content filtering.

8.1.28 RevolSys SMTP kit for Postfix

Homepage: http://smtp.revolsys.org/
Supports: ClamAV via amavisd-new

The RevolSyS SMTP kit for Postfix provides an antispam and antivirus tools installation. It uses amavisd-new, Spamassassin, ClamAV, and Razor. It aims to enhance an already-installed mail server running Postfix.

8.1.29 Sagator

Homepage: http://www.salstar.sk/sagator/
Supports: clamscan, clamd, libclamav

This program is an email antivirus/antispam gateway. It is an interface to the postfix (or any other smtpd), which runs antivirus and/or spamchecker. Its modular architecture can use any combination of antivirus/spamchecker according to configuration.

8.1.30 Scrubber

Homepage: http://projects.gasperino.org/scrubber/
Supports: libclamav

Scrubber is a server-side daemon for filtering mail content. It attempts to solve the issues that plague many server-side content filtering solutions such as extensibility, speed, SMTP-specific dependencies, and virtual hosting. The core of the project a client-server daemon that accepts raw content from SMTP-side client applications, breaking the message into MIME parts, and then sending the content through a series of loadable filter plugins to handle the message accordingly. The final message is sent back to the client-side programs for SMTP reinjection.

8.1.31 Secure Mail Intelligence!

Homepage: http://www.m2smi.com/
Supports: libclamav

SMI! is a server side e-mail protection solution that combines firewall elements, intrusion detection system, anti-virus and anti-spam modules. SMI! can use up to 7 anti-virus scanners (including ClamAV) at the same time and 3 different spam filtering engines. A built-in SMTP engine allows SMI! to directly send mail alerts. Other features include: Routing & Queuing Module, Disclaimer & Messages Module, Updater Module, Policy CheckModule, Mail Storage Module, Image Analysis Module, Cryptography Series and Mail Analysis. SMI! runs on Microsoft Windows 98/NT/2k/XP/2003 platforms (both Professional and Server releases), Linux (i586), OpenBSD, FreeBSD and Solaris 9 (x86 and SPARC) and supports almost all SMTP software including Lotus Domino

and Microsoft Exchange. The daemon part based on libclamav is licensed under the GPL.

8.1.32 simscan

Homepage: `http://www.inter7.com/?page=simscan`
Supports: clamscan

Simscan is a mail filter for qmail, designed to block attachments during the SMTP conversation. It is open source and only uses open components. Very efficent (written in C).

8.1.33 smtpfilter

Homepage: `http://www.gtoal.com/spam/smtpfilter.c.html`
Supports: clamscan

smtpfilter is a filter for an SMTP session which passes the session through transparently in real time, except for the DATA command which is intercepted in order to scan the data for spam and/or viruses.

8.1.34 smtp-vilter

Homepage: `http://www.etc.msys.ch/software/smtp-vilter/`
Supports: clamd

smtp-vilter is a high performance content filter for sendmail using the milter API. The software scans e-mail messages for viruses and drops or marks infected messages. ClamAV is the default scanner backend.

8.1.35 Zabit

Homepage: `http://www.enderunix.org/zabit`
Supports: clamscan

Zabit is a content and attachment filter for Qmail.

8.2 *MTA + POP3 Proxy + ClamAV*

8.2.1 ClamMail

Homepage: `http://www.bransoft.com/`
Supports: libclamav

ClamMail is an anti-virus POP3 proxy for Windows.

8.2.2 POP3 Virus Scanner Daemon

Homepage: http://p3scan.sourceforge.net/
Supports: clamscan

This is a full-transparent proxy-server for POP3-clients. It runs on a Linux box with iptables (for port re-direction). It can be used to provide POP3 email scanning from the Internet, to any internal network and is ideal for helping to protect your Other OS LAN from harm, especially when used in conjunction with a firewall and other Internet Proxy servers.

8.3 *Web/FTP Proxy + ClamAV*

8.3.1 DansGuardian Anti-Virus Patch

Homepage: http://www.harvest.com.br/asp/afn/dg.nsf
Supports: clamscan

DG AntiVirus Patch is a GPL addon that takes the virus scanning capabilities of ClamAV and integrates them into the content filtering web proxy DansGuardian.

8.3.2 Frox

Homepage: http://www.hollo.org/frox/
Supports: clamscan

Frox is a transparent FTP proxy which is released under the GPL. It optionally supports caching (either through an external http cache (eg. squid), or by maintaining a cache locally), and/or running a virus scanner on downloaded files. It is written with security in mind, and in the default setup it runs as a non root user in a chroot jail.

8.3.3 mod_clamav

Homepage: http://software.othello.ch/mod_clamav/
Supports: libclamav, clamd

mod_clamav is an Apache virus scanning filter. It was written and is currently maintained by Andreas Muller.

8.3.4 SafeSquid

Homepage: http://www.safesquid.com/
Supports: clamd

SafeSquid is one of the most feature rich Content Filtering Internet Proxies. It is an ideal content filter for other proxies like Squid, because it chains with them via request

forwarding, ICAP, CARP, ICP. It has a browser based GUI for remote management, a powerful profiles feature to implement user, IP, network based multiple and unique policies. SafeSquid supports PAM and NTLM Authentication besides using any form of external databases, the use of URL Blacklists, to deliver category based content filtering besides, keyword, mime, header, cookie filtering. SafeSquid has an Advanced Bandwidth Management System, to create very granular enterprise and network wide bandwidth usage policies. SafeSquid Free Edition is not time or user-limited.

8.3.5 SquidClamAV Redirector

Homepage: `http://www.jackal-net.at/tiki-read_article.php?articleId=1`
Supports: libclamav

SquidClamAV Redirector is a Squid helper script which adds virus scanning for defined filename extensions. It has been tested with Python, pyclamav, ClamAV, and Squid. SCAVR handles the request as given from Squid, downloads the URL, and scans it for known viruses. It rewrites the URL from Squid to a blocked URL or an information page with information about the scanning results.

8.3.6 Viralator

Homepage: `http://viralator.sourceforge.net/`
Supports: clamscan

Viralator is a perl script that virus scans http downloads on a linux server after passing through the squid proxy server.

8.4 *Filesystem + ClamAV*

8.4.1 Dazuko

Homepage: `http://www.dazuko.org/`
Supports: clamuko

This project provides a kernel module, which provides 3d-party applications an interface for file access control. It was originally developed by H+BEDV Datentechnik GmbH to be used for on-access virus scanning. Other uses include a file-access monitor/logger or external security implementations. It operates by intercepting file-access calls and passing the file information to a 3rd-party application. The 3rd-party application then has the opportunity to tell the kernel module to allow or deny the file-access. The 3rd-party application also receives information about the file, type of access, process id, and user id.

8.4.2 Famuko

Homepage: http://www.campana.vi.it/ottavio/Progetti/Famuko/
Supports: libclamav

Famuko is an on-access scanner based on libfam and working in a userspace.

8.4.3 OpenAntiVirus samba-vscan

Homepage: http://www.openantivirus.org/projects.php#samba-vscan
Supports: clamd

samba-vscan provides on-access scanning of Samba shares. It supports Samba 2.2.x/3.0 with working virtual file system (VFS) support.

8.5 *Mail User Agent + ClamAV*

8.5.1 clamailfilter

Homepage: http://quiston.tpsa.com/hacks/clamailfilter.xhtml
Supports: clamscan, clamdscan

clamailfilter is a Python script that provides anti-virus scanning via procmailrc.

8.5.2 ClamAssassin

Homepage: http://drivel.com/clamassassin/
Supports: clamscan

clamassassin is a simple script for virus scanning with clamscan which works similarily to spamassassin. It's designed for integration with procmail.

8.5.3 clamscan-procfilter

Homepage: http://www.virtualblueness.net/~blueness/clamscan-procfilter/
Supports: clamscan

A procmail filter for clamscan to work in conjunction with procmail. A new email field, X-CLAMAV, with all the viruses found, is generated in the email header.

8.5.4 KMail

Homepage: http://kmail.kde.org/
Supports: clamscan

KMail is a fully-featured email client that fits nicely into the K Desktop Environment, KDE. It supports attachment scanning with clamscan.

8.5.5 MyClamMailFilter

Homepage: http://muncul0.w.interia.pl/projects.html#myclammailfilter
Supports: clamscan

MyClamMailFilter is an e-mail filter for procmail or maildrop. When a virus is found, it renames attachments and modifies the subject. It can also rename potentially dangerous attachments looking at their extensions. The software is simple, fast and easy to customize.

8.5.6 OpenWebMail

Homepage: http://openwebmail.com/openwebmail/
Supports: clamscan

Open WebMail by default can use ClamAV as the external viruscheck module to scan messages fetched from pop3 servers or all incoming messages. If a message or its attachments is found to have virus, Open WebMail will move the message from INBOX to the VIRUS folder automatically.

8.5.7 QClam

Homepage: http://sageshome.net/oss/qclam.php
Supports: clamscan

QClam is a simple program to plug ClamAV antivirus to your QMail mailbox. It runs from your /.qmail file, receives incoming messages from QMail and scans them using clamscan; if a virus found, it returns 99 to QMail telling it that the message should not be processed (and it just gets removed). QClam also writes results of scanning into log file: /qclam.

8.5.8 QMVC - Qmail Mail and Virus Control

Homepage: http://www.fehcom.de/qmail/qmvc.html
Supports: clamdscan, clamscan

QMVC is an unidirectional mail filter for qmail. It works in conjunction with the ”dot-qmail” mechanism for qmail-local and is entirely designed for qmail (no additional patches required).

8.5.9 Sylpheed Claws

Homepage: http://claws.sylpheed.org/
Supports: libclamav

Sylpheed Claws is a bleeding edge branch of Sylpheed, a light weight mail user agent

for UNIX. It can scan attachments in mail received from POP, IMAP or a local account and optionally delete the mail or save it to a designated folder.

8.5.10 SoftlabsAV

Homepage: http://antivirus.softlabs.info/
Supports: clamscan

Softlabs AntiVirus is a generic anti-virus filter for incoming mail servers on Unix, running as plugin for procmail. In addition, it plugs to the Clam AntiVirus scanner (clamscan) if available.

8.6 *Graphical User Interface + ClamAV*

8.6.1 AVScan

Homepage: http://wolfpack.twu.net/Endeavour2/contrib/index.html#avscan
Supports: libclamav

AVScan is an anti-virus scanner for Endeavour Mark II that uses the ClamAV library. It allows you to create a list of scan items for frequently scanned locations and features easy virus database updating, all in a simple GUI environment.

8.6.2 BeClam

Homepage: http://www.bebits.com/app/3930/
Supports: ClamAV

BeClam is a port of ClamAV for the BeOS operating system.

8.6.3 Clamaktion

Homepage: http://web.tiscali.it/rospolosco/clamaktion/
Supports: clamscan

clamaktion is a little utility which allows KDE 3 users to scan files and directories with clamscan from the right-click Konqueror menu.

8.6.4 ClamShell

Homepage: http://home.comcast.net/~schwalbrichard/
Supports: clamscan

ClamShell is a GUI frontend, written in Java, for the Linux version of ClamAV.

8.6.5 ClamTk

Homepage: http://www.rootshell.be/~phen0m/clamtk/
Supports: ClamAV

ClamTk is a perl-tk GUI for ClamAV.

8.6.6 clamXav

Homepage: http://www.markallan.co.uk/clamXav
Supports: ClamAV

clamXav is a virus scanner with GUI for Mac OS X.

8.6.7 ClamWin

Homepage: http://clamwin.sourceforge.net/
Supports: clamscan, freshclam

ClamWin provides Graphical User Interface to Clam AntiVirus scanning engine. It allows to select and scan a folder or file, configure settings and update virus databases. It also includes a Windows Taskbar tray icon. ClamWin also features a context menu handler for Windows Explorer which installs Scan into the right-click explorer menu for files and folders. The package comes with an installer built with InnoSetup. Cygwin dlls are included.

8.6.8 FETCAV

Homepage: http://www.thymox.uklinux.net/
Supports: clamscan

FETCAV stands for Front End To Clam AntiVirus. It's a GUI interface to ClamAV and requires Xdialog.

8.6.9 KlamAV

Homepage: http://sourceforge.net/projects/klamav/
Supports: ClamAV

ClamAV Anti-Virus protection for the KDE desktop. The features include: 'on access' scanning, manual scanning, quarantine management, downloading updates, mail scanning (KMail/Evolution), automated installation (ClamAV and Dazuko pre-packaged).

8.6.10 wbmclamav

Homepage: http://wbmclamav.labs.libre-entreprise.org/
Supports: ClamAV

wbmclamav is a Webmin module to manage Clam AntiVirus, written by Emmanuel Saracco.

8.7 *Library + ClamAV*

8.7.1 ClamAVPlugin

Homepage: http://wiki.apache.org/spamassassin/ClamAVPlugin
Supports: libclamav via File::Scan::ClamAV

A ClamAV plugin for SpamAssassin 3.x.

8.7.2 clamavr

Homepage: http://raa.ruby-lang.org/list.rhtml?name=clamavr
Supports: libclamav

Ruby binding for ClamAV.

8.7.3 D bindings for ClamAV

Homepage: http://dmd.kuehne.cn/diverse.html#clamav_d
Supports: ClamAV

ClamAV bindings for the D programming language (http://digitalmars.com/d/).

8.7.4 File::Scan::ClamAV

Homepage: http://search.cpan.org/~cfaber/File-Scan-ClamAV-1.06/lib/File/Scan/ClamAV.pm
Supports: clamd

Scan files and control clamd directly from Perl.

8.7.5 Mail::ClamAV

Homepage: http://cpan.gossamer-threads.com/modules/by-authors/id/S/SA/SABECK/
Supports: libclamav

Perl binding for ClamAV.

8.7.6 php-clamav

Homepage: http://freshmeat.net/projects/php-clam/
Supports: libclamav

php-clamav is a small module that implements a limited subset of the libclamav API in order to scan buffers and files from within PHP.

8.7.7 pyclamav

Homepage: http://xael.org/norman/python/pyclamav/index.html
Supports: libclamav

Python binding for ClamAV.

8.7.8 WRAVLib

Homepage: http://www.wolfereiter.com/wravlib/
Supports: clamscan, clamd

WRAVLib is an extensible integration library to provide a virus security counter measure for MONO/.NET applications. WRAVLib is written in pure C# and has been tested with Microsoft .NET 1.1 and Novell Mono 1.0.1.

8.8 *Miscellaneous + ClamAV*

8.8.1 INSERT

Homepage: http://www.inside-security.de/INSERT_en.html
Supports: ClamAV

INSERT (the Inside Security Rescue Toolkit) aims to be a multi-functional, multi-purpose disaster recovery and network analysis system. It boots from a credit card-sized CD-ROM and is basically a stripped-down version of Knoppix. It features good hardware detection, fluxbox, emelfm, links-hacked, ssh, tcpdump, nmap, chntpwd, and much more. It provides full read-write support for NTFS partitions (using captive), and the ClamAV virus scanner (including the signature database).

8.8.2 Local Area Security

Homepage: http://www.localareasecurity.com/
Supports: ClamAV

Local Area Security Linux is a Live CD distribution with a strong emphasis on security tools and small footprint. It can be used to run ClamAV from a CDROM.

8.8.3 mailgraph

Homepage: http://people.ee.ethz.ch/~dws/software/mailgraph/
Supports: clamd

mailgraph is a very simple mail statistics RRDtool frontend for Postfix that produces daily, weekly, monthly and yearly graphs of received/sent and bounced/rejected mail (SMTP traffic).

8.8.4 mailman-clamav

Homepage: http://www.tummy.com/Software/mailman-clamav/
Supports: clamd

This module includes a Mailman handler for scanning incoming messages through ClamAV. The handler allows Mailman to be configured to hold or discard messages which contain viruses. Particularly useful is the discard option, which prevents list administrators from having to manually deal with viruses.

8.8.5 Moodle

Homepage: http://moodle.org/
Supports: clamscan

Moodle is a course management system - a software package designed to help educators create quality online courses. It can use ClamAV to scan files submitted by students.

8.8.6 nclamd

Homepage: http://www.kyzo.com/nclamd/
Supports: libclamav

nclamd, nclamav-milter and nclamdscan are rewritten versions of the original tools and use processes instead of threads, and ripMIME instead of the clamav built-in MIME decoder.

8.8.7 qmailmrtg7

Homepage: http://www.inter7.com/qmailmrtg7/
Supports: ClamAV

qmailmrtg7 utilizes qmail and tcpserver/multilog's extensive logging capabilities to create mrtg graphs. It efficiently processes the log files and can graph viruses found by ClamAV.

8.8.8 redWall Firewall

Homepage: `http://redwall.sourceforge.net/`
Supports: ClamAV

redWall is a bootable CD-ROM firewall which focuses on web-based reporting of the firewall's status. It supports virus filtering with amavisd-new and ClamAV.

8.8.9 Scan Log Analyzer

Homepage: `http://pandaemail.sourceforge.net/av-tools/`
Supports: ClamAV

Scan analyzer allows you to plot and view graphical representation of log data from virus logs of RAV, ClamAV and Vexira.

8.8.10 snort-inline

Homepage: `http://snort-inline.sourceforge.net/`
Supports: libclamav

snort-inline ships with a ClamAV preprocessor that will scan your network traffic for viruses. You can choose which protocols must be monitored. If a virus is detected, snort-inline can send a reset and drop the relative packets.

9 Credits

9.1 Database mirrors

Thanks to the help of many companies and organisations we have a few dozens of very fast and reliable mirrors. Moreover, our advanced push-mirroring mechanism allows database maintainers to update all of them in less than one minute!

Mirror	IP	Location	Administrator
clamav.man.olsztyn.pl	213.184.16.3	Olsztyn, Poland	Robert d'Aystetten <dart*man.olsztyn.pl>
avmirror1.prod.rxgsys.com	64.74.124.90	USA	Graham Wooden <graham*rxgsys.com>
avmirror2.prod.rxgsys.com	207.201.202.73	USA	Graham Wooden <graham*rxgsys.com>
clamav.power-netz.de	212.162.12.159	Dusseldorf, Germany	Andreas Gietl <a.gietl*e-admin.de>
clamav.essentkabel.com	195.85.130.84	Netherlands	Chris van Meerendonk <mirror*essentkabel.com>
clamav.inet6.fr	62.210.153.201 62.210.153.202	France	Lionel Bouton <clamavdb*inet6.fr>
clamav.netopia.pt	193.126.14.29	Portugal	Miguel Bettencourt Dias <mbd*netopia.pt>
clamav.sonic.net	209.204.175.217	USA	Kelsey Cummings <kgc*sonic.net>
clamav.gossamer-threads.com	64.69.64.158	Canada	Alex Krohn <mirrors*gossamer-threads.com>
clamav.catt.com	64.18.100.4	USA	Mike Cathey <mirrors*catt.com>
clamav.antispam.or.id	202.134.0.71	Indonesia	Fajar Nugraha <fajar*telkom.co.id>
clamav-du.viaverio.com	199.239.233.95	USA	Scott Wiersdorf <scott*perlcode.org>
clamav-sj.viaverio.com	128.121.60.235	USA	Scott Wiersdorf <scott*perlcode.org>
clamavdb.heanet.ie	193.1.219.100	Ireland	Colm MacCarthaigh <mirrors*heanet.ie>

Mirror	IP	Location	Administrator
clamav.crysys.hu	152.66.249.132	Hungary	Bencsath Boldizsar <boldi*mail2004.crysys.hit.bme.hu>
clamav.rockriver.net	209.94.36.5	Illinois, USA	Thomas D. Harker <tom*rockriver.net>
clamav.xmundo.net	200.68.106.40	Argentina	Cristian Daniel Merz <mirrors*xmundo.net>
clamav.infotex.com	66.139.73.146	Texas, USA	Matthew Jonkman <matt*infotex.com>
clamav.mirror.transip.nl	80.69.67.3	The Netherlands	Walter Hop <walter*transip.nl>
clamavdb.osj.net	218.44.253.75	Japan	Masaki Ikeda <masaki*orange.co.jp>
clamav.ialfa.net	210.22.201.152	People's Republic of China	Alfa Shen <alfa*ialfa.net>
clamavdb.ikk.sztaki.hu	193.225.86.3	Hungary	Gabor Kiss <kissg*debella.ikk.sztaki.hu>
clamav.mirrors.nks.net	24.73.112.74	Florida, USA	James Neal <clam-admin*nks.net>
clamav.kratern.se	212.31.160.239	Sweden	Emil Ljungdahl <emil*kratern.se>
clamav.dif.dk	193.138.115.108	Denmark	Jesper Juhl <juhl*dif.dk>
clamav.dbplc.com	217.154.108.81	United Kingdom	Simon Pither <simon*digitalbrain.com>
clamav.unet.brandeis.edu	129.64.99.170	USA	Rich Graves <rcgraves*brandeis.edu>
clamav.im1.net	65.77.42.207	Florida, US	Dmitri Pavlenkov <dmitri*im1.com>
clamav.elektrotech-ker.hu	80.95.80.7	Hungary	Bodrogi Zsolt <odin*szilank.hu>
clamav.stockingshq.com	212.113.16.74	United Kingdom	<dave*stockingshq.com>
clamav.acnova.com	203.81.40.167	Singapore	Lennard Seah <myself*lennardseah.com>
clamdb.prolocation.net	213.73.255.243	The Netherlands	Raymond Dijkxhoorn <raymond*prolocation.net>
clamav.xyxx.com	65.75.154.69	San Francisco/Palo Alto California, USA	Myron Davis <myrond*xyxx.com>
clamav.walkertek.com	38.136.139.7	USA	Stephen Walker <swalker*walkertek.com>
clamav.mirror.cygnal.ca	24.244.193.21 24.244.193.22	Burlington, Ontario, Canada	Rafal Rzeczkowski <mirrors*cygnal.ca>
clamav.securityminded.net	209.8.40.140	Ashburn, USA	Thomas Petersen <tomp*securityminded.net>
clamav.island.net.au	203.28.142.36	Sydney Australia	Hugh Blandford <hugh*island.net.au>
clamav.iol.cz	194.228.2.38	Czech Republic	Lenka Sevcikova <lenka.sevcikova*ct.cz>
clamav.securitywonks.net	66.197.159.213	USA	D. Raghu Veer <clamav*zyserver.net>
clamav.pcn.de	213.203.254.4	Hamburg, Germany	Karsten Gessner <karsten*pcn.de>

Mirror	IP	Location	Administrator
clamav.enderunix.org	193.140.143.23	Turkey	Omer Faruk Sen <ofsen*enderunix.org>
clamav.ovh.net	213.186.33.38 213.186.33.37	France	Germain Masse <germain.masse*ovh.net>
clamav.spod.org	195.92.99.99	United Kingdom	Ian Kirk <blob*blob.co.uk>
clamav.intercom.net.ua	195.13.43.28	Ukraine	Artie Missirov <kadjy*intercom.net.ua>
clamav.mirror.vutbr.cz	147.229.3.16	Czech Republic	Tomas Kreuzwieser <mirror-adm*cis.vutbr.cz>
database.clamav.ps.pl	212.14.28.36	Poland	Adam Popik <adam*popik.pl>
clamav.fx-services.com	69.93.108.98	USA	Robin Vley <robin*fx-services.com>
clamav.univ-nantes.fr	193.52.101.131	France	Yann Dupont <yann.dupont*univ-nantes.fr>
clamav.blackroute.net	64.246.44.108	Texas, USA	Maarten Van Horenbeeck <maarten*daemon.be>
clamavdb.mithril-linux.org	211.10.155.48	Japan	Hideki Yamane <henrich*samba.gr.jp>
clamavdb.planetmirror.com	203.16.234.78	Australia	Jason Andrade <support*planetmirror.com>
clamavdb.raimei.co.jp	219.106.255.66	Japan	Araki Musashi <araki*raimei.co.jp>
clamav.pathlink.com	129.250.169.81	USA	Kachun Lee <kachun*pathlink.com>
clamav.mirror.camelnetwork.com	213.230.200.242	UK	Chris Burton <clamav.mirror*camelnetwork.com>
clamav.unnet.nl	62.133.206.90	Netherlands	Cliff Albert <cliff*unilogicnetworks.net>
clamav.easynet.fr	212.180.1.29	France	Jean-Louis Bergamo <mailadmin*easynet.fr>
clamav.edebris.com	216.24.174.245	USA	Edward Kujawski <ed*hp.uab.edu>
clamav.inoc.net	64.246.134.133	USA	Robert Blayzor <noc*inoc.net>
clamav.devolution.com	206.58.251.131	California,	Scott Call <scall*atgi.net>
clamavdb.hostlink.com.hk	210.245.160.22	Hong Kong	Alex Fong <alexfkl*hostlink.com.hk>
clamav.clearfield.com	65.110.48.11	USA	Jean-Francois Pirus <jfp*clearfield.com>
clamav.oltrelinux.com	194.242.226.43	Italy	Luca Gibelli <l.gibelli*oltrelinux.com>
clamav.artcoms.ru	80.244.224.247	Russia	Syrnikov Alexei <san*artcoms.ru>
xarch.clamav.net	129.27.62.129	Austria	Reini Urban <rurban*x-ray.at>
clamav.linux.it	213.92.8.5	Italy	Marco d'Itri <md*linux.it>
clamav.eastweb.ru	213.219.245.4	Russia	Leonid Novikov <lenni*eastweb.ru>

Mirror	IP	Location	Administrator
clamav.coldmoon.net	204.89.193.10	Chicago, USA	Scott J. Lopez <scott*coldmoon.net>
clamav.mirrors.webpartner.dk	195.184.96.15	Denmark	Nicolai Gylling <nsg*webpartner.dk> Lasse Brandt <lb*webpartner.dk>
mirror.etf.bg.ac.yu	147.91.8.58	Belgrade, Serbia and Montenegro	Ljubisa Radivojevic <ljubisa*etf.bg.ac.yu>
clamav.bridgeband.net	63.166.28.8	Montana, USA	Mikel Bauer <mikel*bridgeband.net>
clamav.kgt.org	217.20.122.250	Germany	Thomas Koeppe <thomas*kgt.org>
clamav.mirror.waycom.net	195.214.240.53	France	Frederic Deletang <fd*waycom.net>
clamav.cryms.info	194.29.5.19	Lugano, Switzerland	Lorenzo Patocchi <lorenzo.patocchi*cryms.com>
clamav.mirror.pacific.net.au	61.8.0.16	Australia	Martin Foster <mirror-team*pacific.net.au>
clamavdb.mirrors.net.ru	212.16.26.185	Russia	Andrew V. Kovalev <mirrors*mirrors.net.ru>
clamav.cbn.net.id	202.158.56.242	Indonesia	Riv Octovahriz <riv*cbn.net.id>
clamav.forthnet.gr	193.92.150.194	Greece	Nick Katsamas <virus_admin*forthnet.gr>
fuxhausen.tiscali.de	62.26.160.3	Germany	Elke Hahnen <elke.hahnen*de.tiscali.com>
clamav.theshell.com	209.200.146.2	USA	Peter Avalos <pavalos*theshell.com>
clamav.inode.at	81.223.20.171	Austria	Michael Renner <mirror*inode.at>
clamav.informatik.fh-furtwangen.de	141.28.73.8	Germany	Sebastian Siewior <bigeasy*foo.fh-furtwangen.de>
clamav.cpss.edu.hk	218.189.210.14	Hong Kong	Wan Pui Wa <puiwa*cpss.edu.hk>
clamav.irontec.com clamav.optical.com.mx	66.111.55.10 200.53.122.8	Tampa, USA Mexico	Iker Sagasti Markina <iker*irontec.com> Omar Armas <oarmas*mpsnet.net.mx>
idea.sec.dico.unimi.it	159.149.155.69	Italy	Lorenzo Martignoni <lorenzo*cert-it.dico.unimi.it>
clamav.cs.pu.edu.tw	140.128.9.18	Taiwan	Hsun-Chang Chang <hcchang*cs.pu.edu.tw>
clamav.skynet.cz	193.165.254.12	Czech Republic	Jaroslav Jurasek <jaroslav.jurasek*skynet.cz>

9.2 Contributors

The following people contributed to our project in some way (providing patches, bug reports, technical support, documentation, good ideas...):

- Sergey Y. Afonin <asy*kraft-s.ru>
- Robert Allerstorfer <roal*anet.at>
- Claudio Alonso <cfalonso*yahoo.com>
- Kamil Andrusz <wizz*mniam.net>
- Jean-Edouard Babin <Jeb*jeb.com.fr>
- Marc Baudoin <babafou*babafou.eu.org>
- Scott Beck <sbeck*gossamer-threads.com>
- Rolf Eike Beer <eike*mail.math.uni-mannheim.de>
- Rene Bellora <rbellora*tecnoaccion.com.ar>
- Carlo Marcelo Arenas Belon <carenas*sajinet.com.pe>
- Hilko Bengen <bengen*vdst-ka.inka.de>
- Patrick Bihan-Faou <patrick*mindstep.com>
- Martin Blapp <mb*imp.ch>
- Dale Blount <dale*velocity.net>
- Oliver Brandmueller <ob*e-Gitt.NET>
- Boguslaw Brandys <brandys*o2.pl>
- Igor Brezac <igor*ipass.net>
- Mike Brudenell <pmb1*york.ac.uk>
- Brian Bruns <bruns*2mbit.com>
- Len Budney <lbudney*pobox.com>
- Matt Butt <mattb*cre8tiv.com>
- Christopher X. Candreva <chris*westnet.com>

- Eric I. Lopez Carreon <elopezc*technitrade.com>
- Ales Casar <casar*uni-mb.si>
- Andrey Cherezov <andrey*cherezov.koenig.su>
- Alex Cherney <alex*cher.id.au>
- Tom G. Christensen <tgc*statsbiblioteket.dk>
- Nicholas Chua <nicholas*ncmbox.net>
- Chris Conn <cconn*abacom.com>
- Christoph Cordes <ib*precompiled.de>
- Ole Craig <olc*cs.umass.edu>
- Eugene Crosser <crosser*rol.ru>
- Damien Curtain <damien*pagefault.org>
- Krisztian Czako <slapic*linux.co.hu>
- Diego d'Ambra <da*softcom.dk>
- Michael Dankov <misha*btrc.ru>
- Yuri Dario <mc6530*mclink.it>
- David <djgardner*users.sourceforge.net>
- Maxim Dounin <mdounin*rambler-co.ru>
- Alejandro Dubrovsky <s328940*student.uq.edu.au>
- Magnus Ekdahl <magnus*debian.org>
- Mehmet Ekiz <ekizm*tbmm.gov.tr>
- Jens Elkner <elkner*linofee.org>
- Fred van Engen <fred*wooha.org>
- Jason Englander <jason*englanders.cc>
- Oden Eriksson <oeriksson*mandrakesoft.com>
- Andy Fiddaman <af*jeamland.org>

- Edison Figueira Junior <edison*brc.com.br>
- David Ford <david+cert*blue-labs.org>
- Brian J. France <list*firehawksystems.com>
- Free Oscar <freeoscar*wp.pl>
- Martin Fuxa <yeti*email.cz>
- Piotr Gackiewicz <gacek*intertele.pl>
- Jeremy Garcia <jeremy*linuxquestions.org>
- Dean Gaudet <dean-clamav*arctic.org>
- Michel Gaudet <Michel.Gaudet*ehess.fr>
- Philippe Gay <ph.gay*free.fr>
- Nick Gazaloff <nick*sbin.org>
- Luca ’NERvOus’ Gibelli <nervous*nervous.it>
- Scott Gifford <sgifford*suspectclass.com>
- Wieslaw Glod <wkg*x2.pl>
- Stephen Gran <steve*lobefin.net>
- Matthew A. Grant <grantma*anathoth.gen.nz>
- Christophe Grenier <grenier*cgsecurity.org>
- Marek Gutkowski <hobbit*core.segfault.pl>
- Jason Haar <Jason.Haar*trimble.co.nz>
- Hrvoje Habjanic <hrvoje.habjanic*zg.hinet.hr>
- Michal Hajduczenia <michalis*mat.uni.torun.pl>
- Jean-Christophe Heger <jcheger*acytec.com>
- Anders Herbjornsen <andersh*gar.no>
- Paul Hoadley <paulh*logixsquad.net>
- Robert Hogan <robert*roberthogan.net>

- Przemyslaw Holowczyc <doozer*skc.com.pl>
- Thomas W. Holt Jr. <twh*cohesive.net>
- James F. Hranicky <jfh*cise.ufl.edu>
- Douglas J Hunley <doug*hunley.homeip.net>
- Kurt Huwig <kurt*iku-netz.de>
- Andy Igoshin <ai*vsu.ru>
- Jay <sysop-clamav*coronastreet.net>
- Stephane Jeannenot <stephane.jeannenot*wanadoo.fr>
- Dave Jones <dave*kalkbay.co.za>
- Jesper Juhl <juhl*dif.dk>
- Alex Kah <alex*narfonix.com>
- Stefan Kaltenbrunner <stefan*kaltenbrunner.cc>
- Lloyd Kamara <l.kamara*imperial.ac.uk>
- Kazuhiko <kazuhiko*fdiary.net>
- Tomasz Klim <tomek*euroneto.pl>
- Robbert Kouprie <robbert*exx.nl>
- Martin Kraft <martin.kraft*fal.de>
- Petr Kristof <Kristof.P*fce.vutbr.cz>
- Henk Kuipers <henk*opensourcesolutions.nl>
- Nigel Kukard <nkukard*lbsd.net>
- Dr Andrzej Kurpiel <akurpiel*mat.uni.torun.pl>
- Mark Kushinsky <mark*mdspc.com>
- Mike Lambert <lambert*jeol.com>
- Thomas Lamy <Thomas.Lamy*in-online.net>
- Marty Lee <marty*maui.co.uk>

- Dennis Leeuw <dleeuw*made-it.com>
- Martin Lesser <admin-debian*bettercom.de>
- Peter N Lewis <peter*stairways.com.au>
- Matt Leyda <mfleyda*e-one.com>
- James Lick <jlick*drivel.com>
- Mike Loewen <mloewen*sturgeon.cac.psu.edu>
- Roger Lucas <roger*planbit.co.uk>
- Richard Lyons <frob-clamav*webcentral.com.au>
- David S. Madole <david*madole.net>
- Thomas Madsen <tm*softcom.dk>
- Bill Maidment <bill*maidment.com.au>
- Joe Maimon <jmaimon*ttec.com>
- Andrey V. Malyshev <amal*krasn.ru>
- Stefan Martig <sm*officeco.ch>
- Alexander Marx <mad-ml*madness.at>
- Andreas Marx (http://www.av-test.org/)
- Chris Masters <cmasters*insl.co.uk>
- Fletcher Mattox <fletcher*cs.utexas.edu>
- Serhiy V. Matveyev <matveyev*uatele.com>
- Reinhard Max <max*suse.de>
- Brian May <bam*debian.org>
- Ken McKittrick <klmac*usadatanet.com>
- Chris van Meerendonk <cvm*castel.nl>
- Andrey J. Melnikoff <temnota*kmv.ru>
- Damian Menscher <menscher*uiuc.edu>

- Arkadiusz Miskiewicz <misiek*pld-linux.org>
- Mark Mielke <mark*mark.mielke.cc>
- Jo Mills <Jonathan.Mills*frequentis.com>
- Dustin Mollo <dustin.mollo*sonoma.edu>
- Remi Mommsen <remigius.mommsen*cern.ch>
- Doug Monroe <doug*planetconnect.com>
- Alex S Moore <asmoore*edge.net>
- Dirk Mueller <mueller*kde.org>
- Flinn Mueller<flinn*activeintra.net>
- Hendrik Muhs <Hendrik.Muhs*student.uni-magdeburg.de>
- Simon Munton <simon*munton.demon.co.uk>
- Farit Nabiullin http://program.farit.ru/
- Nemosoft Unv. <nemosoft*smcc.demon.nl>
- Wojciech Noworyta <wnow*konarski.edu.pl>
- Jorgen Norgaard <jnp*anneli.dk>
- Fajar A. Nugraha <fajar*telkom.co.id>
- Joe Oaks <joe.oaks*hp.com>
- Washington Odhiambo <wash*wananchi.com>
- Masaki Ogawa <proc*mac.com>
- Phil Oleson <oz*nixil.net>
- Jan Ondrej <ondrejj*salstar.sk>
- Martijn van Oosterhout <kleptog*svana.org>
- OpenAntiVirus Team (http://www.OpenAntiVirus.org/)
- Tomasz Papszun <tomek*lodz.tpsa.pl>
- Eric Parsonage <eric*eparsonage.com>

- Oliver Paukstadt <pstadt*stud.fh-heilbronn.de>
- Christian Pelissier <Christian.Pelissier*onera.fr>
- Rudolph Pereira <r.pereira*isu.usyd.edu.au>
- Ed Phillips <ed*UDel.Edu>
- Andreas Piesk <Andreas.Piesk*heise.de>
- Alex Pleiner <pleiner*zeitform.de>
- Ant La Porte <ant*dvere.net>
- Christophe Poujol <Christophe.Poujol*atosorigin.com>
- Sergei Pronin <sp*finndesign.fi>
- Thomas Quinot <thomas*cuivre.fr.eu.org>
- Ed Ravin <eravin*panix.com>
- Brian A. Reiter <breiter*wolfereiter.com>
- Rupert Roesler-Schmidt <r.roesler-schmidt*uplink.at>
- David Sanchez <dsanchez*veloxia.com>
- David Santinoli <david*santinoli.com>
- Vijay Sarvepalli <vssarvep*office.uncg.edu>
- Martin Schitter
- Theo Schlossnagle <jesus*omniti.com>
- Enrico Scholz <enrico.scholz*informatik.tu-chemnitz.de>
- Karina Schwarz <k.schwarz*uplink.at>
- Scsi <scsi*softland.ru>
- Dr Matthew J Seaman <m.seaman*infracaninophile.co.uk>
- Hector M. Rulot Segovia <Hector.Rulot*uv.es>
- Omer Faruk Sen <ofsen*enderunix.org>
- Sergey <a_s_y*sama.ru>

- Tuomas Silen <tuomas.silen*nodeta.fi>
- Al Smith <ajs+clamav*aeschi.ch.eu.org>
- Kevin Spicer <kevin*kevinspicer.co.uk>
- Ole Stanstrup <ole*stanstrup.dk>
- Adam Stein <adam*scan.mc.xerox.com>
- Steve <steveb*webtribe.net>
- Richard Stevenson <richard*endace.com>
- Matt Sullivan <matt*sullivan.gen.nz>
- Dr Zbigniew Szewczak <zssz*mat.uni.torun.pl>
- Joe Talbott <josepht*cstone.net>
- Gernot Tenchio <g.tenchio*telco-tech.de>
- Masahiro Teramoto <markun*onohara.to>
- Ryan Thompson <clamav*sasknow.com>
- Yar Tikhiy <yar*comp.chem.msu.su>
- Michael L. Torrie <torriem*chem.byu.edu>
- Trashware <trashware*gmx.net>
- Matthew Trent <mtrent*localaccess.com>
- Reini Urban <rurban*x-ray.at>
- Daniel Mario Vega <dv5a*dc.uba.ar>
- Laurent Wacrenier <lwa*teaser.fr>
- Charlie Watts <cewatts*brainstorminternet.net>
- Nicklaus Wicker <n.wicker*cnk-networks.de>
- David Woakes <david*mitredata.co.uk>
- Troy Wollenslegel <troy*intranet.org>
- Dale Woolridge <dwoolridge*drh.net>

- David Wu <dyw*iohk.com>
- Takumi Yamane <yamtak*b-session.com>
- Youza Youzovic <youza*post.cz>
- Leonid Zeitlin <lz*europe.com>
- ZMan Z. <x86zman*go-a-way.dyndns.org>
- Andoni Zubimendi <andoni*lpsat.net>

9.3 Donors

We've received financial support from: (in alphabetical order)

- ActiveIntra.net Inc. (http://www.activeintra.net/)
- Advance Healthcare Group (http://www.ahgl.com.au/)
- American Computer & Electronic Services Corp. (http://www.acesnw.com/)
- Anonymous donor from Colorado, US
- Atlas College (http://www.atlascollege.nl/)
- AWD Online (http://www.awdonline.com/)
- Bear and Bear Consulting, Inc. (http://www.bear-consulting.com/)
- Aaron Begley
- Craig H. Block
- Norman E. Brake, Jr.
- cedarcreeksoftware.com (http://www.cedarcreeksoftware.com/)
- Thanos Chatziathanassiou
- Cheahch from Singapore
- Conexim Australia - business web hosting (http://www.conexim.com.au)
- Joe Cooper
- Steve Donegan (http://www.donegan.org/)

- Dynamic Network Services, Inc (http://www.dyndns.org/)
- Electric Embers (http://electricembers.net)
- Epublica
- Bernhard Erdmann
- David Eriksson (http://www.2good.nu/)
- Philip Ershler
- Explido Software USA Inc. (http://www.explido.us/)
- David Farrick
- Jim Feldman
- Petr Ferschmann (http://petr.ferschmann.cz/)
- Andries Filmer (http://www.netexpo.nl/)
- The Free Shopping Cart people (http://www.precisionweb.net/)
- Paul Freeman
- Jack Fung
- Paolo Galeazzi
- GANDI (http://www.gandi.net/)
- Jeremy Garcia (http://www.linuxquestions.org/)
- GBC Internet Service Center GmbH (http://www.gbc.net/)
- GCS Tech (http://www.gcstech.net/)
- GHRS (http://www.ghrshotels.com/)
- Todd Goodman
- Bill Gradwohl (http://www.ycc.com/)
- Grain-of-Salt Consulting
- Terje Gravvold
- Hart Computer (http://www.hart.co.jp/)

- Hosting Metro LLC (http://www.hostingmetro.com/)
- IDEAL Software GmbH (http://www.IdealSoftware.com/)
- Industry Standard Computers (http://www.ISCnetwork.com/)
- Invisik Corporation (http://www.invisik.com/)
- Craig Jackson
- Stuart Jones
- Jason Judge
- Keith (http://www.textpad.com/)
- Brad Koehn
- Logic Partners Inc. (http://www.logicpartners.com/)
- Mark Lotspaih (http://www.lotcom.org/)
- Michel Machado (http://oss.digirati.com.br/)
- Olivier Marechal
- Midcoast Internet Solutions
- Mimecast (http://www.mimecast.com/)
- Kazuhiro Miyaji
- Bozidar Mladenovic
- Paul Morgan
- Tomas Morkus
- Michael Nolan (http://www.michaelnolan.co.uk/)
- Oneworkspace.com (http://www.oneworkspace.com/)
- Origin Solutions (http://www.originsolutions.com.au/)
- outermedia GmbH (http://www.outermedia.de/)
- Alexander Panzhin
- Dan Pelleg

- Thodoris Pitikaris
- Paul Rantin
- Luke Reeves (http://www.neuro-tech.net/)
- RHX (http://www.rhx.it/)
- Stefano Rizzetto
- Roaring Penguin Software Inc. (http://www.roaringpenguin.com/)
- Luke Rosenthal
- School of Engineering, University of Pennsylvania (http://www.seas.upenn.edu/)
- Tim Scoff
- Seattle Server (http://www.seattleserver.com/)
- Software Workshop Inc (http://www.softwareworkshop.com/)
- Solutions In A Box (http://www.siab.com.au/)
- Stephane Rault
- Fernando Augusto Medeiros Silva (http://www.linuxplace.com.br/)
- StarBand (http://www.starband.com/)
- Synchro Sistemas de Informacao (http://synchro.com.br/)
- Sahil Tandon
- Brad Tarver
- Per Reedtz Thomsen
- William Tisdale
- Up Time Technology (http://www.uptimetech.com/)
- Ulfi
- Jeremy Vanderburg (http://www.jeremytech.com/)
- Webzone Srl (http://www.webzone.it/)

- Markus Welsch (http://www.linux-corner.net/)
- Nicklaus Wicker
- David Williams (http://kayakero.net/)

9.4 Graphics

The authors of the nice ClamAV logo (look at the title page) and other graphics are Mia Kalenius and Sergei Pronin <sp*finndesign.fi> from Finndesign http://www.finndesign.fi/

9.5 OpenAntiVirus

Our database includes the virus database (about 7000 signatures) from http://OpenAntiVirus.org

10 Authors

- aCaB <acab*clamav.net>, Italy
  Role: virus database maintainer, coder
- Mike Cathey <mike*clamav.net>, USA
  Role: co-sysadmin
- Christoph Cordes <ccordes*clamav.net>, Germany
  Role: virus database maintainer
- Diego d'Ambra <diego*clamav.net>, Denmark
  Role: virus database maintainer
- Jason Englander <jason*clamav.net>, USA
  Role: inactive
- Luca Gibelli <luca*clamav.net>, Italy
  Role: sysadmin, mirror coordinator
- Nigel Horne <njh*clamav.net>, United Kingdom
  Role: coder
- Tomasz Kojm <tkojm*clamav.net>, Poland
  Role: project leader, coder, virus database maintainer

- Thomas Lamy <tlamy*clamav.net>, Germany
  Role: random hacker
- Thomas Madsen <tmadsen*clamav.net>, Denmark
  Role: virus submission management
- Denis De Messemacker <ddm*clamav.net>, Belgium
  Role: virus database maintainer
- Tomasz Papszun <tomek*clamav.net>, Poland
  Role: virus database maintainer
- Trog <trog*clamav.net>, United Kingdom
  Role: coder, virus database maintainer