Readme for clamtk

This README was last checked or updated on 20240116.

Table of contents:

About

clamtk is a frontend for ClamAV (Clam Antivirus). It is intended to be an easy to use, light-weight, on-demand scanner for Linux systems.

Although its earliest incarnations date to 2003, clamtk was first uploaded for distribution in 2004 to a rootshell.be account and finally to Sourceforge.net in 2005. At the end of 2013, it was moved to a Google Code page, then to Github, Gitlab, and Bitbucket. It is now 2024 and for some reason development is still going. In fact, February 2024 marks 20 years of activity (of being publicly available, that is).

Contributing

1. Report bugs or suggestions at the following:

   https://github.com/dave-theunsub/clamtk/issues
   https://gitlab.com/dave_m/clamtk/issues
   https://launchpad.net/clamtk

2. Do you speak more than one language? See the Launchpad page.

3. If you feel like it, "star" clamtk or its related projects at one or both of the following:

   https://github.com/dave-theunsub/clamtk/
   https://gitlab.com/dave_m/clamtk/

Important Links

Official clamtk links

https://github.com/dave-theunsub/clamtk/
https://gitlab.com/dave_m/clamtk/wikis/home
https://gitlab.com/dave_m/clamtk/
https://launchpad.net/clamtk

Related links

Installation

RPMs

The easiest way to install clamtk is to use the rpms. The commands dnf and yum will pull in requirements.

First, start with the official repositories.

sudo yum install clamtk or sudo dnf install clamtk.

If this does not work, download the file from [the official site](#). You should be able to just double click the file for installation or upgrade.

For these examples, we will use version 6.17. The name of the file may differ based on your distribution.

To install using a terminal window:

sudo yum install clamtk-6.17-1.el9.noarch.rpm or sudo dnf install clamtk-6.17-1.fc39.noarch.rpm

To remove clamtk:

sudo yum erase clamtk or sudo dnf erase clamtk.

Source

Warning: Don't do this. It's much easier to just double click a .deb or .rpm. Really, put down the source.

The tarball contains all the sources. One way to do this, as tested on Fedora, is to run the following commands:

```
tar xzf clamtk-6.17.tar.xz
sudo mkdir -p /usr/share/perl5/vendor_perl/ClamTk
sudo cp lib/*.pm /usr/share/perl5/vendor_perl/ClamTk
sudo chmod +x clamtk
sudo cp clamtk /usr/local/bin (or /usr/bin)
```

Examples:

perl clamtk

or

```
chmod +x /path/to/clamtk
/path/to/clamtk
```

- If you have installed this program as an rpm or .deb, you do not need to take these steps.
- Did you get errors with this? Check the TROUBLESHOOTING section at the end.

DEBs

You should be able to just double click the .deb file to install it. Your package manager should retrieve any necessary dependencies.

From the commandline, you can do this:

```
sudo apt install clamtk
```

If you downloaded the file, then use this:

```
sudo apt install clamtk_6.17-1_all.deb
```

To remove clamtk:

```
sudo dpkg --purge clamtk
```

Note that the Debian/Ubuntu builds are no longer gpg-signed.

Integrity

It is recommended you install clamtk from official repositories. Check your distribution first, and always install from trusted sources.

While the Debian/Ubuntu .debs used to be digitally signed, they are not anymore; the way I used to do that no longer works. The rpms are digitally signed. Here's how you can verify the rpms:

1. Get and import the key in one step:
   ```
   rpm --import https://davem.fedorapeople.org/RPM-GPG-KEY-DaveM-20230506
   ```
2. Verify the list of gpg keys installed in RPM DB:
   ```
   rpm -q gpg-pubkey --qf '%{name}-%{version}-%{release} --> %{summary}\n'
   ```
3. Check the signature of the rpm. For this example, we'll use version 6.17:
   ```
   rpm --checksig clamtk-6.17-1.fc39.noarch.rpm
   ```
4. You should see something like this:
   ```
   /home/you/clamtk-6.17-1.fc39.noarch.rpm: rsa sha1 (md5) pgp md5 OK
   ```

You can also verify the tarball. Using 6.17 as the example version, ensure you have downloaded the tarball, its detached signature (.asc), and the key in step 1 above.

1. Get the key (skip this step if you already have it):
   ```
   wget https://davem.fedorapeople.org/RPM-GPG-KEY-DaveM-20230506
   ```
2. Import it (skip this step if you have done it already):
   ```
   gpg --import RPM-GPG-KEY-DaveM-20230506
   ```

3. Verify like so:

`gpg2 --verify clamtk-6.17.tar.xz.asc clamtk-6.17.tar.gz` or

`gpg --verify clamtk-6.17.tar.xz.asc clamtk-6.17.tar.xz`

4. You should see something like this:

`gpg: Signature made Sun 11 Sep 2016 06:29:41 AM CDT using RSA key ID` (snipped for brevity).

You can now use minisign, too!
[Minisign](#)

First, you will need my public minisign key:
[Public minisign key](#)

Then you will need the minisig file for the program you are verifying.

A link to it will be with the rest of the downloads.

For this example:

https://github.com/dave-theunsub/clamtk/releases/download/v6.17/clamtk-6.17.tar.xz.minisig

Next, verify like so:

```
minisign -V -x clamtk-6.17.tar.xz.minisig -p davemminisign.pub -m clamtk-
6.17.tar.xz
```

Usage

Running clamtk

- Any recent version of clamtk will automatically search for signatures if you do not have them set already. This way it should work right out of the box.
- Consider the extra scanning options in Settings.
- Select "Scan files beginning with a dot (.*)" to scan those files beginning with a ".". These are sometimes referred to as "hidden" files.
- Select "Scan directories recursively" to scan all files and directories within a directory.
- The "Scan for PUAs" option enables the ability to scan for Potentially Unwanted Applications as well as broken executables. Note that this can result in what may be false positives.
- By default, clamtk will avoid scanning files larger than 20MB. To force scanning of these files, check the "Scan files larger than 20 MB" box.
- You can also check for updates upon startup. This requires an active Internet connection.
- Information on items quarantined is available under the "Quarantine" option. If you believe there is a false positive contained, you can easily move it back to your home directory. You may also delete this file(s). *There is no recycle bin - once deleted, the files are gone forever.*
- Scan a file or directory by right-clicking on it within the file manager (e.g., Nautilus). This functionality requires an extra package (clamtk-gnome).
- You can STOP the scan by clicking the Cancel button. Due to the speed of the scanning, however, it may not stop immediately; it will continue scanning and displaying files it has already "read" until the stop catches up.

- View previous scans by selecting "History".
- The Update Assistant is necessary because some systems are set up to do automatic updates, while others must manually update them.
- If you require specific proxy settings, select "Network".
- As of version 5.xx, you can use the "Analysis" button to see if a particular file is considered malicious by other antivirus products. This uses results from Virustotal. If you desire, you can submit a file for further review. Please do *not* submit files with personal, financial, or security information.
- The "Whitelist" option provides the ability to skip specific directories during scan time. For example, you may wish to skip directories containing music or videos.

Commandline

clamtk can run from the commandline, too:

```
clamtk file_to_be_scanned
```

or

```
clamtk directory_to_be_scanned
```

The main reason for the commandline option (however basic) is to allow for right-click scanning within your file manager (e.g., Files, Caja, or Dolphin). If you require more extensive commandline options, it is recommended that you use the clamscan executable itself. (Type `man clamscan` at the commandline.)

Afterwards

You can view and delete scan logs by selecting the "History" option.

You also have a few options with the files displayed. Click on the file scanned to select it, then right-click: you should have four options there.

- Quarantine this file: This drops the selected file into a "quarantined" folder with the executable bit removed. The quarantine folder is held in the user's clamtk folder (`~/.clamtk/viruses`).
- Delete this file: Be careful: There is no recycle bin!
- Cancel: Cancels this menu.

Quarantine/Maintenance

If you've quarantined files for later examination, you have the option to restore them to their previous location (if known), or delete them.

Plugins

To add a right-click, context menu ability to send files and directories to the scanner, install the appropriate plugin. Links to the latest versions are available here:

https://github.com/dave-theunsub/clamtk/

https://gitlab.com/dave_m/clamtk/wikis/Downloads

Here are the specific pages. Note that these are mirrored on Github as well.

Gnome (Files file manager):

https://github.com/dave-theunsub/clamtk-gnome

https://gitlab.com/dave_m/clamtk-gnome

KDE (Dolphin file manager):

https://github.com/dave-theunsub/clamtk-kde

https://gitlab.com/dave_m/clamtk-kde

XFCE (Thunar file manager):

https://github.com/dave-theunsub/thunar-sendto-clamtk

https://gitlab.com/dave_m/thunar-sendto-clamtk

Mate (Nemo file manager):

https://github.com/dave-theunsub/nemo-sendto-clamtk

https://gitlab.com/dave_m/nemo-sendto-clamtk

Troubleshooting

- Are your signatures up to date, but clamtk says they're not?

  You probably have more than one virus signature directory. See below answer for finding signatures.

- If you are getting an error that clamtk cannot find your signatures:

  clamtk is trying to find its virus definitions. Typically these are held under /var/lib/clamav or /var/clamav or somewhere else. If you are sure these files exist, please find their location and send it. Try the following to determine their location:

  1. `find /var -name "daily.cvd" -print`
  2. `find /var -name "daily.cld" -print`

- Are you using the source and you see something like this: Can't locate Foo/Bar.pm in @INC. (etc, etc).

  This means you are missing some of the dependencies. Try to find the dependency through your distribution's repositories, or simply go to CPAN. Always try your distribution's repository first. It is more than likely your distribution already packages these for easy installation. Depending on your distro, you will likely use `yum`, `dnf`, `apt` or some "Update Manager" and the like.

- I can't right click on files/directories to scan anymore!

  That's because we no longer bundle this functionality. Not everyone uses Gnome. There are add-ons for XFCE, KDE, Mate, and Gnome - they're small packages, easy to install, and contain that functionality.

Limitations/Bugs

Probably a lot. Let me know, please. Ranting on some bulletin board somewhere on one of dozens of Linux sites will not fix bugs or improve the program. See the section below for contact info.

Other

As of version 3.10, clamtk will not scan standard mail directories, such as .evolution, .mozilla or .thunderbird. This is due to parsing problems. If a smart way of doing that comes up, it will be added.

Also, please note that version numbers mean absolutely nothing. There is no rhyme or reason to odd or even numbers (i.e., an odd number does not mean "unstable"). A new version means it goes up 1 (or, rather, .01).

GUI

clamtk started out using the Tk libraries (thus its name). In 2005, this was changed to perl-Gtk2 (or Gtk2-perl, whatever). The Tk version is still available on sourceforge.net but has not been updated for some time now and should not be used.

The plan for the 5.xx series was to use Gtk3. Unfortunately, Debian and Ubuntu did not have a recent version of libgtk3-perl, and CentOS did not have perl-Gtk3. So, at the last second, the 5.00 version was rewritten to use Gtk2. Again.

Version 6.xx has been written to use Gtk3, as Gtk2 is deprecated. There's no new design this time, as this was an effort to ensure the Gtk3 version could be included in upcoming distribution releases (such as with Debian).

Version 7.xx will likely have a new design, and may be written in a different language as well.

And there's also a Gtk4 in the works.

Thank you

Many people have contributed their time, energy, opinions, recommendations, and expertise to this software. I cannot thank them enough. Their names are listed in the credits file.

Also a big thank you to:

- Everyone who has contributed in one way or another to clamtk - including language files, bug notifications, and feature requests
- Dag, without whom rpms would likely not exist
- All the gtk2-perl and gtk3-perl folks for their time and effort
- Perlmonks

Contact

- Dave M, dave.nerd @gmail.com 0xC81DF0FAC4AFEB22