James Chad Ballay

**Find out about the anti-virus software on the computer you use.**

Home machine is Ubuntu 18.04 LTS. I had to wipe and reimage it recently after breaking too many things recently playing around with Kubernetes and just various other ill advised playing around. Before then I’ve used ClamAV on occasion.

**What is the manufacturer? How do you know they're trustworthy?**

ClamAV. (<https://www.clamav.net/>) I honestly don’t know but I trusted the wisdom of the crowds as well as the inherent protection that the openness of open sourced software entails. With that being said, I’ve went on a bit of a research quest. It wasn’t a good quest. It’s better than nothing but there are several other’s that are better. Much better. Sophos seems to be the current front runner.

**How does it stay up to date?**

It phones home and pulls down an update of its virus database. Configuration is controlled in the freshclam utility that comes with it.

**How can you tell if it's working properly?**

Look for its daemon running using ps to see if it is running at all. To test if it is working properly that doesn’t rely on the vendor to tell me would probably be along the lines of sending a known virus/worm/trojan at myself and confirm that it is blocked.

**Has it ever reported a virus to you? If so, what happened?**

Yes. Most of the viruses it reported were windows based viruses in email or on usb thumbdrives. In both types of situations it offered the choice of attempting to clean the virus up or block the file/email.

**Do a little research on how anti-virus and malware prevention products work.**

Well that was more info then I needed to know about how precarious things are. It’s an unending arms race where anti-virus and malware companies have to play 100% defense and all it takes is for one lucky worm/virus/trojan to get through for a catastrophe to befall someone. The gist is that these products will attack the problem in two main ways. The first line is that they will usually try to lock down the glaring security holes. Offer to enable a firewall solution or maybe quarantine incoming files and emails. (Windows autoplay and Outlook preview type situations.) The next line of defense is these incoming streams of data are compared against an internal database of signatures. Looking for file size, chksum and various other “fingerprints”. Once these items are identified they will either contain the data by quarantining it or they will use a predefined recipe for cleaning. (Maybe delete sections of the executable.)

I have always been good about backing up critical items to storage as well as separating my actions into admin and regular accounts. Mostly this is due to having to wipe and reimage my machine after pushing too far with modifying it and playing around with settings. Careless running of sudo commands that I copy and paste from random Medium walkthroughs have bitten me often. I try to make it a habit of wiping and reimaging every two months or so. It looks like that has the side effect of mitigating the pain of some ransomware or trojan from getting me.

* Time to automate things more. Halfheartedly, following a parts of these guides but I need to polish my setup more. (<https://dotfiles.github.io/>)
* I’ve got no reason to not use a paid tool for antivirus/malware detection. It’s not that paid is inherently better but it looks like this is the current best one and all it requires is $30. (<https://home.sophos.com/en-us.aspx>)