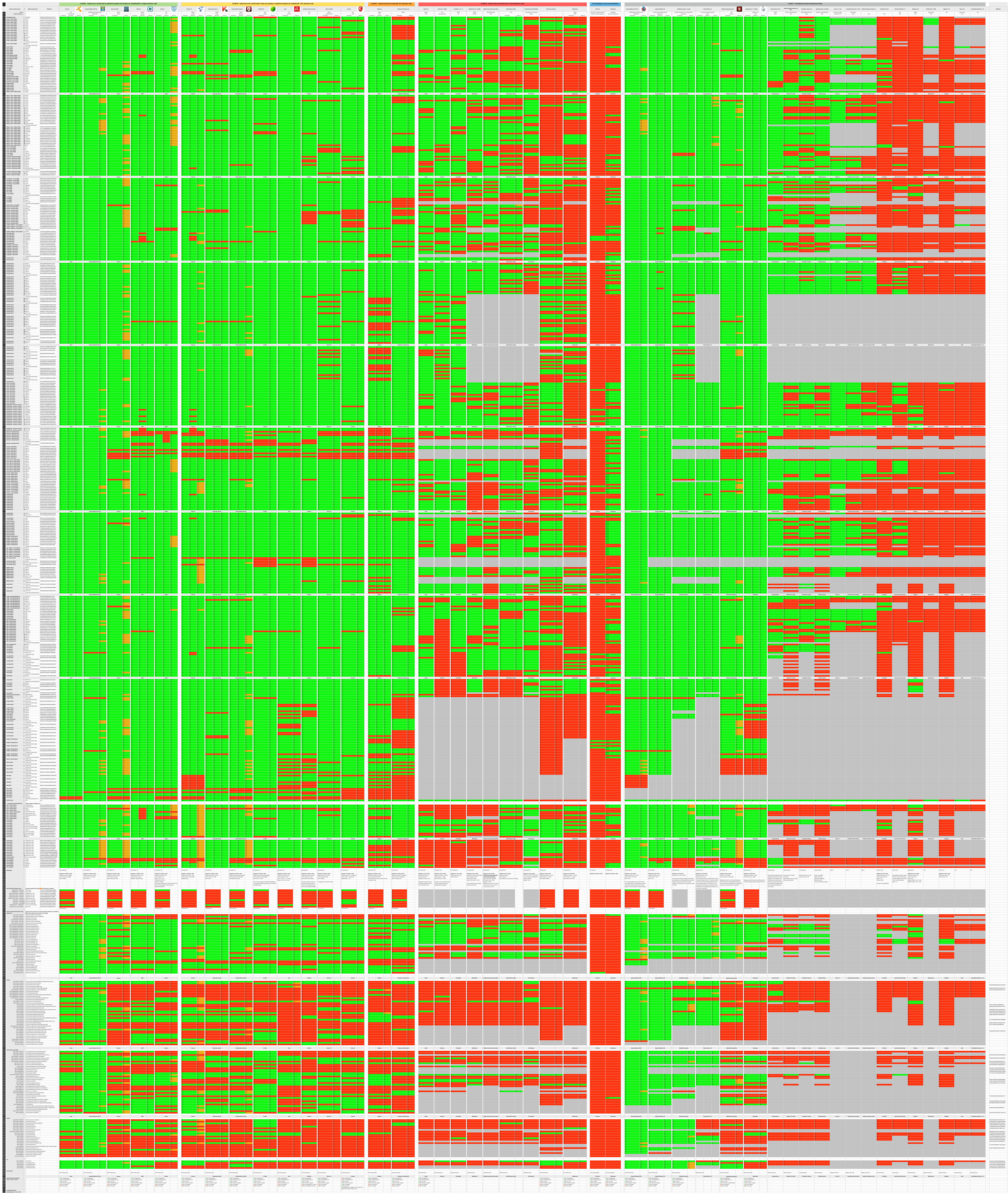

CLASS A - Tested once a month (and as significant updates and samples are available) (95% or higher detection rate)

CLASS B - Tested every two months (and if many new samples or significant updates are available) (95 - 85% detection rate)

CLASS C - Tested every three months (85-75% detection rate)

CLASS D - Tested every six months (75% or lower detection rates)

For Comparison, not an actual Antivirus

CLASS F - Excluded from future testing (read notes)

Notes, comments, remarks, FAQ and everything else.

About the applications excluded from future testing
This list has a mix of applications that are discontinued, do not run properly on major versions of OS X, perform extremely poor and/or have multiple versions. If a company has multiple applications that all perform the same there is no need to list them all. McAfee is a good example of this and since October 2013 so is Panda, their 10.7.x version is now a VirusBarrier clone with the same functions and results.

Discontinued applications that may still be in use by people and perform poorly are also excluded with the strong recommendation to those users to upgrade to a newer version of that product or move on to a different brand. Discontinued applications that may still be in use by people and perform well are still tested and listed.

Some applications in this list have no business calling themselves anti-virus/malware but were tested just to show users how poorly they perform. After these one time tests they are excluded from future testing until the vendor contacts us asking for a re-test or we hear the vendor has significantly improved their product.

Samples marked in grey were acquired after the testing of these applications stopped.

About XProtect
XProtect is a list of blocked files and plug-ins that is maintained by Apple. Even though this is not an antivirus or antimalware application, just a blacklist called on by OS X when a file is opened, I included it to show that in the majority of the cases OS X does not protect you. Even in the few cases where a piece of malware is blocked, it usually takes Apple several weeks to block it, leaving users plenty of time to get infected.

About Gatekeeper
On the default setting of OS X, Gatekeeper will not open applications that are not from the App Store or an Identified Developer. As you can see from the results, this blocks a decent amount of malware. However since Gatekeeper can easily be bypassed I would not count on it as a foolproof way of protection. There has also been malware out there that is signed with a valid developer ID which walks right through Gatekeeper's defenses.

About the trace files
This list is compiled of several things. Online documentation and detection results of each AV product. It is not complete but it shows how efficient a scanner is. Detecting malware samples is fairly easy as they are all in one folder, all the AV scanner has to do is compare the files to their signature database. Thoroughly scanning an operating system and finding malicious files hidden is a whole other story. Infected users will not have a sample set sitting in their downloads folder, they will actually have malicious files hidden in various places. Finding and deleting a malicious app doesn't do you any good if there is a script in your startup items folder that will just re-download and install it next time you start your Mac, for example. So while the detection of samples gives us an indication of how well vendors stay current on the latest threats, the trace detection shows how well the scanner performs. You want a good sample detection rate and a good trace detection rate.

Clean-Up
These results show how well an AV can cure/repair/delete (clean) infected files for you.
Green = Infection cleaned
Orange = Detected, pointed out but unable to clean and/or pointed out but user has to clean manually.
Red = Not detected, not pointed out.

Is there a favorite?
The favorite AV product is the one consistently showing good results and having a similar history. I'm not paid or sponsored by any of these companies/products and do not let the results be influenced by other factors. For example; MacKeeper is a product with a very shady past and to this day I would not recommend it (though a re-test is in order some day). However when it comes to just the malware detection it performs quite well so it is in the list ranked where it deserves to be. Any vendors reading this that feel like sending me some cash are more than welcome to but it will not affect the testing or results in any way :)

Purchasing/installing AV products based on this test
While this test is a good indication how an AV product performs at the time of testing, this can change over night. By adding more samples a product that showed 90% detection can suddenly show way less if the new samples are not detected. Those that have been following this test for a while will see that applications like Sophos and Avast have been first place several times but suddenly found themselves ranking 5th or 6th place as well. If you plan on basing your purchase/install on this test I recommend downloading earlier PDF's to look for trends. Applications that have always performed well are likely to keep doing so. Applications that are all over the place may not. Previous versions of this PDF can be found on the webpage this file was downloaded from: http://securityspread.com/detection-rate-results/

Is this all the malware that exists?
These are all the major malware families but there are many, many more samples out there that I did not include in this test. I didn't feel it necessary to have 30 samples of each malware family as that would be overkill and make this PDF way to big. New samples are added periodically if I find out they are seen in the wild more often and/or are important to the test. In general each family has enough samples in this test for you to see if a product can detect it or not. For example; if a product does not detect most or all of the samples in this test, it's a fair assumption the other 50 samples of that same family will not be detected either.

Always have the most up to date version of this PDF
A widget on the front page of the website shows you exactly when the last update was. If there were significant changes there will be a post on the front page as well. Look for this box:

Malware Detection Rate Results

Last updated:
Sunday October 13h, 2:15PM EST
332 Samples, 37 Applications
Get it here.

Comments or feedback
If there is something unclear about this test or if you have comments or suggestions feel free to reach out using the contact form on the website. I usually respond quickly.