

Forum:[Hack Forums](#)

Thread: [\[BHCPU\] Antivirus Products Test Results](#)

-Hyperion - December 13, 2014, 6:16 pm

Hey guys, it's Hyperion ?

I have 5 years of experience with removing malware, 3 with pentesting (penetration testing) and now work for a fortune 500 company.

Today I will be testing 19 of the most popular Antivirus products for you in order to help you make an informed decision.

There will be 8 free products and 9 paid tested and they will each be rated on performance during idle, interface, protection and removal (1-10 scoring with 10 being the best). Malwarebytes and Herdprotect will be tested as a bonus too.

All versions are tested on a fresh install of Windows 7 Home Premium SP1 64-bits VM (Virtual Machine, under VirtualBox) with most recent updates and only a few tools installed (Process Explorer, Malwarebytes and AdwCleaner). Each Antivirus will be installed, then 5 infected links will be opened in Internet Explorer 11 and 10 different pieces of malware will be tested (worms, trojans, ransomwares and a rootkit). The links and malware are all fresh samples less than 24 hours old from VirusTotal and are in different forms from .exe to Microsoft Office Word documents.

After each test is done the box will be restored completely to its original state (using a snapshot that was taken after a clean installation). I will be using Process Explorer to monitor, and run a Malwarebytes/AdwCleaner scan after each test to see if any residual files are found and what PUPs the AVs may have installed.

[img]http://myphotos.mypclinuxos.com/images/Abraxas012X/avastl.png[/img]

avast! Free

Infected Links : 10/10

Infected Files : 10/10

Interface : 6/10

System Impact : 10/10

.4% cpu 9MB ram

Has a potentially annoying voice(can be turned off) and complex interface also it tries to install a Google toolbar and Chrome during installation.

[img]http://im.tech2.in.com/gallery/2011/sep/avg_finaltext242_141838496597_640x360.jpg[/img]

AVG Free

Infected Links : 10/10

Infected Files : 10/10

Interface : 7/10

System Impact : 10/10

.3% CPU, 2MB RAM

Dood user friendly interface, includes rootkit protection but it did ask to install the AVG toolbar twice after it was installed. Did not stop file immediately on download, took up to 10 seconds to scan and stop a file which long enough for me to potentially execute one.

[img]http://mydownload.me/software/programs/security/Anti_virus/Avira/logo/Avira_antivirus_computer_icon.png[/img]

Avira Free

Infected Links : 5/10

Infected Files : 7/10

Interface : 8/10

System Impact : 7/10

10% CPU, 14MB RAM

Tried to offer free addons and it did include Dropbox with the install. One of the few free include a firewall.

[img]<http://www.techandsoft.com/wp-content/uploads/2012/07/Panda-Cloud-Protection.jpg>[/img]

Panda Cloud Antivirus

Infected Links : 9/10

Infected Files : 10/10

Interface : 7/10

System Impact : 8/10

.7% CPU, 25MB RAM

Tried to install Yahoo toolbar and Mypage as default homepage to many "ads" on interface on the interface.

COMODO Internet Security

Infected Links : 7/10

Infected Files : 4/10

Interface : 4/10

System Impact : 7/10

.9% CPU, 10MB RAM

Full Suite! Asks on detection if you want a geekbuddy to remove it or clean it yourself. Let me actually open 6 of them before giving a warning. Changes DNS to theirs and home page to Yahoo, installed geek buddy and comodo dragon browser. Every time you open the interface it pops up with "call technician".

[img]<http://securitysamurais.com/wp-content/uploads/2013/09/kaspersky-coupon-codes.jpg>[/img]

Kaspersky Internet Security

Infected Links : 10/10

Infected Files : 10/10

Interface : 10/10

System Impact : 6/10

.1% CPU, 85MB RAM

Awesome AV suite and one of my favorites if you have a good computer to run it.

[img]http://www.eset.co.ke/resources/graphics/eset_logo_dark.gif[/img]

ESET Nod32

Infected Links : 10/10

Infected Files : 10/10

Interface : 9/10

System Impact : 7/10

.1% CPU, 54MB RAM

Excellent AV and I would use it if I did not have a chub for Kaspersky. Cannot go wrong with either.

[img]<http://siliconangle.com/files/2011/09/Norton-Logo.jpg>[/img]

Norton 360

Infected Links : 5/10

Infected Files : 13/10 (deleted parts of itself)

Interface : 3/10

System Impact : 2/10

13% CPU, 122MB RAM

Wtf these resources during idle. The damn map that shows real world protection they are fighting live still works offline and worse of all part of itself got infected and it tried to delete itself. McAfee is in the same boat so stay away from these two.

F-Secure Internet Security

Infected Links : 10/10

Infected Files : 10/10

Interface : 10/10

System Impact : 8/10

.1% CPU, 35MB RAM

Very light weight AV that did extremely well would highly recommend to someone who wants a paid AV.

Emsisoft Internet Security

Infected Links : 10/10

Infected Files : 10/10

Interface : 9/10

System Impact : 7/10

.3% CPU, 65MB RAM

Another great AV that uses 2 different engines to scan your system. One of the most friendly and easy to use I have ever seen.

Microsoft Security Essentials (now Windows Defender under Windows 8/8.1)

Infected Links : N/A

Infected Files : 3/10

Interface : 9/10

System Impact : 10/10

.1% CPU, 7MB RAM

Piece of shit from Microsoft that cannot keep up with latest threats and has a backdoor bigger than Blackshades. I would highly recommend using anything over this.

Malwarebytes AntiMalware Security

Infected Links : N/A

Infected Files : 7/10

Interface : 10/10

System Impact : 9/10

.2% CPU, 25MB RAM

Found the 3 files it missed after they were run with a full scan. Surprising done well for not being an AV. With more and more Malware being trojans etc this could be a viable choice in another year. Still a must have for checking for infections.

[img]<http://s52.radikal.ru/i137/1403/22/78287617268f.jpg>[/img]

Qihoo 360 Internet Security

Infected Links : 10/10

Infected Files : 10/10

Interface : 10/10

System Impact : 8/10

.1% CPU, 60MB RAM

Holy balls batman this shit is crazy fast. One of the fastest I have ever seen. Qihoo internet security was tested as well and the main difference is it used 10 mb less ram but has 2 less AV engines it scans with. This is hands down my new favorite free AV! It is also very easy to use file exception. perfect for you blackhats ?

[img]http://cdn.techpp.com/wp-content/uploads/2010/10/bitdefender_logo.png[/img]

Bitdefender Total Security

Infected Links : 10/10

Infected Files : 10/10

Interface : 8/10

System Impact : 6/10

.3% CPU, 111MB RAM

Little heavier then even Kaspersky still not as bad as Norton. Very good engine that other AV's use. It does include tune up and file encryption.

[img]<http://www.comvio.eu/sites/default/files/LogoSophos.jpg>[/img]

Sophos On Premise

Infected Links : 10/10

Infected Files : 10/10

Interface : 9/10

System Impact : 2/10

2% CPU, 678MB RAM

Ho lee shiiiiit if not for the huge ram usage do to multiple features this would be a Kaspersky killer. Nice clean, crisp, interface and one of the few to detect my samples even as a zip file which means it is proactively scanning.

This is definitely a must have if you a sysadmin with lots of users (they more enterprise geared) I would use this if I had 16GB or more of RAM.

Trend Micro Maximum Security

Infected Links : 9/10

Infected Files : 10/10

Interface : 6/10

System Impact : 8/10

.4% CPU, 38MB RAM

Excellent for enterprise and while they score highest on AV comparatives their end user interface is slow and the scan engine took 3 minutes to find all threats after unpacked. Long enough for me to potentially execute a file that could disable it.

Ahnlab v3 Internet Security

Infected Links : 4/10

Infected Files : 7/10

Interface : 4/10

System Impact : 10/10

.5% CPU, 5MB RAM

Lightest weight AV tested, includes option of installing their firewall by default, which then tried to block itself from accessing the internet during database update. Very early 2000's feel to the interface.

F-PROT Antivirus

Infected Links : NA

Infected Files : 7/10

Interface : 5/10

System Impact : 9/10
.1% CPU, 12MB RAM

Very reminiscent of Clam AV, more geared towards linux then windows. Not updated since 2011.

And bonus! herdProtect

Infected Links : N/A

Infected Files : 10/10

Interface : 8/10

System Impact : 8/10

.1% CPU, 32MB RAM

68 engines included but it is only a 2nd line of defense you can use with an AV. Not an actual one with real time protection. Did find all malware after it was installed but, took forever to scan.

My closing thoughts are that Qihoo or Panda Cloud are the best choices for free and that for paid products, you cannot go wrong with Kaspersky, ESET, Emsisoft or F-Secure. You get what you pay for and most of the paid products are complete suites with a firewall. Almost all Antivirus will detect new threats within 24 hours now and will only miss a FUD (Fully Undetectable) file. Though some now will detect malicious behavior and warn you. A little common sense is still the first line of defense. I hope that this has given you some insight into which Antivirus product you should get and use. It still is up to you to pick the one that meets your needs.

Thread formatting, editing and add-ons done by [Aura](#)

Hunting Rifle - December 13, 2014, 6:17 pm

Nice thread skid.

Make the next one about fake positives on virus total.

Aura - December 13, 2014, 6:17 pm

(Dec 13, 2014 07:17 PM)Hunting Rifle Wrote: [\[CITE\]](#) Nice thread skid.

Make the next one about fake positives on virus total.

Don't give him thread ideas, guess who's stuck doing the formatting so it looks decent after ?

Also, big fucking lol at the comments, I'm dying on my char everytime I read them.

-Hyperion - December 13, 2014, 7:30 pm

(Dec 13, 2014 07:17 PM)Hunting Rifle Wrote: [\[CITE\]](#) Nice thread skid.

Make the next one about fake positives on virus total.

That is a great idea how to read a report etc

Aura - December 13, 2014, 7:31 pm

(Dec 13, 2014 08:30 PM)-Hyperion Wrote: [\[CITE\]](#) That is a great idea how to read a report etc

Throw other reports in it, like malwr.com, hybrid-analysis, Anubis, etc.

Aura 2.0 - December 13, 2014, 7:33 pm

Did all the VMs have the exact same specs?

-Hyperion - December 13, 2014, 7:46 pm

(Dec 13, 2014 08:33 PM)Mapl3 Wrote: [\[CITE\]](#) Did all the VMs have the exact same specs?

Yes all where exactly the same Maple

Paathurnax - December 14, 2014, 4:32 pm

Came to this thread from the link you posted on another thread ten minutes ago.

This was a good read actually. I'm glad I clicked. The part about Norton getting itself infected and trying to delete itself made me laugh.

-Hyperion - December 14, 2014, 7:02 pm

I am thinking of adding a shit ton more tests just to see how other products do

KFC Watermelon - December 15, 2014, 6:33 pm

There is no way antivirus software like AVG are using 2MB of RAM. There are hidden processes and services that use additional RAM and are not visible in task manager as they run above userland. The real tests are CPU bound and how fast the scanner works.

You also gave little information about the threats thrown at the security software.

Other than that, thank you for taking your time to test these products. In my experience, Kaspersky and ESET are top tier, ESET is a complete bitch to deal with for malware coders. COMODO use to be great...No so much anymore.

Windows defender is a joke. I love malwarebytes, but I have personally seen it let in so much adware and malware that it shouldn't had.

Aura - December 15, 2014, 6:34 pm

(Dec 15, 2014 07:33 PM)KFC Watermelon Wrote: [\[CITE\]](#) There is no way antivirus software like AVG are using 2MB of RAM. There are hidden processes and services that use additional RAM and are not visible in task manager as they run above userland. The real tests are CPU bound and how fast the scanner works.

You also gave little information about the threats thrown at the security software.
Holy fuck you are still alive. Please work on KFCleaner to make it more efficient.

-Hyperion - December 15, 2014, 7:06 pm

(Dec 15, 2014 07:33 PM)KFC Watermelon Wrote: [\[CITE\]](#) There is no way antivirus software like AVG are using 2MB of RAM. There are hidden processes and services that use additional RAM and are not visible in task manager as they run above userland. The real tests are CPU bound and how fast the scanner works.

You also gave little information about the threats thrown at the security software.

Other than that, thank you for taking your time to test these products. In my experience, Kaspersky and ESET are top tier, ESET is a complete bitch to deal with for malware coders. COMODO use to be great...No so much anymore.

Windows defender is a joke. I love malwarebytes, but I have personally seen it let in so much adware and malware that it shouldn't had.

thank you for your kind words. To give more info process explorer was used and these measurements where taken during idle it was more a general idea to be user friendly to understand. The threats where from virus totals free pack and where less then 24 hours old. I can send you the pack of what was ran but it included some trojans, worms, rootkit and a variant of zeus.

M?tt - December 15, 2014, 9:31 pm

I've never heard of Emisoft, but I guess it's a good thing I stopped recommending Avira. I've moved to Avast over the last 2 years and I've noticed that it's much better and I find the interface not too bad. I've used it more often than most though so maybe that's why. I was a huge fan of ESET NOD32 as well.

Great read altogether and actually took some "notes" down from this.

AAE32 - December 16, 2014, 3:25 pm

Thats wasnt nice

Well if you think about panda cloud antivirus sometimes it dosent even detect unencrypted darkcomet stubs and ohter rats stubs.

[Virusotal Darkcomet Scan](#)

Aura - December 16, 2014, 4:03 pm

(Dec 16, 2014 04:25 PM)AAE32 Wrote: [\[CITE\]](#) Thats wasnt nice

Well if you think about panda cloud antivirus sometimes it dosent even detect unencrypted darkcomet stubs and ohter rats stubs.

[Virusotal Darkcomet Scan](#)

Did you try it in real time ? If not, I will for you in a VM tonight.

AAE32 - December 16, 2014, 4:05 pm

(Dec 16, 2014 05:03 PM)Aur? Wrote: [\[CITE\]](#) Did you try it in real time ? If not, I will for you in a VM tonight.Ok hold on i will try it in real time.

-Hyperion - December 16, 2014, 4:28 pm

(Dec 16, 2014 04:25 PM)AAE32 Wrote: [\[CITE\]](#) Thats wasnt nice

Well if you think about panda cloud antivirus sometimes it dosent even detect unencrypted darkcomet stubs and ohter rats stubs.

[Virusotal Darkcomet Scan](#)

you seriously would recommend MSE over anything else? LOL and only a few AV with recognize fresh stubs unless they are submitted or recognized as malicious. The files I tested where less then 24 hours old. MSE is at the bottom even from AV comparative.

Aura - December 16, 2014, 6:24 pm

(Dec 16, 2014 05:28 PM)-Hyperion Wrote: [\[CITE\]](#) you seriously would recommend MSE over anything else? LOL and only a few AV with recognize fresh stubs unless they are submitted or recognized as malicious. The files I tested where less then 24 hours old. MSE is at the bottom even from AV comparative.

I don't think it's even included in AV-Comparatives benchmarks anymore.

AAE32 - December 16, 2014, 6:39 pm

(Dec 16, 2014 07:24 PM)Aur? Wrote: [\[CITE\]](#) I don't think it's even included in AV-Comparatives benchmarks anymore.

Aura - December 16, 2014, 6:48 pm

(Dec 16, 2014 07:39 PM)AAE32 Wrote: [\[CITE\]](#)

Latest benchmark results from AV-Comparatives :

Spoiler [\(Click to View\)](#)

I do not see Microsoft, nor Windows listed. The only place where Windows is listed is the middle line used for "Out-of-the-box protection (blocked) by Microsoft Windows 7 & 8", that's it. I guess that FOR Windows 8/8.1, they evaluate Windows Defender, since it's included, but they do not test Microsoft Security Essentials.

By the way, I tested Panda Cloud Antivirus in a VM, with the most basic DarkComet RAT Stub there is and guess what, it was detected and deleted:

Spoiler [\(Click to View\)](#)

-Hyperion - December 16, 2014, 6:50 pm

Must be defender now I swear it used to say MSE

Aura - December 16, 2014, 7:27 pm

(Dec 16, 2014 07:50 PM)-Hyperion Wrote: [\[CITE\]](#) Must be defender now I swear it used to say MSE
Like I said before, Microsoft Security Essentials USED to be in the benchmarks of AV-Comparatives, but they removed it due to the low detection ratio it have and the fact that it dropped in popularity and I guess people were just not interested in it anymore.

mv3.dds - December 17, 2014, 9:52 am

(Dec 16, 2014 08:27 PM)Aur? Wrote: [\[CITE\]](#) Like I said before, Microsoft Security Essentials USED to be in the benchmarks of AV-Comparatives, but they removed it due to the low detection ratio it have and the fact that it dropped in popularity and I guess people were just not interested in it anymore.

MS is still there. Their results are prob separate due to being DQ'd from the competition bc they are OOB or bc they are being used as a baseline. To see their marks, you enable it from the legend/selection filter.

Kinda interesting how they allowed the mix of free, paid consumer, and paid enterprise to be matched against each other.

Aura - December 17, 2014, 9:58 am

(Dec 17, 2014 10:52 AM)mv3.dds Wrote: [\[CITE\]](#) MS is still there. Their results are prob separate due to being DQ'd from the competition bc they are OOB or bc they are being used as a baseline. To see their marks, you enable it from the legend/selection filter.

Kinda interesting how they allowed the mix of free, paid consumer, and paid enterprise to be matched against each other.

If you go to the award page, and try to see awards for 2013/2014, here's what you get :

Quote:Microsoft is used as non-competitive baseline since 2013.

Also, I can't find the option you're talking about.

mv3.dds - December 17, 2014, 10:27 am

(Dec 17, 2014 10:58 AM)Aur? Wrote: [\[CITE\]](#) If you go to the award page, and try to see awards for 2013/2014, here's what you get :

Also, I can't find the option you're talking about.

i'm assuming you found the legend/selection filter as the previous image was updated.

states in the report's footnotes that MS is not presented in the Awards page due to their being OOB, thus can not be part of the competition.

I honestly prefer AV-Test as their results seems more comprehensive in what was covered and real world OS' involved in the testing. Kapersky was upset w their Home User, but the reasoning was a mixed bag..both agree and disagree w it. If you want to use his status against that 1 portion, then you have to also consider he is extremely against OD test results which a lot of people here swear by.

gizemli56 - December 17, 2014, 11:33 am

I am thinking of adding a shit ton more tests just to see how other products do

Aura - December 17, 2014, 12:03 pm

(Dec 17, 2014 11:27 AM)mv3.dds Wrote: [\[CITE\]](#) i'm assuming you found the legend/selection filter as the previous image was updated.

states in the report's footnotes that MS is not presented in the Awards page due to their being OOB, thus can not be part of the competition.

I honestly prefer AV-Test as their results seems more comprehensive in what was covered and real world OS' involved in the testing. Kapersky was upset w their Home User, but the reasoning was a mixed bag..both agree and disagree w it. If you want to use his status against that 1 portion, then you have to also consider he is extremely against OD test results which a lot of people here swear by.

I don't know why Kaspersky would be upset with their Home User protection results, they scored a perfect score:

Or am I missing something here?

-Hyperion - December 17, 2014, 2:35 pm

(Dec 17, 2014 12:33 PM)gizemli56 Wrote: [\[CITE\]](#) I am thinking of adding a shit ton more tests just to see how other products do

This is not your thread? So I will be doing more products.

Revamp - December 17, 2014, 2:37 pm

You should try 360 Total Security. Its pretty good.

-Hyperion - December 17, 2014, 2:42 pm

(Dec 17, 2014 03:37 PM)?C??c??? Wrote: [\[CITE\]](#) You should try 360 Total Security. Its pretty good. It's a Norton product... Anything but their enterprise is basically crap bloatware. You should never

need a special tool to uninstall a program.

Aura - December 17, 2014, 5:48 pm

(Dec 17, 2014 03:42 PM)-Hyperion Wrote: [\[CITE\]](#) It's a Norton product... Anything but their enterprise is basically crap bloatware. You should never need a special tool to uninstall a program.

Nah he's talking about Qihoo 360 Total Security. This Norton product doesn't exist anymore now with their new rebranding.

-Hyperion - December 17, 2014, 6:13 pm

(Dec 17, 2014 06:48 PM)Aur? Wrote: [\[CITE\]](#) Nah he's talking about Qihoo 360 Total Security. This Norton product doesn't exist anymore now with their new rebranding.

Damn these companies and their similar names. I almost have another 5 to test

Aura - December 17, 2014, 6:25 pm

(Dec 17, 2014 07:13 PM)-Hyperion Wrote: [\[CITE\]](#) Damn these companies and their similar names. I almost have another 5 to test

Do it, it's fun. Now I don't have to do it because you're on it ?

mv3.dds - December 17, 2014, 6:38 pm

(Dec 17, 2014 01:03 PM)Aur? Wrote: [\[CITE\]](#) I don't know why Kaspersky would be upset with their Home User protection results, they scored a perfect score:

Or am I missing something here?

he's upset bc they removed the "Repair" category.

they removed the category bc it's very misleading topic and has almost 0 to do with actual prevention which of course is more important.

he is a fantastic person in IT Sec community, but it's a controversial topic.

Aura - December 17, 2014, 6:45 pm

(Dec 17, 2014 07:38 PM)mv3.dds Wrote: [\[CITE\]](#) he's upset bc they removed the "Repair" category.

they removed the category bc it's very misleading topic and has almost 0 to do with actual prevention which of course is more important.

he is a fantastic person in IT Sec community, but it's a controversial topic.

And what the "Repair" category had to do here ? What was it's real signification ?

-Hyperion - December 17, 2014, 7:01 pm

Now in testing:

Qihoo

Bitdefender

Sophos

Trend Micro

eScan

and bonus! herdprotect

Aura - December 17, 2014, 7:32 pm

(Dec 17, 2014 08:01 PM)-Hyperion Wrote: [\[CITE\]](#) Now in testing:

Qihoo

Bitdefender

Sophos

Trend Micro
eScan
and bonus! herdprotect
Why don't you throw AhnLab in that while you're at it ?

-Hyperion - December 17, 2014, 7:44 pm

(Dec 17, 2014 08:32 PM)Aur? Wrote: [\[CITE\]](#) Why don't you throw AhnLab in that while you're at it ?
Now testing AhnLab and LavaSoft... jk on Lava

mv3.dds - December 17, 2014, 8:07 pm

(Dec 17, 2014 07:45 PM)Aur? Wrote: [\[CITE\]](#) And what the "Repair" category had to do here ? What was it's real signification ?

Kaspersky is upset bc the Testing would become a free for all with much inferior products submitting their products..the same products that would have failed miserably in the Repair category. That it would lead to poor choices in people choosing/recommending AV software applications/suites. He was right of course. haha..

Testing for treatment and recovery after serious infections is so extremely flawed due to it being extremely user dependent..even moreso considering it's Home User category, but he pointed out that removal of the category would lead to horrible software achieving certification and bad IT being rampant w OD as proof rather than as OD results which are extremely unrealistic. he was right on that too sadly, but it was expected.

He is fine with the results of all their main categories presented in the 'Home User' testing.

Loki123 - December 18, 2014, 4:04 am

(Dec 17, 2014 08:32 PM)Aur? Wrote: [\[CITE\]](#) Why don't you throw AhnLab in that while you're at it ?
F-Prot

Would be nice to see how that one does in this test. Icelandic Antivirus :P

P.S

For the record, this doesn't tell you anything what the "best" antivirus is or the percentage of viruses they will detect.

-Hyperion - December 18, 2014, 4:05 am

(Dec 18, 2014 05:04 AM)Loki123 Wrote: [\[CITE\]](#) F-Prot

Would be nice to see how that one does in this test. Icelandic Antivirus :P
it only has a 5% detection rate...jk I will test it tonight

Loki123 - December 18, 2014, 4:06 am

(Dec 18, 2014 05:05 AM)-Hyperion Wrote: [\[CITE\]](#) it only has a 5% detection rate...jk I will test it tonight

Yeh, I would it would have about that... In a proper testing.

Aura - December 18, 2014, 7:39 am

(Dec 18, 2014 05:04 AM)Loki123 Wrote: [\[CITE\]](#) F-Prot

Would be nice to see how that one does in this test. Icelandic Antivirus :P

P.S

For the record, this doesn't tell you anything what the "best" antivirus is or the percentage of viruses they will detect.

It doesn't no, we would need way more samples to throw at them. I think AV-Test uses over a thousand samples when testing the products.

Loki123 - December 18, 2014, 8:28 am

(Dec 18, 2014 08:39 AM)Aur? Wrote: [\[CITE\]](#) It doesn't no, we would need way more samples to throw at them. I think AV-Test uses over a thousand samples when testing the products.

More samples and more details about what viruses were in use. New or old ? (New as completely new virus or crypted rat ? Old as in known..)

What kind of virus ? Backdor ? etc

Aura - December 18, 2014, 8:38 am

(Dec 18, 2014 09:28 AM)Loki123 Wrote: [\[CITE\]](#) More samples and more details about what viruses were in use. New or old ? (New as completely new virus or crypted rat ? Old as in known..)

What kind of virus ? Backdor ? etc

All of this shit ?

If I had more hardware accessible I would do it. I should have that, a computer dedicated to VMs, well, a VM server then while I'm at it.

mv3.dds - December 18, 2014, 11:05 am

(Dec 18, 2014 08:39 AM)Aur? Wrote: [\[CITE\]](#) It doesn't no, we would need way more samples to throw at them. I think AV-Test uses over a thousand samples when testing the products.

they use 100k-150k current wild samples for OD set1

they user over 2k samples (from current live in the wild) for OD set2 - extreme malicious test.

they use a mix of OD and Realtime for their Protection testing.

Jagster™ - December 18, 2014, 4:23 pm

Nice thread buddy! Good to see you're still helping out around here :D

<3

Aura - December 19, 2014, 7:45 pm

Alright, 5-6 Antivirus products are being added right now, and new tests will be done to add new categories.

-Hyperion - December 19, 2014, 7:57 pm

Updated now to include 19 total with qihoo being the new free winner. Scan time and false positives are being added.

AAE32 - December 19, 2014, 11:12 pm

Next time test Nano-antivirus i would like to see how it goes for that antivirus.

Aura - December 19, 2014, 11:18 pm

(Dec 20, 2014 12:12 AM)AAE32 Wrote: [\[CITE\]](#) Next time test Nano-antivirus i would like to see how it goes for that antivirus.

You are talking about this one?

http://www.nanoav.ru/index.php?option=com_content&view=article&id=12&Itemid=74&lang=en

AAE32 - December 19, 2014, 11:35 pm

(Dec 20, 2014 12:18 AM)Aur? Wrote: [\[CITE\]](#) You are talking about this one?

http://www.nanoav.ru/index.php?option=com_content&view=article&id=12&Itemid=74&lang=en

Yeah i was talking about that one yes.

Zher0 - December 19, 2014, 11:47 pm

NanoAV looks interesting, I would like to see it tested out.

Aura - December 19, 2014, 11:51 pm

(Dec 20, 2014 12:35 AM)AAE32 Wrote: [\[CITE\]](#) Yeah i was talking about that one yes.

(Dec 20, 2014 12:47 AM)Zher0 Wrote: [\[CITE\]](#) NanoAV looks interesting, I would like to see it tested out.

Looks like it's actively developped. -Hyperion will add it to it's list of Antivirus products to test.

Aura 2.0 - December 20, 2014, 2:05 pm

(Dec 20, 2014 03:05 PM)Omniscient Wrote: [\[CITE\]](#) This is a paid sticky until December 27, 2014 .HackForums does not endorse the product nor vouch for the seller. As always any deals on HF are at your own risk.

lol, you bought a sticky for your thread.

Aura - December 20, 2014, 2:06 pm

(Dec 20, 2014 03:05 PM)Mapl3 Wrote: [\[CITE\]](#) lol, you bought a sticky for your thread.

Could be worst. Null bought a sticky in the White Hat Help section when I got the White Hat Helper award.

-Hyperion - December 20, 2014, 2:07 pm

(Dec 20, 2014 03:05 PM)Mapl3 Wrote: [\[CITE\]](#) lol, you bought a sticky for your thread.

yeah I felt like they both need to be seen

Hunting Rifle - December 20, 2014, 2:07 pm

(Dec 20, 2014 03:06 PM)Aur? Wrote: [\[CITE\]](#) Could be worst. Null bought a sticky in the White Hat Help section when I got the White Hat Helper award.

How is that worse?

It's the best thing to happen ever.

Proton! - December 22, 2014, 1:32 pm

This is a great thread, thanks for the guidelines :D

Mercury - December 23, 2014, 10:38 pm

Just downloaded Qihoo. Best decision ever. Such a nice GUI. Works great too.

Null. - December 25, 2014, 2:27 pm

Nice effort, Like putting a lot of comments in it so that user's would have a lot of background knowledge about this products.

-Hyperion - December 25, 2014, 4:09 pm

working on adding 2-3 more parts to the review

Aura - December 25, 2014, 5:20 pm

(Dec 25, 2014 05:09 PM)-Hyperion Wrote: [\[CITE\]](#) working on adding 2-3 more parts to the review We should had created a thread with 4-5 posts to counter the image limit.

NoScript - December 27, 2014, 10:45 pm

COMODO has seem to have fallen in the past years, F-Secure seems to be doing really good, I may try it out sometime.

Also I'm glad you included 360 IS, It is also one of my favorites.

AAE32 - December 30, 2014, 8:40 am

I agree. Qihoo is a good antivirus nice and smooth interface and its very fast.

Legendair - February 3, 2015, 11:09 am

Should i start using Qihoo instead of avira ? I hesitate i don't know what to do, ATM i'm still with Avira but i'd like your feedbacks

obviouslyracist - February 3, 2015, 12:31 pm

(Feb 3, 2015 12:09 PM)Legendair Wrote: [\[CITE\]](#) Should i start using Qihoo instead of avira ? I hesitate i don't know what to do, ATM i'm still with Avira but i'd like your feedbacks Avira is still very good. I think you should keep it if you have the specs to run it without problems.

-Hyperion - February 4, 2015, 3:09 pm

Read the review qihoo IS preformed awesome

NoScript - February 4, 2015, 4:30 pm

These are some great results, Qihoo 360 Internet Security is truly the best Anti-Virus for windows!

Chronos46and2 - February 19, 2015, 9:14 am

@-Hyperion, I appreciate that post. I had not seen that one before. The version I have is not the Total Security Suite. I have a different version and I have it bundled with a few extra layers of protection. They all play nicely together and I can't tell if there is any lag. That was cool of you to post those scores. I may try something different when my license is up. Thanks-

dragonmage70 - February 22, 2015, 7:13 am

Hi there, The 360totalsecurity one that you recommended as your favourite new free anti-virus software doesn't work on windows 8.1 it won't let me install it, please could you help?

Cooldax - February 22, 2015, 9:29 pm

Very high quality thread thing about changing my anti virus

legendaryfiles - February 23, 2015, 5:24 am

I am going to test 360 Internet Security and 360 Total Security.
Can i know whats difference between these two

Nick Burkhardt - February 23, 2015, 2:12 pm

You should add your opinions on:

1. TrustPort
2. G Data
3. wontok

I've heard these should be quite good! :)

Null Byte - February 23, 2015, 5:23 pm

(Feb 23, 2015 06:24 AM)legendaryfiles Wrote: [\[CITE\]](#) I am going to test 360 Internet Security and 360 Total Security.

Can i know whats difference between these two
360 Total Security has some extra options for optimizing startup objects and cleaning unnecessary data. It's basically the same thing as the Internet Security version but with some tuneup capabilities.

Aceman - February 24, 2015, 12:07 pm

Read it thoroughly and I now have some good options when installing free anti viruses. Thanks a lot for this. ?

-Hyperion - February 24, 2015, 6:48 pm

(Feb 23, 2015 06:23 PM)Null Byte Wrote: [\[CITE\]](#) 360 Total Security has some extra options for optimizing startup objects and cleaning unnecessary data. It's basically the same thing as the Internet Security version but with some tuneup capabilities.
it also tested differently which was not as good

legendaryfiles - February 25, 2015, 5:42 am

I have observed that avira free version is slower than 360 IS
360 IS has faster startup time than avira and 360 also uses less RAM and CPU than avira
Thanks -Hyperion for this thread. :D

Vuln - February 25, 2015, 6:32 am

Nice work Hyperion, definitely helpful.

For those of you wanting to try Qihoo 360, please know that it's a company located in Beijing with a shady history full of malicious accusations and even confirmed backdoors.

Millions and millions of users (mostly in China) are using it, but I myself am not ready to trust them just yet.

-Hyperion - February 25, 2015, 3:33 pm

(Feb 25, 2015 07:32 AM)Jailbyte Wrote: [\[CITE\]](#) Nice work Hyperion, definitely helpful.

For those of you wanting to try Qihoo 360, please know that it's a company located in Beijing with a shady history full of malicious accusations and even confirmed backdoors.

Millions and millions of users (mostly in China) are using it, but I myself am not ready to trust them just yet.

I would like to see sources from reputable security researches showing a backdoor please.

Pepesi - February 26, 2015, 2:07 am

(Feb 25, 2015 07:32 AM)Jailbyte Wrote: [\[CITE\]](#) Nice work Hyperion, definitely helpful.

For those of you wanting to try Qihoo 360, please know that it's a company located in Beijing with a shady history full of malicious accusations and even confirmed backdoors.

Millions and millions of users (mostly in China) are using it, but I myself am not ready to trust them just yet.

???? can you give any more info? I'd like to know

Vuln - February 26, 2015, 2:53 pm

Can't find my original source, but it looks like IDF did some decent research.

<http://blog.idf.cn/2012/11/independent-report-on-alleged-hidden-backdoor-in-qihoo-360-secure-browser/>

There are tons and tons of other articles as well, some with proof, others just accusations and perhaps propaganda. It might be also worth mentioning that Qihoo had a reputation of avoiding difficult questions and denying explanation requests. The vast majority of the articles and research I

found was (obviously) in Chinese, so I won't look into it much further myself. I just wanted to let you know so you could decide for yourself.

Some food for thought (propaganda or not, you tell me):

<http://www.ibtimes.com/privacy-issues-chinas-qihoo-360-technology-which-provides-free-antivirus-software-are-becoming-more>

http://static.cdn-seekingalpha.com/uploads/2012/8/2/582827-13439356679495025-Matt-Berry_origin.jpg

<http://seekingalpha.com/instablog/582827-matt-berry/722711-qihoo-backdoor-suspicious-erupt-in-user-backlash>

<http://tech.huanqiu.com/Internet/2012-05/2771631.html>

<http://www.programdevelop.com/2378989/>

<http://news.cnblogs.com/n/152835/>

http://www.theregister.co.uk/2013/02/01/qihoo_government_warning_fraud/

<http://www.globaltimes.cn/content/773944.shtml>

All accusations were in the past though, and I'm sure it's a legit company now. But I'm not going to trust them anyway.

(Feb 25, 2015 04:33 PM)-Hyperion Wrote: [\[CITE\]](#) I would like to see sources from reputable security researches showing a backdoor please.

(Feb 26, 2015 03:07 AM)Pepesi Wrote: [\[CITE\]](#) ???? can you give any more info? I'd like to know

Warren Buffett - February 26, 2015, 7:10 pm

It tried deleting itself! Haha that was funny.

legendaryfiles - February 27, 2015, 11:30 pm

(Feb 26, 2015 03:53 PM)Jailbyte Wrote: [\[CITE\]](#) Can't find my original source, but it looks like IDF did some decent research.

<http://blog.idf.cn/2012/11/independent-report-on-alleged-hidden-backdoor-in-qihoo-360-secure-browser/>

There are tons and tons of other articles as well, some with proof, others just accusations and perhaps propaganda. It might be also worth mentioning that Qihoo had a reputation of avoiding difficult questions and denying explanation requests. The vast majority of the articles and research I found was (obviously) in Chinese, so I won't look into it much further myself. I just wanted to let you know so you could decide for yourself.

Some food for thought (propaganda or not, you tell me):

<http://www.ibtimes.com/privacy-issues-chinas-qihoo-360-technology-which-provides-free-antivirus-software-are-becoming-more>

http://static.cdn-seekingalpha.com/uploads/2012/8/2/582827-13439356679495025-Matt-Berry_origin.jpg

<http://seekingalpha.com/instablog/582827-matt-berry/722711-qihoo-backdoor-suspicious-erupt-in-user-backlash>

<http://tech.huanqiu.com/Internet/2012-05/2771631.html>

<http://www.programdevelop.com/2378989/>

<http://news.cnblogs.com/n/152835/>

http://www.theregister.co.uk/2013/02/01/qihoo_government_warning_fraud/

<http://www.globaltimes.cn/content/773944.shtml>

All accusations were in the past though, and I'm sure it's a legit company now. But I'm not going to trust them anyway.

I didn't know about this.

I would never trust chinese softwares.

They just have some kind of shit inside them.

Thanks for this info bro.

-Hyperion - February 28, 2015, 5:13 pm

(Feb 28, 2015 12:30 AM)legendaryfiles Wrote: [\[CITE\]](#) I didn't know about this.

I would never trust chinese softwares.

They just have some kind of shit inside them.

Thanks for this info bro.

do you realize how much of the software you use is coded in china and india?

Nanaz - March 23, 2015, 12:58 am

Thank you!! Was very shocked on a couple of them might have to make a few changes myself. :)

Retribute - March 24, 2015, 11:13 pm

Nice contribution to this section. Good work.

archangel.dmitry - March 25, 2015, 7:19 am

First of all, it is a good work you have done. But it needs some input.

I am sorry but your report on CPU usage is bogus. Defender hogs a lot CPU once you start doing anything on your computer. By a lot, I mean 20% and higher.

Based on number you have provided avast Free is better than anything else. Who cares if its interface is not pretty. Avira free does not have own firewall. It monitors Windows Firewall.

-Hyperion - March 25, 2015, 7:45 am

(Mar 25, 2015 07:19 AM)archangel.dmitry Wrote: [\[CITE\]](#) First of all, it is a good work you have done. But it needs some input.

I am sorry but your report on CPU usage is bogus. Defender hogs a lot CPU once you start doing anything on your computer. By a lot, I mean 20% and higher.

Based on number you have provided avast Free is better than anything else. Who cares if its interface is not pretty. Avira free does not have own firewall. It monitors Windows Firewall.

To address your points every computer tests differently and if you read for it was tested everything was tested at idle, MSE not defender on 8 was tested. Second Avg actually scored higher but my recommendations take into account other factors such as ease of use.

archangel.dmitry - March 25, 2015, 8:09 am

Quote:Microsoft Security Essentials (now Windows Defender under Windows 8/8.1)

Quote:... MSE not defender on 8 was tested ...

You can't use MSE on Windows 8.1 and probably 8.

Quote:... Second Avg actually scored higher ...

Difference is 0.1% (no difference based on tools you used) for CPU.

There is difference in RAM but I am not sure if it is relevant. If AV engine keeps its definitions cached in RAM, it makes the engine work faster. I am not so sure, if it is disadvantage.

-Hyperion - *March 25, 2015, 8:32 am*

(Mar 25, 2015 08:09 AM)archangel.dmitry Wrote: [\[CITE\]](#) You can't use MSE on Windows 8.1 and probably 8.

Difference is 0.1% (no difference based on tools you used) for CPU.

There is difference in RAM but I am not sure if it is relevant. If AV engine keeps its definitions cached in RAM, it makes the engine work faster. I am not so sure, if it is disadvantage.

Everything was tested on 7 their engines however are pretty much the same