Security Survey 2011

Language: English

Last Revision: 10th March 2011

www.av-comparatives.org

Introduction

To improve our service we asked our website visitors on their opinion about various topics related to Anti-Virus Software Testing and Anti-Virus Software in general. The results are very helpful for us and we want thank all who joined the survey and spent their time to complete it.

Key data

Survey Period:	**15th December 2010 – 15th January 2011**
Total Survey Submissions:	**1247**
Invalid responses:	**182** (84 invalid, 98 responses from AV-related participants)
Valid responses:	**1065**

The survey contained a few tricky questions and checks to allow us to filter out invalid responses and users who tried to distort the results or by giving impossible/conflicting answers. As we were primarily interested in the opinions of real/common users and visitors to our website, the survey results in this public report does not take into account the responses of the AV-related participants.

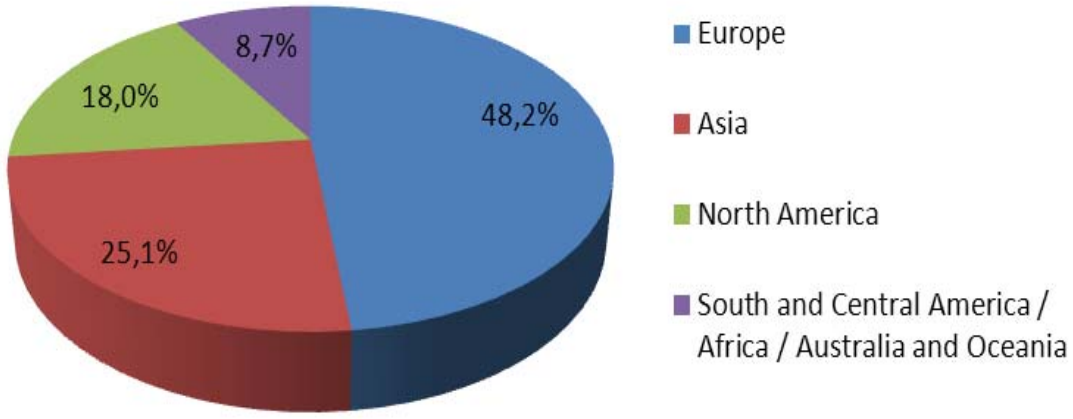
Please note that the survey participants, who kindly filled out our long survey, are only a representative subset of our website visitors. Please do not overstretch the results of the survey; they just give an indication based on what the survey participants answered. Be aware that this report also contains some personal comments and opinions.

The results of the survey are very valuable to us; you will find in this report the results of some of the survey questions which we would like to share with you.

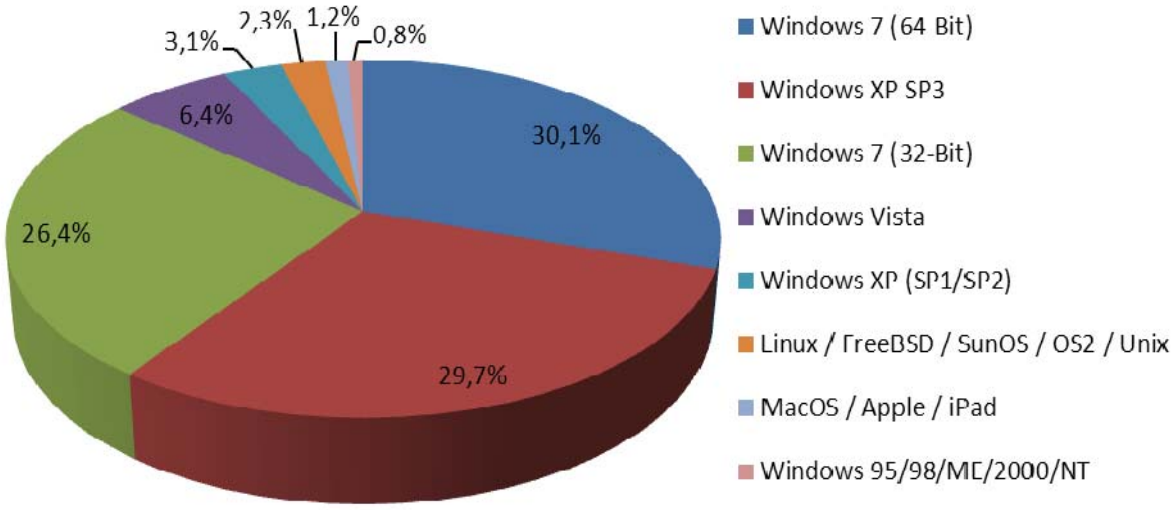
Sample population

The following three questions cover population aspects, so that we could compare them with our internal website statistics, and get a feeling for whether the sample set of survey participants is big enough to represent our visitors. The answers to the questions correspond with our website statistics in the survey period (indicating that the survey participants are a representative sample of our users).

1. Where are you from?



2. Which operating system are you primarily using?



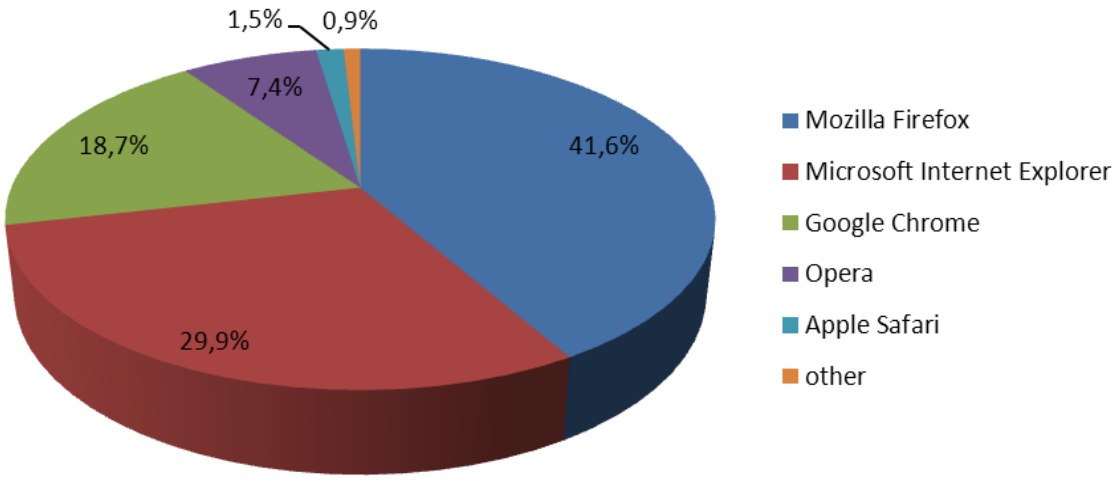
Windows 7 now finally seems to be the operating system that has taken over from Windows XP, at least for the home users who took part in our survey. In business environments XP is probably still widely used, although it will be surpassed there too in the next few years. According to the Global Stats of Statcounter[1], about 48% of the users worldwide are using Windows XP and only about 29% are using Windows 7 so far. The 64-bit variant of Windows 7 is more used than the 32-bit variant, most probably because under 64-bit it is possible to use more than 4GB of RAM.

[1] http://www.statcounter.com

Although in detection tests there is practically no difference between different operating systems used, there is definitely a difference in performance, due to which we switched to Windows 7 in 2010 for the performance tests. We may also consider switching to Windows 7 for the dynamic tests in 2012; currently we still perform them under XP, as we want to evaluate primarily the protection provided by the security products, not the protection provided by a specific OS (if all users used up-to-date and patched operating systems and software, maybe there wouldn't be so many successful malware attacks in the world).

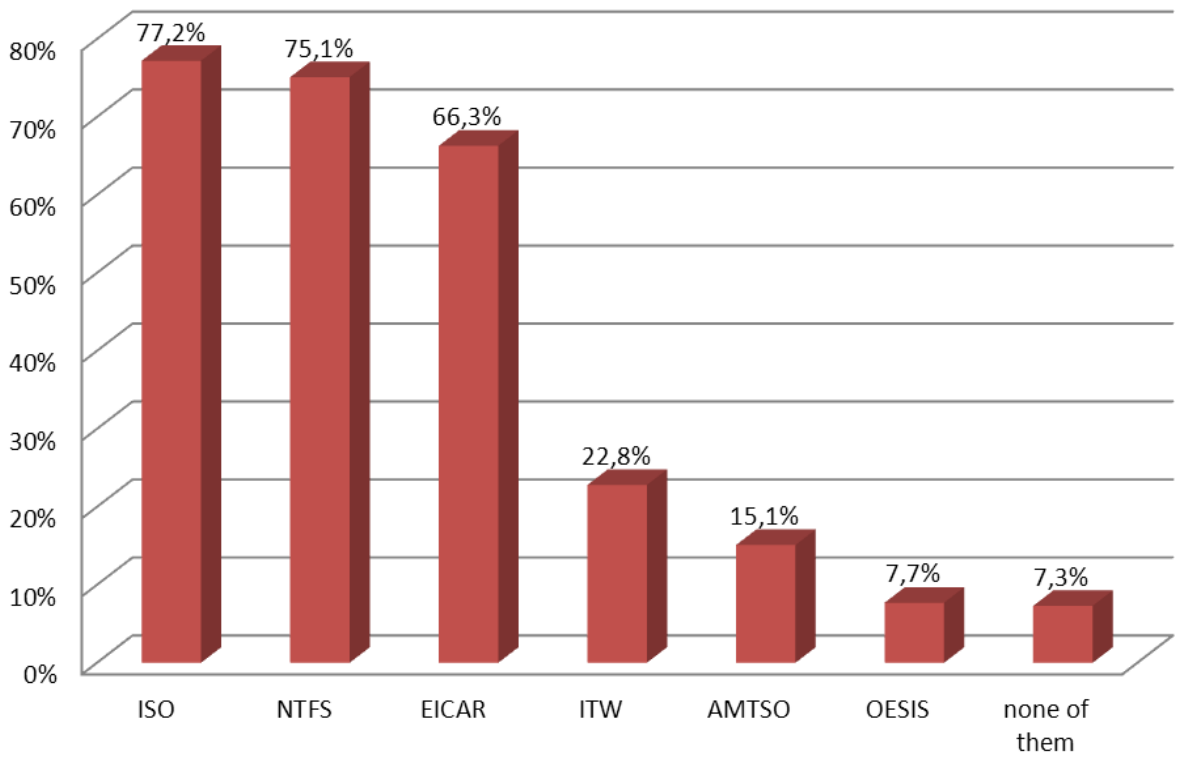
Furthermore, as our tests are geared more towards the average user in general than the more security-aware readers of our website, the choice of operating system considers the global stats of OS usage.

3. Which browser are you primarily using?



According to the Global Stats of Statcounter, about 46% of the users worldwide are currently using Microsoft Internet Explorer and only about 30% are using Mozilla Firefox (except in Europe, were users tend to prefer Mozilla Firefox).

4. Which of those acronyms are known to you?



5. Which Antivirus solution are you currently primarily using?

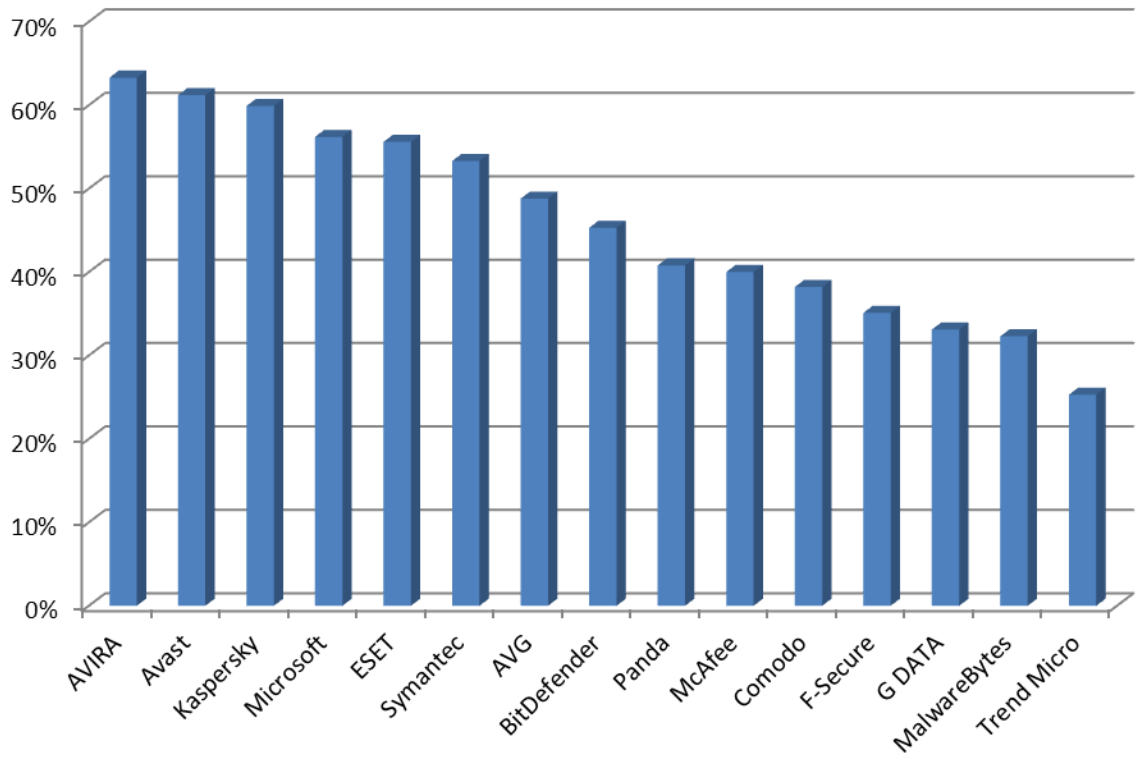
Among the most used antivirus solutions, the survey results suggest that the free available software versions prevail, e.g. Avast, AVIRA, Microsoft, AVG, Comodo, etc. followed closely by well-known commercial security solutions like from Symantec, Kaspersky, ESET, McAfee, etc.

The results confirm the assumption that about the half of all users are using free antivirus solutions. Also a survey from OPSWAT[2] came to similar results.

[2] http://www.oesisok.com/news-resources/reports/worldwide-antivirus-market-share-report%202010

6. Which security solutions would you like to see in our tests?

We list here only the vendors which at least 25% of the survey participants voted for:



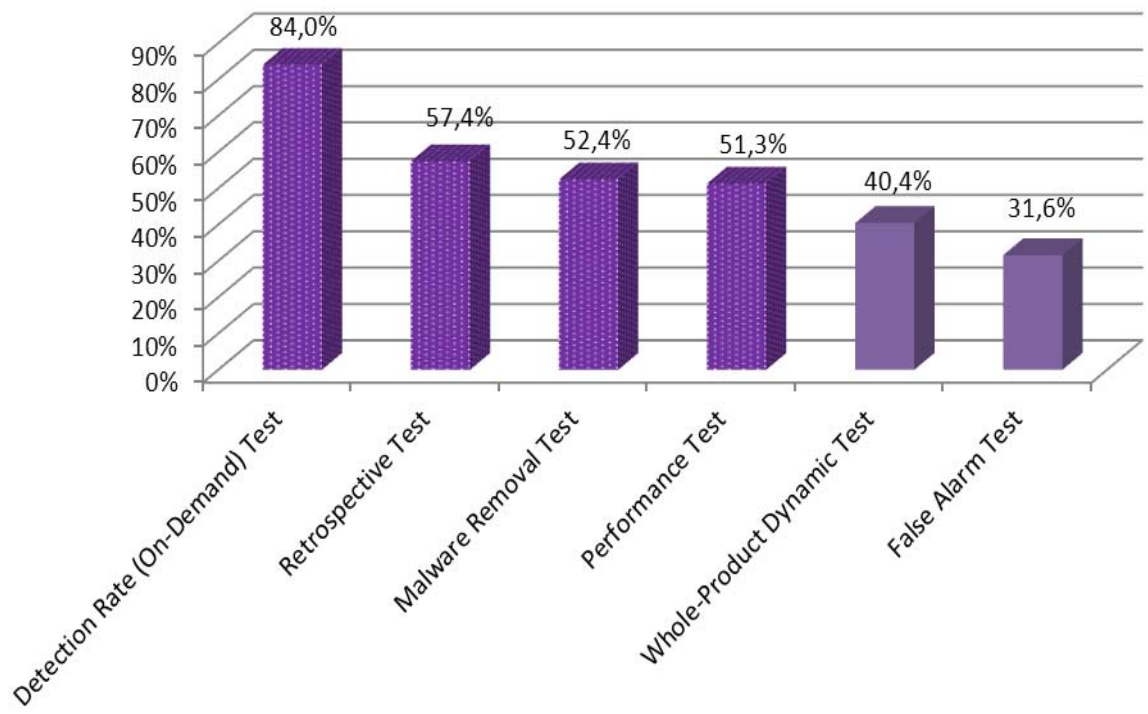
The above are the top 15 requested products (from a list of 70 well-known ones).

MalwareBytes is not intended primarily as a full replacement[3] of an antivirus product or security suite, but rather as a complimentary tool focussed on a smaller set of threats and its removal from compromised systems. Therefore, it would be wrong to compare it to AV products as we usually test.

Unfortunately, although Comodo is a high demanded test candidate in this survey, Comodo did not apply to participate in our 2011 test series, but they agreed to be tested separately in a Single Product (On-Demand) Test.

[3] http://www.wilderssecurity.com/showpost.php?p=1826047&postcount=2

7. Which type of tests are you most interested in?



Based on the responses (users had to **choose 4 from 12 tests** which they are most interested in), users do not seem to be interested at all in anti-spam tests. Tests based on the Wildlist and tests against potentially unwanted applications also seem not to be very interesting for users.

Clearly the great majority of users are interested in on-demand malware detection rate tests, as well as retrospective tests which evaluate the heuristics etc. Malware removal and performance testing also have high value. Last year we were not able to perform the malware removal test in time, but considering how much users want this type of test, we will do our best to conduct a malware removal test again this year.

Surprisingly, the Whole-Product Dynamic Test, which aims to perform an in-depth test of the security software under real-world conditions, and which is promoted by the AV industry as the best type of test to reflect product capabilities, still only gets a modest 5th in the users' list of requested tests. We expect that over time, users will start to appreciate this type of test more and more. Anyway, we see and understand that the users will continue to be interested also in the "conventional" tests which measure on-demand detection rates etc.

8. In your opinion, which of the following testing labs are...

The survey participants had to rate 22 testing labs, with the following three choices:

- Reliable/trustworthy/independent
- Biased by vendors/unreliable
- I do not know them

The five most trustworthy/reliable/independent testing labs according to the survey participants:

1. AV-Comparatives
2. Virus Bulletin / AV-Test
3. ICSA Labs / West Coast Labs

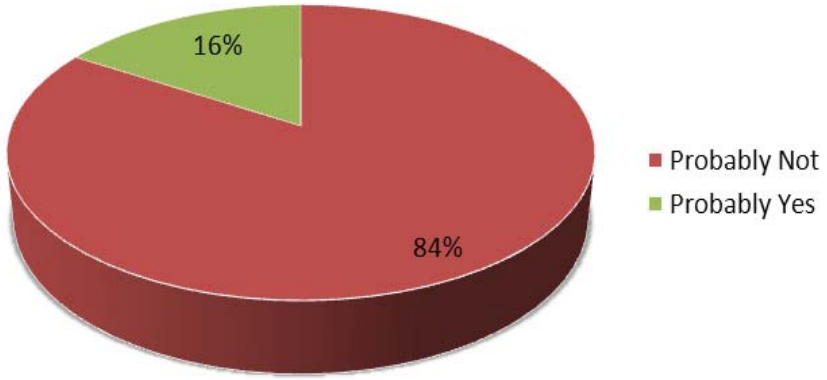
VirusBulletin and AV-Test were rated similarly, as well as the two certification labs ICSALabs and WestCoastLabs (which is why we put them on same level). AV-Comparatives got by far the highest positive rating, but as the survey was produced by us and the survey participants are our website visitors, this was to be expected – although other surveys on unrelated websites have also rated AV-Comparatives on top (thank you!).

The five most unknown labs according to the survey (which almost nobody had ever heard of):

1. TollyGroup
2. ENEX
3. JCSR
4. eKaitse
5. Cyveillance

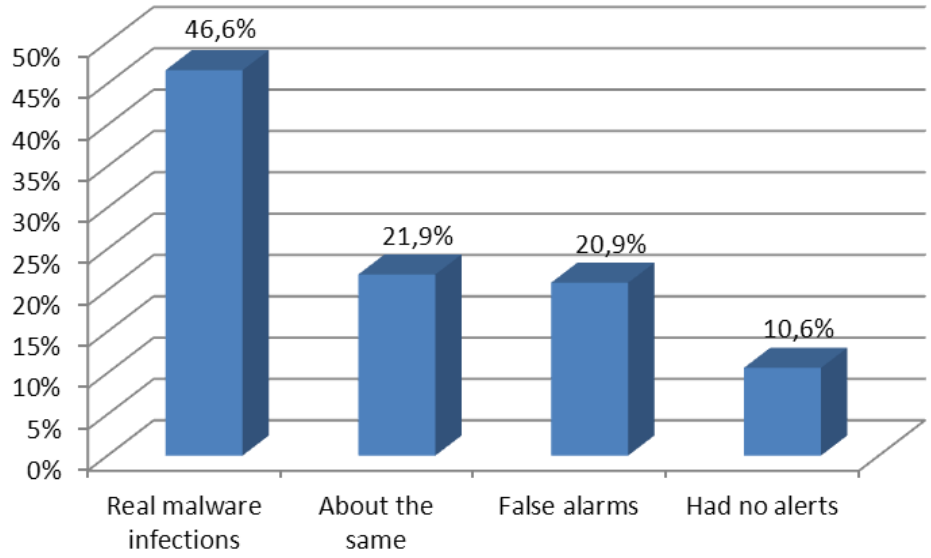
To do no "harm" to specific testing labs/websites, we will keep confidential which ones were considered by the survey participants as the most unreliable and vendor-biased.

9. Would you use an AV which does not include any on-demand scanning feature?



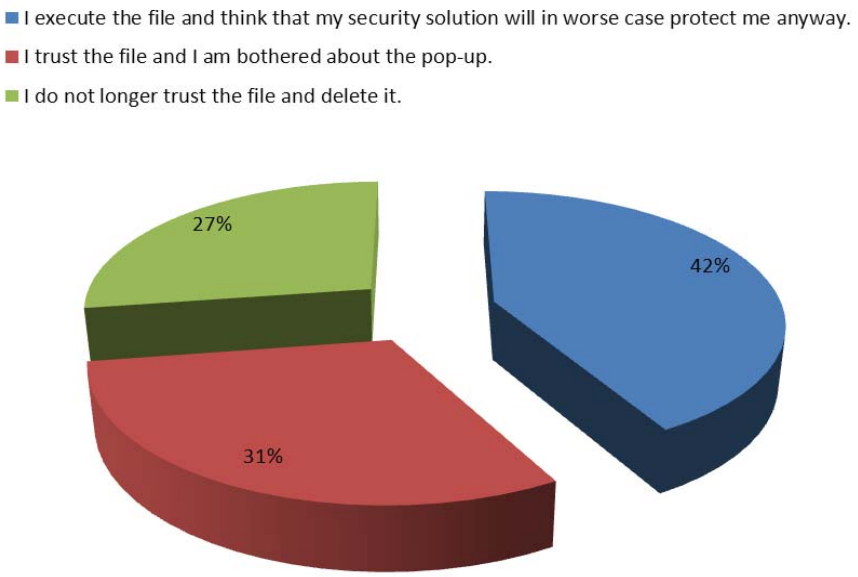
The reason for the above question was that we heard of an idea by some vendors not to provide an on-demand scanning function anymore in their products. In our opinion, some vendors are not in touch with users' needs and wishes, so we wanted to see if the survey participants agree with us that removing such a feature would not be welcome.

10. If you had any malware alerts in the last 12 months, do you think they were mostly real or mostly false positives?



Fortunately most alerts seem to have been real ones, but the false alarm incidence seems to be an issue which is underestimated and underrated by some vendors.

11. If your AV product or your operating system asks you if you trust a file that you downloaded on purpose from the Internet, how do you usually answer?



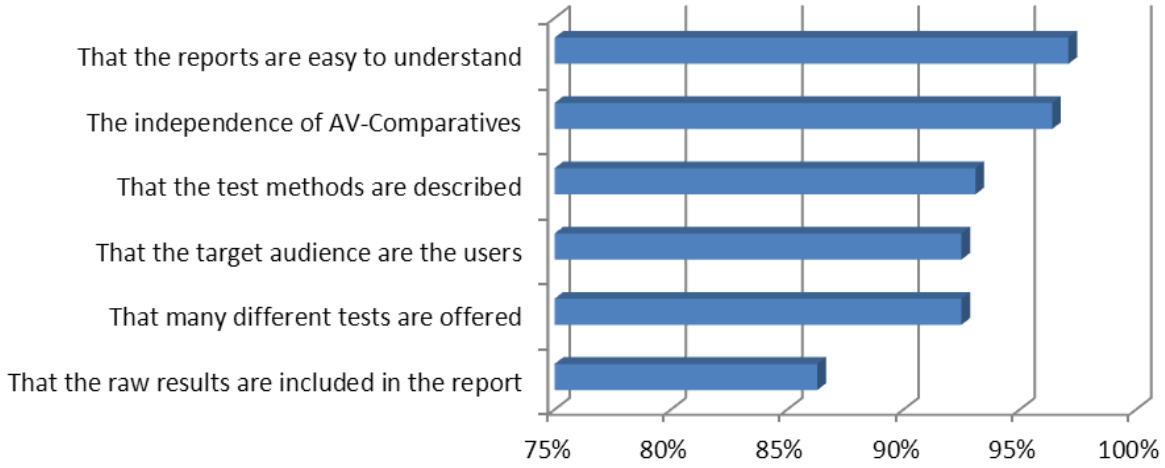
Apparently not everyone seems to have understood this (we concede that the question was rather confusing), so take the result with a pinch of salt. Based on our field experience with customers, we believe that most everyday users often ignore questions and warnings from their operating system/security software.

It should be noted that there are two common types of security notification that are encountered by users. Windows will typically ask for user confirmation before executing ANY program file downloaded from the Internet, without making any assumption as to whether the file is good or bad. For example, running the setup file for a genuine Antivirus, typically the safest of safe files, brings up a Windows 7 UAC prompt, requiring the user to confirm that the file should be run. This relies entirely on the user to decide if the file is good or bad; always clicking "No" would mean that the user could never install any legitimate software that he/she had downloaded from the Internet. The second type of security notification comes from security software such as antivirus programs or Windows Defender (to be seen here as a separate application rather than part of Windows). Security programs may warn that a SPECIFIC file could be dangerous, on the basis of e.g. behaviour/reputation. In this case, the sensible option is always to click "No" to installation, as a legitimate application would probably not have produced such a warning.

Our advice to users is: if you see a prompt asking you whether to install software, or warning you against it, STOP AND THINK before clicking on anything.

Our advice to software manufacturers is: remember that many average users don't think before clicking on security prompts; they expect their product will decide for them if something is good or bad, and block it if it's bad. The story of "The boy who cried WOLF" applies here: too many false alarms and user interactions lead to genuine warnings being ignored, its human nature.

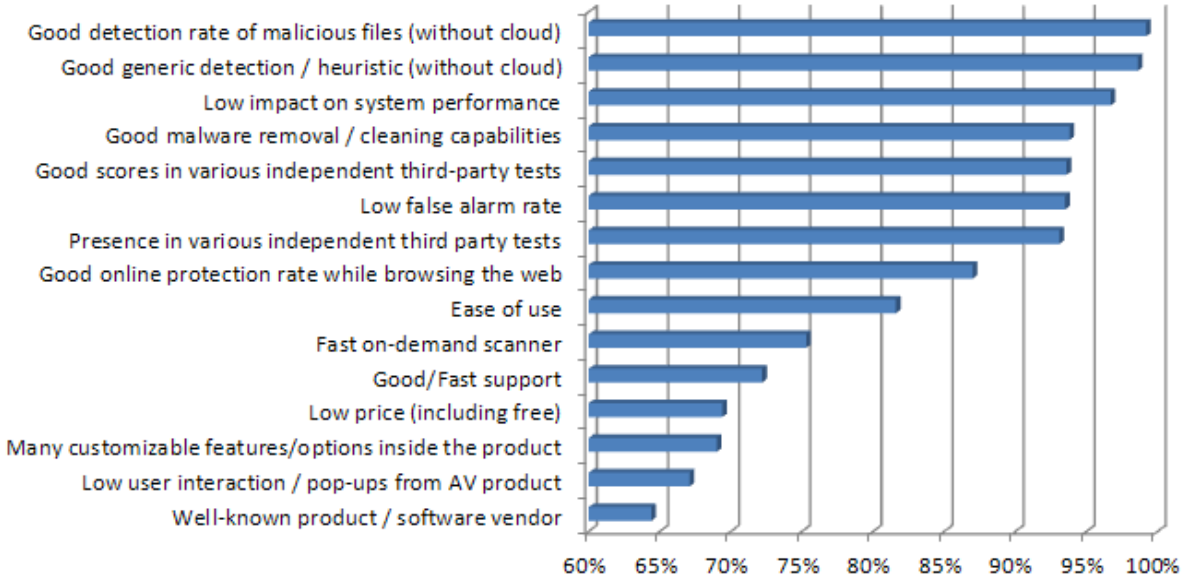
12. What do you find important on AV-Comparatives?



Furthermore, about half of the users said that they like the fact that they can contact us (the testers) if they want to, and that we have started to provide reports in various languages.

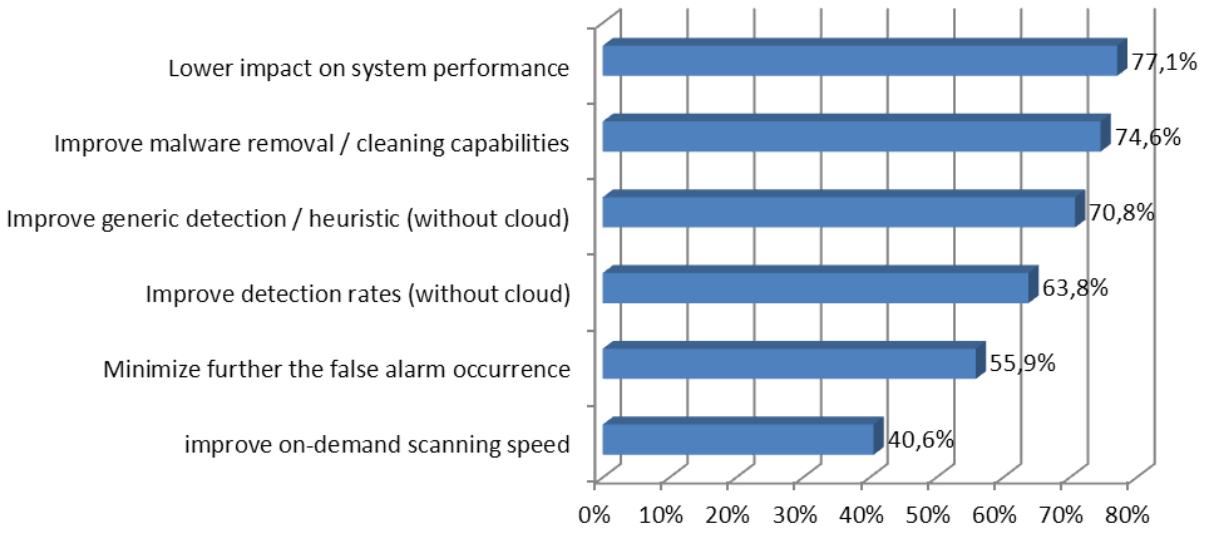
We also noted the nice comments towards AV-Comparatives and we will try to fulfil some of the expressed wishes. Some requests are not possible to realize (e.g. because they would require too many unavailable resources; we are not Google ☺), while some others are already in place on our website/in reports, but maybe not have been noticed/read by all users.

13. What is important for you in a security product?



Note: "*Without cloud*" means "*without being dependent of cloud/online connection*." This was explicitly written in the survey, as we knew/expected that most users still prefer products not being dependent of clouds / online connectivity to provide reliable protection.

14. What should AV vendors try to improve more, in your opinion?



Users had to **select 6 product aspects** which in their opinion AV vendors should improve more. The graph above shows the 6 most selected product aspects. It may be an indication of what users *feel* to be weak aspects of the products. Some few further expressed user wishes (under 20%) were: stronger default configurations, detection of commercial keyloggers etc. (non-detection is a reason to mistrust AV products), rely less on cloud/online connectivity, lower prices and better customer support.

Copyright and Disclaimer

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (March 2011)