



Release rates & update sizes of
Signature databases of some main
top Anti-Virus products

Date: July 2006

Last revision: 10th August 2006

Author: Andreas Clementi

Website: <http://www.av-comparatives.org>

1. Introduction

This test report provides data about the release rates of virus signature updates and the average size of each single incremental update. For this test four products that scored very highly in the last two on-demand tests of August 2005 and February 2006 and consistently received the ADVANCED+ certification in those tests were selected. The products included in this test report are:

- ❖ ESET NOD32 Anti-Virus 2.51.8
- ❖ Kaspersky Anti-Virus 6.0.0.300
- ❖ McAfee VirusScan 10.0.27
- ❖ Symantec Norton Anti-Virus 12.2.0.13

Note that the data in this report refers to the product version listed above. Past versions may differ (e.g. they may not support incremental updates), so we recommend you keep your program versions up-to-date to get optimal/new features.

Beside the importance of high proactive on-demand detection rates of Anti-Virus products, it is important that signature updates are released at least daily and cover new malware as much as possible. This is especially important if products do not have high on-demand proactive detection rates when it comes to new malware (i.e. do not have strong heuristics or generic detection capabilities). Such products need to deliver signature updates to the users as soon as possible.

In this test rather than look at the response time to worldwide outbreaks of specific viruses (which may vary from malware to malware), we examine the normal pattern of release of signature updates for malware in general. As many new viruses and other types of malware appear very day, it is clearly preferable that Anti-Virus products are able to detect such threats in advance with generic and/or heuristic techniques (see our retrospective tests reports).

In cases where such proactive detection is unsuccessful or unavailable, new updates must be provided, as often and as fast as possible to the user, in order to identify and remove those new threats. Even if nowadays most anti-virus products provide daily or even hourly updates, it is also important to look at how many new signatures the released updates contain, and the importance of the signature. Users should set their AV products to automatically receive updates, in order that the new updates are installed as soon as they are available. Furthermore, especially for the users that have a dial-up or low-speed connection etc. it can be of importance that the updates are of small size and do not take too much time to download and consume too much of the available bandwidth.

The data contained in this test report is based on observations over some few weeks in June/July, but is anyway of interest and gives lot of information. As it is, the data includes some slight variance of time due to numbers being rounded, as exact (unrounded) numbers would not make sense.

We decided to exclude some other data which would require a longer measurement time-frame (e.g. the rate of growth of the virus signature database in a month, the required time to scan the same set of files over the time, etc.), but we may provide such data in future, including more AV products and measuring over a longer time period¹, if time permits.

¹ We have to further refine the methods for such a test.

2. Average release rate of signature updates

The release schedule of normal signature updates of ESET, Kaspersky, McAfee and Symantec are as follow:

Kaspersky: usually once per hour

ESET: no fixed schedule, but usually twice per day

Symantec: usually once per day

McAfee: usually once per day (except weekends)

We observed the following release rate for those companies:

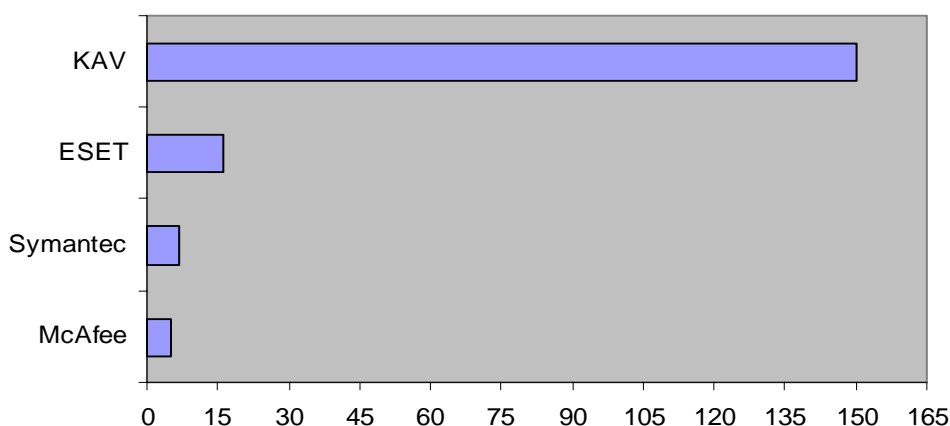
Kaspersky: ~150 updates per week

ESET: ~ 16 updates per week

Symantec: ~ 7 updates per week

McAfee: ~ 5 updates per week

Average release rate – Updates per week



According to this data, Kaspersky releases updates more often than any of the other three tested Anti-Virus products in this report.

Sometimes these (Kaspersky) updates contain only 1 signature for 1 malware sample sent in by 1 user. For that user it may be important to get the update as soon as possible (if the user is really infected), but for other peoples that update may be not of importance to get immediately.

In similar cases McAfee often sends an ExtraDAT file to the user quite quickly and later includes that signature in the daily updates, which will be then shipped to all users. It is worth noting that, even if an AV vendor is providing hourly updates or which add a few new signatures, it does not mean that the AV vendor has added all samples currently available in their lab. Some samples may get added weeks, months or even years later, depending on the priority the vendor gives to the sample. (This is often to do with submission source and viability of the sample)

The more quickly updates are released, the shorter is the time available for QA testing, to assure the quality and accuracy of the newly added signatures. (QA is needed to avoid problems like false positives or conflicts on the system). That's why sometimes AV vendors release (sometimes several) updated versions of the same signatures.

This is shown in the fact that Symantec and McAfee have fewer false positives than Kaspersky and ESET (see test report No. 10)².

² <http://www.av-comparatives.org/seiten/ergebnisse/report10.pdf>

3. Average size of single incremental updates

The numbers below show the average size per incremental update. The sizes vary from a few KB's to several MB's, but in the observed weeks, the average download size of the incremental updates was:

KAV:	around	2 KB per update	(~300 KB per week)
ESET:	around	30 KB per update	(~480 KB per week)
Symantec:	around	70 KB per update	(~490 KB per week)
McAfee:	around	100 KB per update ³	(~500 KB per week)

According to this data, the overhead in download traffic over a week is more or less the same for all products and is of an affordable size (in terms of download time/bandwidth available).

If the Anti-virus product is set to update very often, the total traffic caused per day may be higher in those that deliver updates fewer times, as every check for new updates - even if no new updates are available - requires the exchange of a few KB's of traffic⁴.

Some products may sometimes include in their incremental updates other program components, for instance heuristics modules, engine updates etc. which may require more size than the signatures alone. In the case of larger updates or updates that contain major alterations to the program, the size of the updates can be much higher, (possibly several MB's). The time needed to download the updates depends both on the speed (load/network capability) of the download servers and the connection speed of the users. Sometimes; especially where AV vendors release weekly or monthly cumulative updates or have slower responding servers in case of bigger updates; the update download servers are unreachable and many hours can pass before the users can finally update their software.

We recommend that users download trial versions of the Anti-Virus products to observe for themselves how often the updates are released and how large they actually are, together with the speed of the servers etc.

4. Average download size of full signature databases

The average download size of full signature databases is mainly only of interest in case of a full manual update, or the initial installation of a product. During the test period the full update sizes to download for those products were:

McAfee:	about	7,7 MB ⁵
ESET:	about	9,7 MB
KAV:	about	9,8 MB
Symantec:	about	11,3 MB

So, there is an average of ~9.6 MB.

AV vendors do their best to keep the size of the updates as low as possible. Some vendors may during coming months make changes to their products which will shrink their databases and update sizes, as part of a long term strategy to minimize database size. Often they replace signature definitions with more generic detections, and use different packing and compression methods, etc. (without any negative influence to the detection rates).

³ The new product line of McAfee (which will be released in August) decrease the size of the updates significantly.

⁴ e.g. if you try to update KAV every 3 minutes, you will have ~400 KB extra traffic at day for nothing.

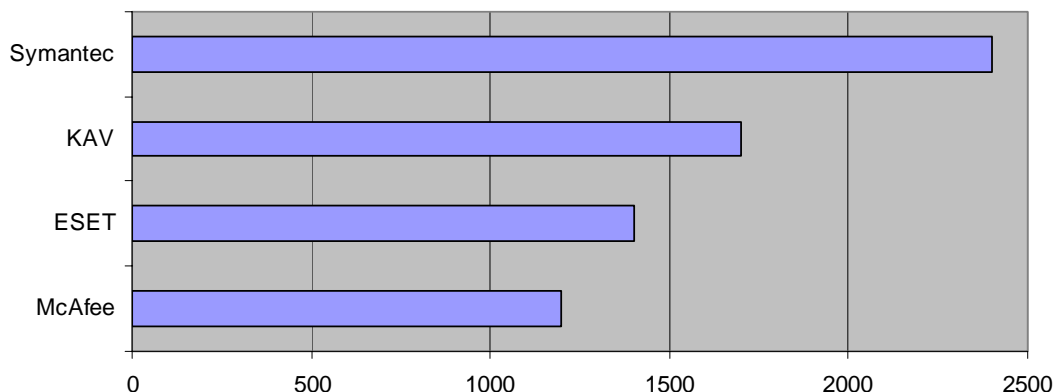
⁵ The average download size of full signature databases of the new product line of McAfee (which will be released in August) will have a size of about 5 MB.

5. Average number of new signatures in updates

The average number of new signatures in updates varies from week to week and between products. Sometimes some Anti-Virus companies release very large signature updates on one day containing a rollup of signatures (for example lower-risk threats, older malware, samples from collections, etc.) for other malware that has not been considered urgent or required to include immediately in the usual daily updates. It is also more efficient to release such signatures at one time in a single larger update, in order to maximize the QA work, improving reliability and avoiding false positives due to more extensive testing before releasing. Some additions⁶ of samples collections submitted by users or from other Anti-Virus companies are handled in this way, and can give rise to an update containing several hundreds of signatures. These usually occur in the first half of the month, with relative high spikes. The addition of samples coming from collections depends on vendor schedules, priorities, resources, etc. The numbers below are observed average numbers of signatures released per week, rounded to whole hundreds:

Symantec: around 2400 at week
KAV: around 1700 at week
ESET: around 1300 at week
McAfee: around 1200 at week

Average number of signatures released per week



Symantec seems to release most (of the tested group) new/updated signatures per week.

Products with higher proactive on-demand detection rates (e.g. due to heuristics and/or good generic signatures, packer support, etc.) may not need to release as many signatures each week.

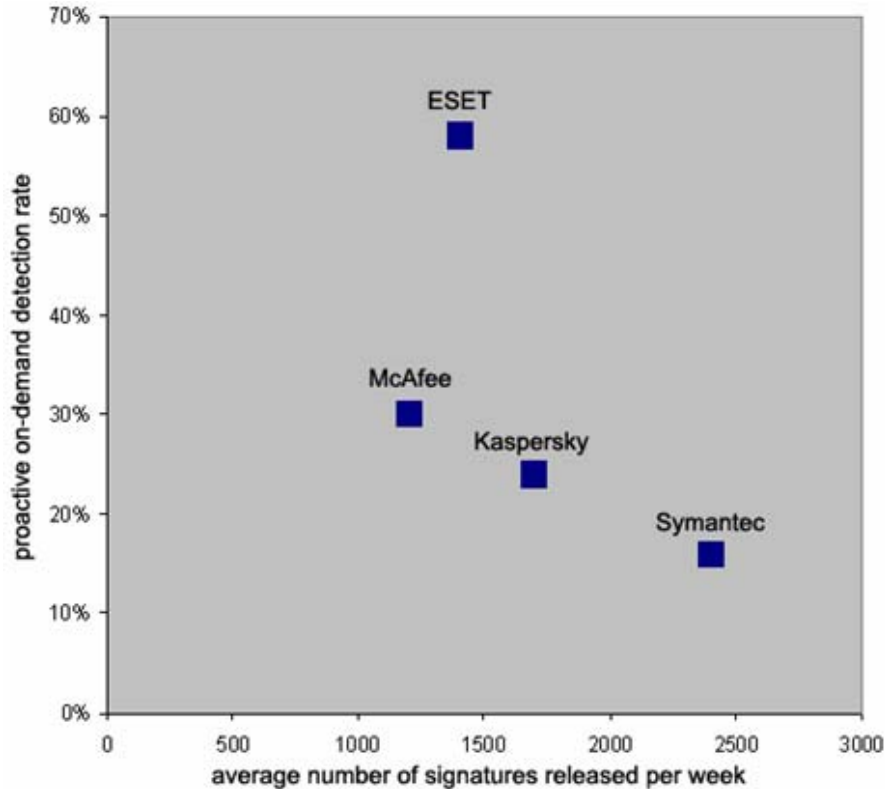
Important note: these numbers only tell how many signatures are usually added during one week, but it does not indicate how many pieces of malware may be detected by those signatures (a generic signature may only be one signature, but may detect thousands of variants of a malware family). These numbers will fluctuate much every week, but the proportions usually remain (surprisingly) more or less consistent.

It is important to remember that those four products are all top Anti-Virus products with ADVANCED+ rating in our on-demand tests. Products with lower detection rates or which have still many malware

⁶ Often done automatically.

to add in their queue, poor packer support or weak heuristics etc., may need to release a higher number of signatures at week to try to win the fight against the malware.

The graph below shows for those four products the average number of signatures released and the proactive on-demand detection rates reached in the last retrospective test of May 2006.



ESET releases a relatively high number of signatures considering that they have a very high proactive on-demand detection rate.

The number of total virus signatures shown in some products does not contain information about the detection quality, how the numbers were counted nor how many malware a product is able to detect, etc. Some products may claim to have 500.000 virus signatures, while some other products claim to have only 70.000 virus signatures - but it is quite possible that the program with only 70.000 virus records can detect more than the other product, because they count in a different way or because they have good generic detection or packer/compression support. Depending how the numbers are interpreted, lower numbers of virus signatures may even be better than high numbers. To get an idea of the total virus record growth over the years, here is an overview of average number of signatures in the period from July 1998 to July 2006, based on some Anti-Virus products (numbers rounded):

July 1998: ~ 31000 virus records
July 1999: ~ 37000 virus records (+ 8000 compared to previous year)
July 2000: ~ 47000 virus records (+10000 compared to previous year)
July 2001: ~ 54000 virus records (+ 7000 compared to previous year)
July 2002: ~ 62000 virus records (+ 8000 compared to previous year)
July 2003: ~ 79000 virus records (+17000 compared to previous year)
July 2004: ~105000 virus records (+26000 compared to previous year)
July 2005: ~152000 virus records (+47000 compared to previous year)
July 2006: ~232000 virus records (+80000 compared to previous year)

Since 2002, the numbers of newly added virus records more or less doubled every year.

6. Copyright and Disclaimer

This publication is Copyright (c) 2006 by AV-Comparatives. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of Andreas Clementi, prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

Andreas Clementi, AV-Comparatives (August 2006)