Kaspersky Whitelisting Database Test

A test commissioned by Kaspersky Lab and performed by AV-Test GmbH

Date of the report: February 14th, 2013, last update: April 4th, 2013

Summary

During November 2012 and January 2013, AV-Test performed a test of Kaspersky Whitelisting Database in order to determine the coverage and quality of this service. In total five different test cases have been applied:

- Test Case 01 - Database Coverage
- Test Case 02 - Database Quality
- Test Case 03 - Database Speed
- Test Case 04 - Database False Rate
- Test Case 05 - Default Deny Mode

With these individual tests it is ensured that both the quality as well as the quantity of the service and the underlying data is verified.

AV-TEST used data from its own clean file project which includes over 10 Terabyte of data with over 20 million files. In order to build the set AV-TEST downloads software from popular download portals as well as from vendors directly, installs them and captures all created files together with their metadata.

Four different data sets extracted from the full AV-TEST clean file set were used to perform the test:

- **Daily Set** – A set of files that have been tested the same day they have been discovered by AV-TEST, both installers as well as installed files
- **Historic Set** – A set of files that have been discovered by AV-TEST before the start of this test, both installers as well as installed files
- **Installer Set** – A set of files that have been discovered by AV-TEST before the start of this test, just installers, no installed files
- **Windows Set** – A set of files from standard Windows installations

The Kaspersky Whitelisting Database is a part of Kaspersky Security Network (KSN) infrastructure which is fully integrated into their consumer and corporate products in order to provide a real-time access to a huge amount of world-wide collected information and expertise for every single customer.

The results of the test indicate that Kaspersky has a very good coverage of files that have been known to AV-TEST prior to the test (Historic Set and Installer Set) with over 91% of the files known to Kaspersky at the time of the test. The new files (Daily Set) that have been tested on the day of their discovery were already known to Kaspersky in the amount of 50%. Finally about 98% of the standard Windows files were known to the Kaspersky Whitelist at the time of the test. When only looking at the relevant executables and libraries 99,9% of the files were known.

Methodology

Please refer to the Appendix for a detailed description of the methodology.

Test Results

The following table lists the number of files submitted to the Whitelisting service and the number of files that were known to the Whitelist at the time of the test.

File Set	Files Submitted	Files known	Percentage of known files
Daily Set	253.191	125.427	49,54%
Historic Set	4.686.589	4.270.647	91,12%
Installer Set	231.598	208.600	90,07%
Windows Set	65.470	64.154	97,99%

As mentioned before, files that have been published before the start of the test are covered very well in the Kaspersky Whitelist and even new files that were published during the test are covered good. Furthermore, not all unknown files are really a problem. It is not necessary for a Whitelisting service to cover text files or media files, so these could account for some of the unknown files. On the other hand it is important to cover executable files and program libraries as these are the files that need to be controlled. Similar observations can be mode for different categories, markets of regions.

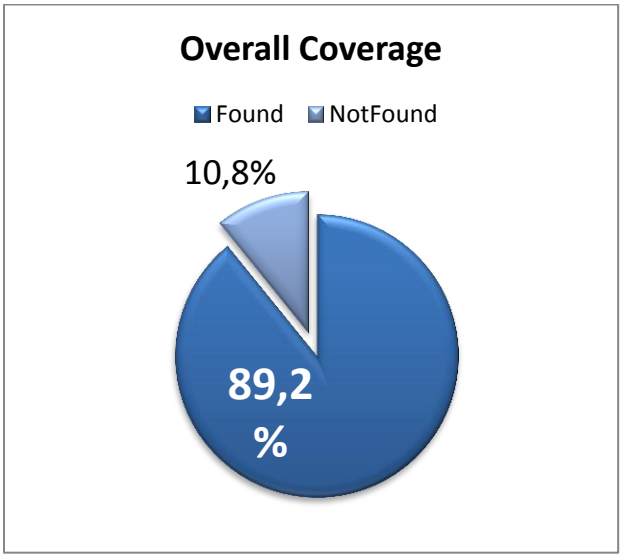
The full details of all test results are shown in the appendix. Below are the main findings from each Test Case.

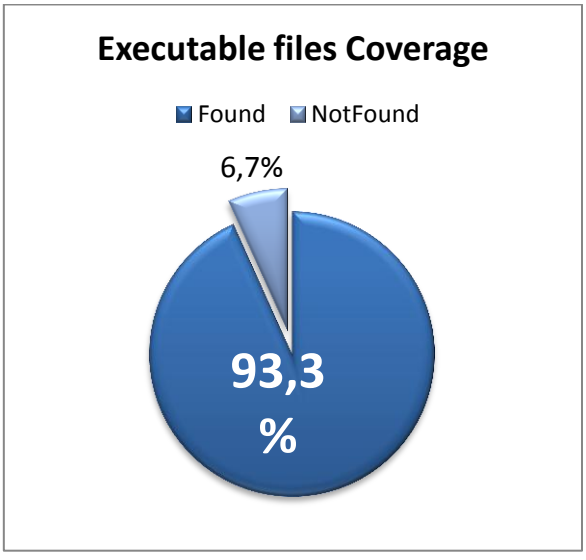
Test Case 01 - Database Coverage

This test aims to verify the coverage of the database particular areas of software as well as different application types. There are further categories that will be checked:

- The % coverage ratio of files associated with the consumer market
- The % coverage ratio of files associated with the corporate market
- The % coverage ratio of files associated with System, Office, Tools and Games application types
- The % coverage ratio of files associated with different file format types

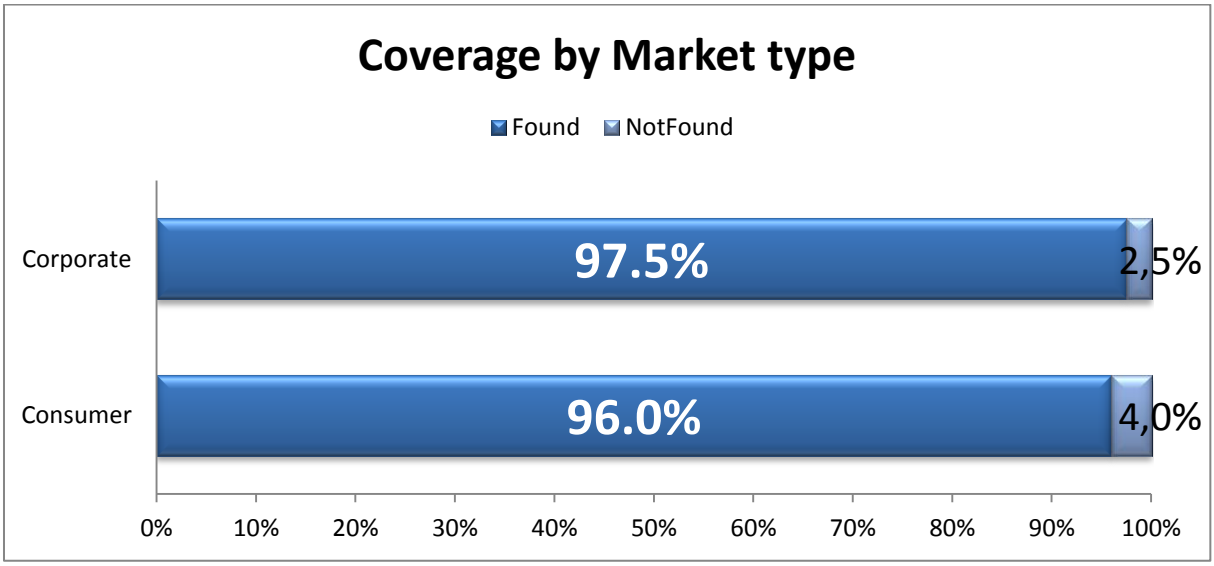
The charts below indicate overall coverage as well as coverage of executable files subset.



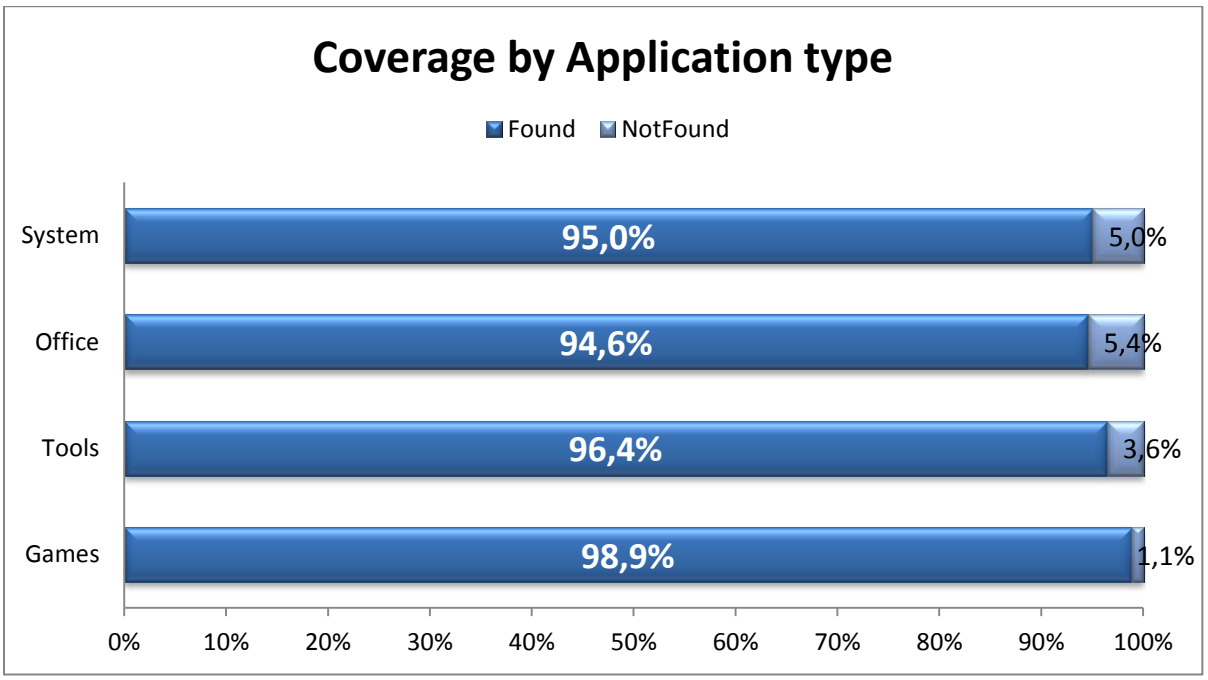


The next chart shows coverage of both corporate and consumer subsets of software that was tested on purpose to measure abilities of Whiteliting service to identify software specific for each group.

The corporate subset contains software such as Acronis® Backup and Security 2010, AutoCAD, Microsoft SQL Server Analysis Services, Crystal Reports 11, Microsoft® Office and so on. Instead, consumer subset was compiled with software such as Adobe Acrobat Reader, Apple iTunes, BitTorrent, DivX Player, Windows Movie Maker and other.



Because there is no clear separation between corporate and consumer usage of the most common software, measurements of coverage was made in additional dimension. A tested subset of applications was divided into four common groups named System, Office, Tools and Games. The chart below represent coverage for each of four types of application stated above.

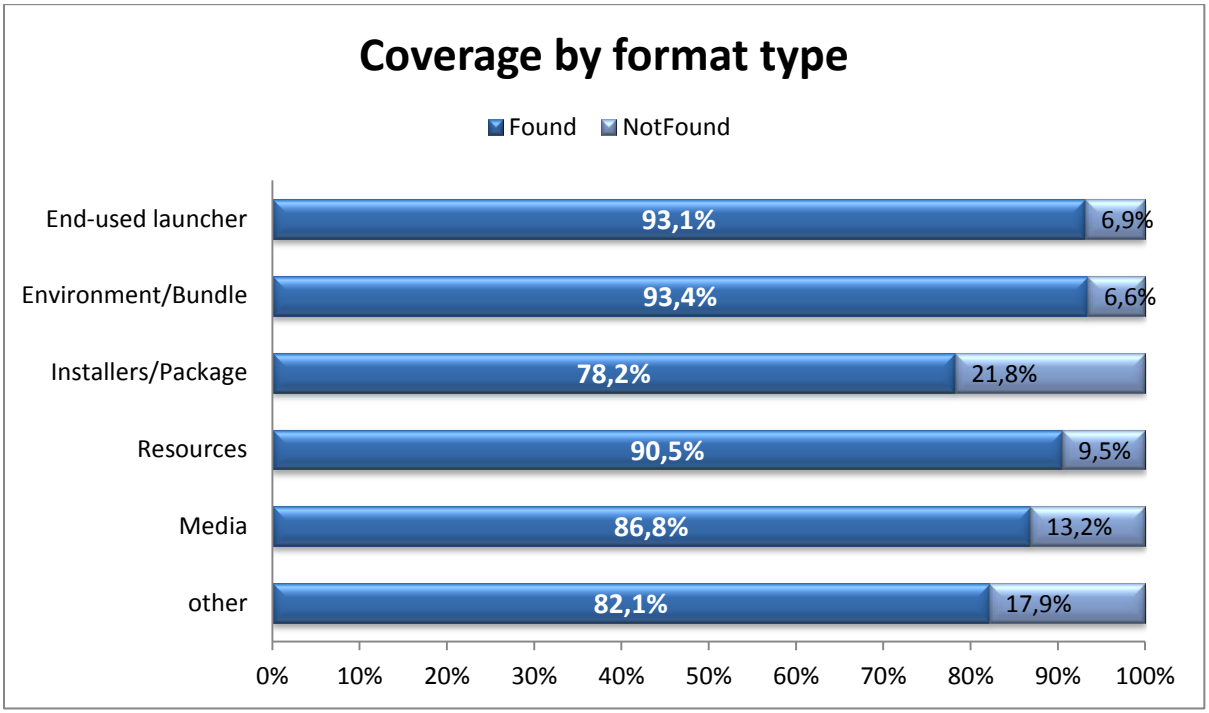


The **System** subset mostly consist of Microsoft Windows system's files and 3rd party drivers produced by 3Com, Canon, NVIDIA and others.

The **Office** subset consists of whole Microsoft Office suite, Crystal Office, BillQuick®, NetMeeting and others.

The **Tools** subset contains entertainment, video and audio codes, development tools, backup and recovery software that is simply neither Office software nor Games. For example, the Tools subset was compiled with Acronis True Image, ApexSQL, CyberLink PowerDVD, Microsoft Visual Studio, Nero Burning ROM and many others.

As well as corporate and consumer groups shares different application's types, the applications themselves are consist of files which vary by its format type. It is obvious that injection or substitution of any of those files by malware may lead to significant changes in application behavior. For this reason, it is valuable from Whitelisting perspective to ensure integrity of all application's files and not only end-used launchers. The chart below represents results for common file types.



Test Case 02 - Database Quality

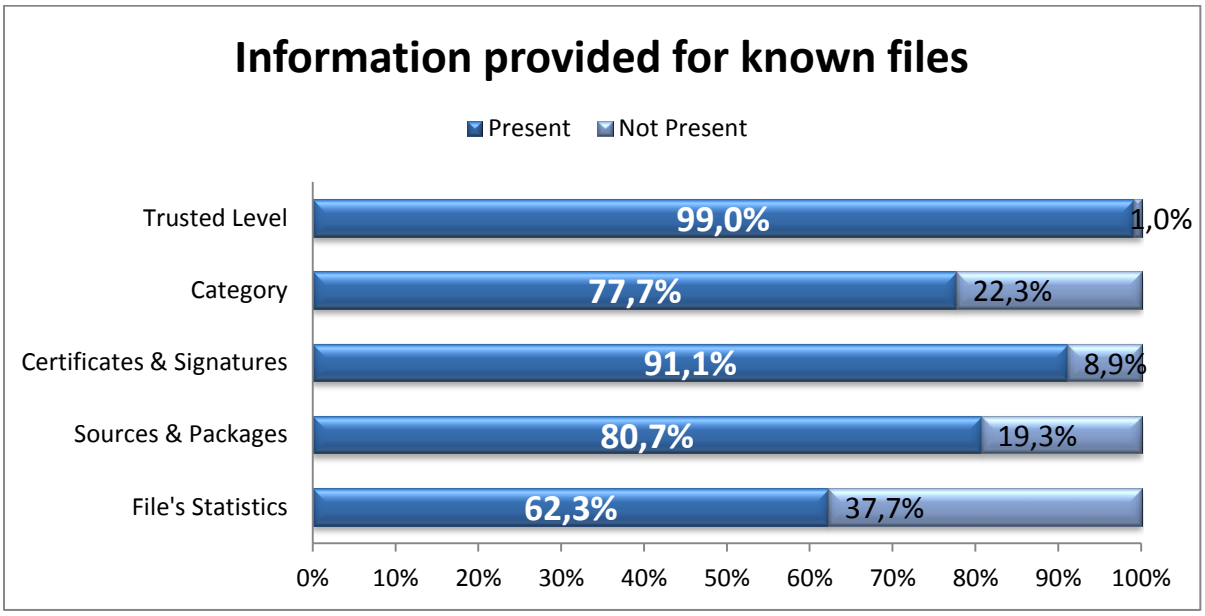
While quantitative coverage results are indicates "How many" files were known for Whitelisting service, the qualitative results of "What was known" are important as well. The chart below represents results of how much valuable information provided for known files[1].

The Trusted Level results represent expert knowledge of whenever particular file is a clean one or malware. Instead, the Category part results represent information of application's category assigned by Kaspersky for particular clean file. The set of categories defined by Kaspersky is slight different to

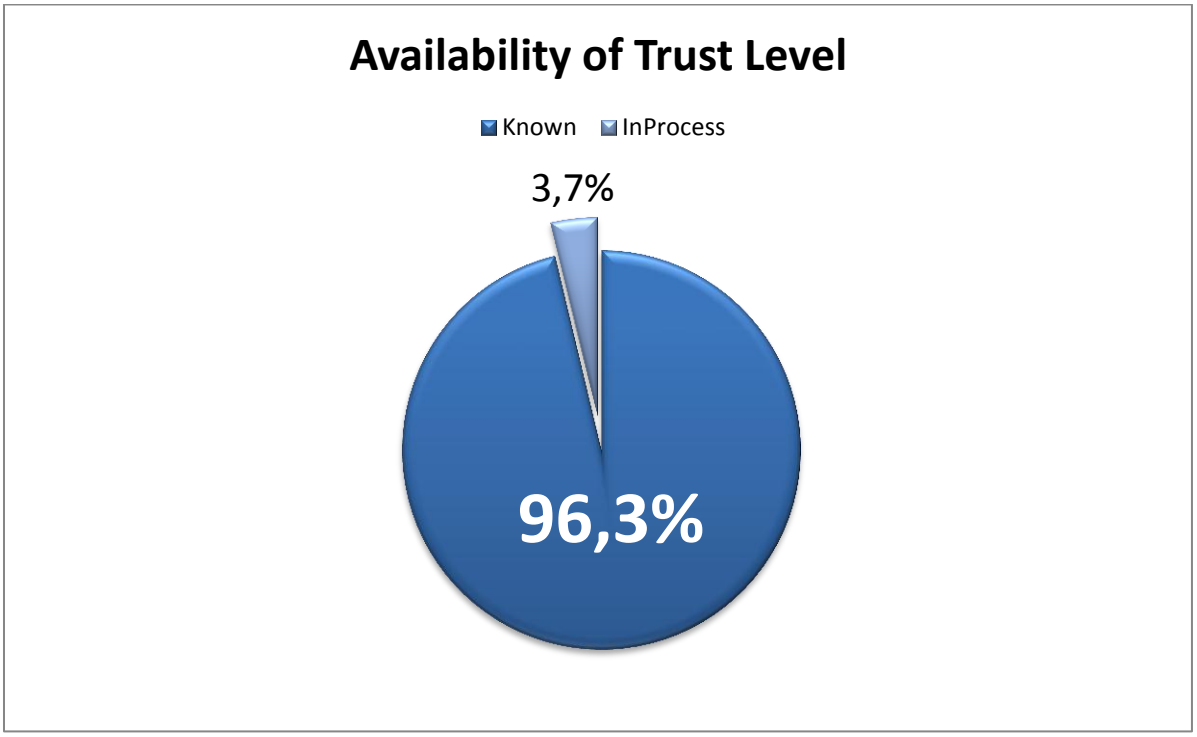
[1] To measure the % coverage ratio of presented information the full subset of files that was known for Whitelisting service at the time of the test was selected as expected count. However, the subset of files that was used to measure coverage ratio for Certificates & Signatures part was reduced to subset of signed files, which signatures was verified locally. Similar to Category part the subset of files was reduced to those which has both valid digital signature and FileVersionInfo structure, because it is a current limitation of Kaspersky's categorization process. The goal of such measurements is to compare the ratio of what was known against what should be known.

what was presented above as Application Types in that Kaspersky has defined 16 high level and 95 leaf categories.

The Certificates And Signatures results represent knowledge of digital signatures and certificated that exists for a files. The Sources and Packages part provide information about file's containers and links from which both a files or its container was downloaded. The last part named File's Statistics represent information of file's popularity around the globe, count of participant of Kaspersky's Security Network program who decide to trust or not to trust a particular file.



The important note about Trusted Level is that its' value may be in one of two states: "known" which means that the final decision was already made and "In process" which means that the final decision is still in question. The chart below represents distribution of 99% of available Trusted Level by defined states.



Test Case 03 – Database Speed

This test aimed to examine the responsiveness of the whitelisting database using the returning of requests from queries made against the database. Specifically, this testing considered:

• The time taken for the Whitelist database to respond to verification requests against individual checksums.
• The time required for the addition of a previously unknown clean file into the whitelist after it was submitted to Kaspersky for verification.
• The time required for Kaspersky to respond to the reporting of, and take appropriate actions upon, a reported false positive result.

The below table shows the average response time required for different sizes of hash chunks that have been submitted to the database.

Chunk Size	Time taken per Hash
Small (below 250 hashes)	1,121s
Medium (over 250 and below 500)	0,565s
Big (over 2.000 hashes)	0,558s
Very big (over 25.000 hashes)	0,145s

Results show that the database responds very fast, especially when sending big amounts of hashes. This is more than sufficient to be used in a normal working environment.

Test Case 04 - Database False Rate

This test aimed to examine the trustworthiness or "correctness" of the database. The testing was specifically focused on the following areas:

• Number of False Negatives i.e. those files classified as genuine by the solution but in fact malicious, based against a set of samples drawn from AV-TEST's collections of recent malware.
• Number of False Positives i.e. those files classified by the solution to be malicious, but in fact genuine.
• Availability of the database in terms of being able to respond to a file lookup request, irrespective of the result of the lookup.

	False Positives	False Negatives
Result	0,00%	0,00%

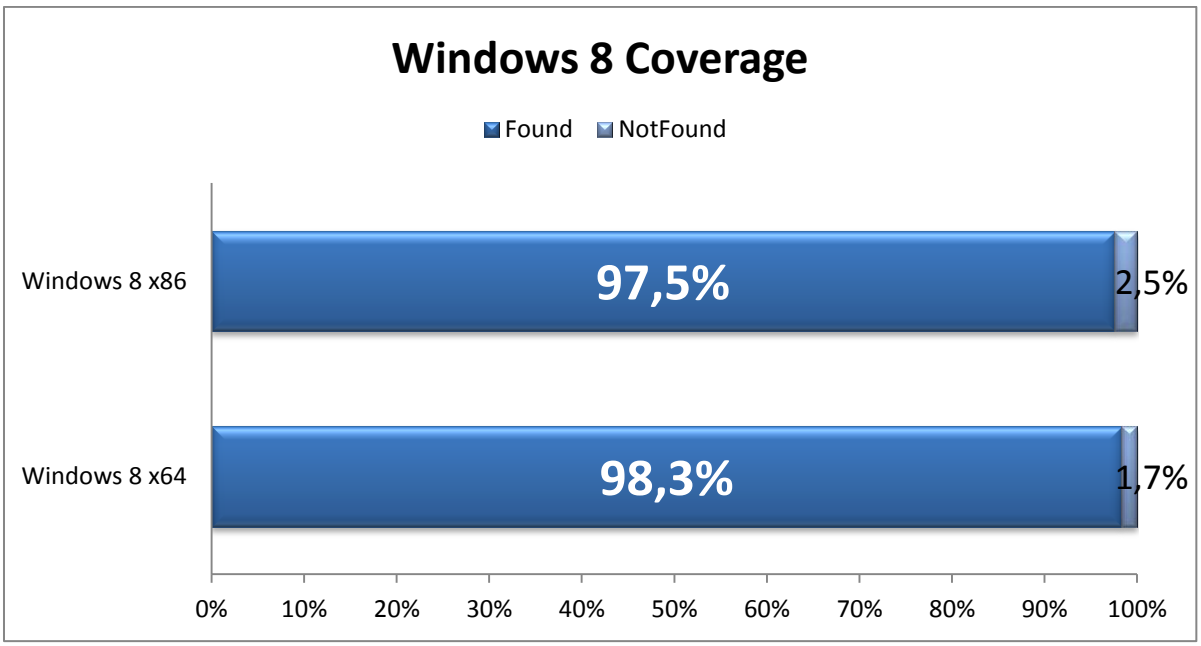
No false positives or false negatives were noticed during the test.

Test Case 05 – Default Deny Mode

One of the purpose of Whitelisting service is to support the Default Deny mode of modern Application Control in which only known trusted applications will be allow to execute and everything else will be block by default. This is a vital requirement for Whitelisting service to be able to identify critical system's files to support Default Deny mode. The last chart represents quantitative coverage of modern Windows 8 files for both 32-bit and 64-bit platforms.

When looking at the results of Test Case 01 it is obvious that coverage of Windows files is very good, the details are shown in the following table.

Even though the coverage results are less than a 100%, the remainder part consists of non-executable binaries, images and other similar files which are not affecting the Default Deny mode.



Appendix

The following part describes the AV-TEST Whitelist Testing methodology for a test of the Kaspersky Whitelisting services. The first part of this document describes the test collection that will be used to carry out the test. The second part of the document describes the actual test cases and the used methodology.

Test Collection

AV-TEST downloads hundreds of applications for the Windows operating system every day from many popular download sites (e.g. cnet.com, zdnet.com) and from the vendors directly (e.g. adobe.com, java.com, ibm.com). All in all over 300 different sources are covered. We then actually install the downloaded programs. All the downloaded and installed files are stored as well as detailed information about these files (Productname, Productversion, Filename and Path, Size, Download URL, ...). So we always know which file belongs to which product, where did we download it from and how old is it.

On average we add around 45,000 new, unique files per day with a total size of 18-20 GB. Currently we have over 10 TB of data in more than 20 million unique files in the clean file collection (historic sec). All types of files are included in this collection, it is not limited to PE files. Languages covered are English, German, French and Spanish.

Tests will be carried out on both the historic set as well as the daily added new files over a certain period of time.

Test Methodology

Test Case 01 - Database Coverage (TC01)

TEST OBJECTIVE

This test aims to verify the coverage of the database, both for specific regions, and also for particular areas of software, such as consumer or corporate. There are further categories that will be checked:

- The % coverage ratio of files associated with specific regions/languages
- The % coverage ratio of files associated with the consumer market
- The % coverage ratio of files associated with the corporate market
- Popularity, Platform, Category, File Type and Reputation

TEST DESCRIPTION

AV-TEST will check all new files over a period of two weeks as well as the historic set against the Kaspersky database and will later extract numbers for the different regions, markets and other categories. No pre-sorting of the collection is done.

The collection is known to include software in English, German, French and Spanish language. Furthermore it is known that consumer software as well as corporate software is included.

The returned outputs against each hash is saved to a combined log file for analysis, and various measurements will also be taken, such as the time taken to perform the lookup, and start/finish times for the process. This allows to perform the analysis of the results after the test has been finished.

Test Case 02 - Database Quality (TC02)

TEST OBJECTIVE

This test aimed at verifying the structure and value of metainformation that is available in the database about each file from the test collection. The result also aimed to reflect the usefulness of any associated

information for analytical purposes according to a predetermined weighting system agreed in advance with Kaspersky. Each metainformation parameter was assigned a weight, and thus a metric based approach to evaluate the quality of the Whitelisting database could be assessed based upon the composition and perceived importance of each parameter.

TEST DESCRIPTION

Using the output generated by TC01, the hashes could be determined for which data had been returned. Following this, the data on a per hash basis can be extracted and it can be checked how many of a predetermined set of data flags were returned. The specific data sets, or flags, that were used in this test were then awarded a weighted value based on their level of importance, according to appropriate weighting system agreed in advance with Kaspersky. This allowed for a weighted measure (expressed as a percentage score) of data completeness to be awarded to each returned hash so that a judgment on the value and quality of the data could be determined.

Test Case 03 - Database Speed (TC03)

TEST OBJECTIVE

This test aimed to examine the responsiveness of the whitelisting database using the returning of requests from queries made against the database. Specifically, this testing considered:

- The time taken for the Whitelist database to respond to verification requests against individual checksums.
- The time required for the addition of a previously unknown clean file into the whitelist after it was submitted to Kaspersky for verification.
- The time required for Kaspersky to respond to the reporting of, and take appropriate actions upon, a reported false positive result.

TEST DESCRIPTION

The testing of database speed again bases on the data from TC01 which provides information about how long a request takes to answer. Different chunk sizes (between 10 and 1000 hashes per request) will be used.

The timings were subsequently analysed in order to determine the length of average time recorded for processing each of these groupings, as well as to ascertain the average time per single hash when processed in these groups.

Test Case 04 - Database False Rate (TC04)

TEST OBJECTIVE

This test aimed to examine the trustworthiness or “correctness” of the database. The testing was specifically focused on the following areas:

- Number of False Negatives i.e. those files classified as genuine by the solution but in fact malicious, based against a set of samples drawn from AV-TEST’s collections of recent malware.
- Number of False Positives i.e. those files classified by the solution to be malicious, but in fact genuine.
- Availability of the database in terms of being able to respond to a file lookup request, irrespective of the result of the lookup.

TEST DESCRIPTION

A list of 20,000 hashes that are associated with files contained within AV-TEST’s malware collections was compiled, with the criteria for this being that these had been collected just prior to the start of the test. Using the methodology that was employed for TC01, each of these hashes was then parsed through the application against the database, and the subsequent returns and outputs were recorded.
Subsequent to this, further analysis was also conducted against the output taken from TC01 in order to determine how many of the known-good files were reported by the whitelist database as infected.

Test Case 05 – Default Deny Mode (TC05)

TEST OBJECTIVE

This test aimed to determine whether the whitelisting database contained the necessary information which is necessary for running a “default deny mode” when using Kaspersky’s Endpoint product (which utilises Kaspersky Whitelisting database). Note that the database only was tested, and not the implementation Default Deny mode is, in this case, defined as a restricted mode of PC operation when everything is blocked except for certain particular pieces software which are necessary for the basic operation and general functionality of a given system – in other words the Operating System and critical drivers.

TEST DESCRIPTION

The checksums of various example operating systems as per the list below were submitted to the database using the tools and methodologies as in TC01, and the results returned were recorded as to whether they were included in the default deny list or not:

- Windows 8 Pro (32 bit)
- Windows 8 Pro (64 bit)