westcoast labs

Commercial in Confidence

Test Report December 2011

Kaspersky Whitelist Database

Kaspersky Whitelisting - Test Report

WCL Corporate Offices and Test Facilities

USA Headquarters and Test Facility

West Coast Labs, 16842 Von Karman Avenue, Suite 125, Irvine, CA 92606, U.S.A. Tel: +1 (949) 870 3250, Fax: +1 (949) 251 1586

European Headquarters and Test Facility

West Coast Labs, Unit 9 Oak Tree Court, Mulberry Drive, Cardiff Gate Business Park, Cardiff, CF23 8RS, UK.
Tel: +44 (0) 29 2054 8400, Fax: +44 (0) 29 2054 8401

Asia Headquarters and Test Facility

West Coast Labs, A2/9 Lower Ground Floor, Safdarjung Enclave, Main Africa Avenue Road, New Delhi 110 029, India. Tel: +91 (0) 11 4602 0622, Fax: +91 (0) 11 4602 0633

Date: 14th December 2011 **Version:** 1.0

Authors: Richard Thomas, Mark Thomas, Matt Garrad, Chris Thomas

Kaspersky Whitelisting - Test Report

Contents

Kaspersky Whitelisting - Test Report

Introduction

Following discussions between representatives of Kaspersky Lab (hereafter referred to as Kaspersky) and West Coast Labs (hereafter referred to as WCL) a test outline was constructed for, and agreed with, Kaspersky related to the testing of the database used by Kaspersky to provide their whitelisting technologies.

This document forms the report of those tests carried out against the Whitelist database, looking at several aspects of the solution including database coverage, fullness, speed of access, false positive/negative rates, default deny capabilities and additional services that Kaspersky has made available to partners and prospective partners.

It is important to note that the testing conducted as part of this framework, and which is summarised in this report does not verify the operation of Kaspersky's whitelisting technology itself, or any implementations of the technology, but only assesses the underlying database.

The technical lookup portions of this test were conducted using a web service–based application, provided by Kaspersky to WCL, which allowed MD5 checksums (a method of file identification used for data integrity checking) of files to be passed to the service as a parameter, with the end result being the return of records from the database related to each specific checksum that showed the appropriate metainformation.

The rest of this document details the high level test objectives, the test environment that was used, the composition of the test collection, individual test cases, and their associated methodology, test results, and finally a conclusion drawing together all of the tests and processes.

Kaspersky Whitelisting - Test Report

Competitive vendors

At Kaspersky's request, WCL approached several other vendors in the whitelisting database space to request their involvement in a comparative test based around the methodologies, collections, and analysis as detailed below.

Each vendor was given the opportunity to view their own results against each of the tests and categories that were appropriate to them, and had the option to request anonymisation within this final report.

All three competitive vendors politely declined to take part and, given that this sort of testing requires direct access into a vendor's databases for accurate results, the matter could unfortunately not be progressed any further.

The vendors approached were:

- Harris Corporation (formerly SignaCert)
- Lumension
- Bit9

Kaspersky Whitelisting - Test Report

Test Objectives

The overall objective of this testing programme was to determine the effectiveness of the whitelist database by conducting a series of test cases, each designed to assess a specific area of the database and associated processes. Results are provided in the following areas, along with discussion:

Test Case 01 - Database Coverage (TC01)

This test case aimed to verify the coverage of the database in terms of consumer and corporate specific software, as well as region specific software.

Test Case 02 – Database Fullness (TC02)

This test case aimed to determine the quality and quantity of information and metainformation included within the database for the MD5 checksum (hereafter referred to as MD5) associated with each of the files.

Test Case 03 – Database Speed (TC03)

The aim of this test is to examine the responsiveness of the Whitelisting database when returning data for a given MD5 or groups of MD5s.

Test Case 04 – Database False Rate (TC04)

This test case will examine the trustworthiness or "correctness" of the database when returning metainformation for both known-bad and known-good MD5s.

Test Case 05 – Additional Services (TC05)

This test case will examine and report upon the added functionality that is extended to partners of Kaspersky.

Test Case 06 – Default Deny (TC06)

This test case will examine whether the database contains information that is necessary for running a "default deny mode".

Kaspersky Whitelisting - Test Report

Test Network

Testing was carried out at WCL's European Headquarters, located in Cardiff, UK.

The Ubuntu variant of the Linux OS was installed to a number of machines located within the lab environment. Once installation of the OS was complete, the Oracle VirtualBox application was installed on each of the machines and configured to run an instance of Windows XP patched to Service Pack 3.

A Windows-based application, provided by Kaspersky Lab to enable direct access to their whitelist database, was then placed on the root of each Windows XP virtual machine.

The test collection of MD5 checksums was then parsed through these applications, with the web traffic being transported over Cisco switches and routers and a live Internet connection as provided by a UK-based ISP.

Kaspersky Whitelisting - Test Report

Test Collection

The test collection prepared by WCL consisted of a series of MD5 checksums that were taken of Windows-based software. This software was sourced from different locations and covered a number of different geographical areas. The number of checksums in the overall collection, after deduplication, was over 843,000 and included all file types related to the applications being tested, not just "Portable Executable" types.

The software sources used for the collection were as follows:

- Software distributed within WCL's usual office and testing environments, except where this was in breach of any existing NDAs or legal obligations.
- Software distributed within WCL's parent company Haymarket Media Group, adhering to the same legal restrictions as above.
- Commonly used software from Adobe (such as Acrobat Reader) and from Microsoft, including base versions of the Microsoft Operating Systems Windows XP, Windows Vista, and Windows 7, along with various Operating System patches from Microsoft.
- Extracts from the Kaspersky Security Network of popular software among Kaspersky users (a separate and distinct entity from the whitelisting database being tested). Total number of MD5s was not more than 6% of total collection.
- Software acquired prior to the testing by WCL. This covered:
    - The top 100 popular downloads from sites such as tucows, sourceforge, download.com, brothersoft and softpedia in the month immediately before the testing commenced.
    - Video and audio codecs.
    - Top games in the week prior to the commencement of testing purchased from an "over the counter" retailer local to WCL in the UK. This list was constructed from an online retailer (Amazon), a specialist

Kaspersky Whitelisting - Test Report

Test Collections

online and high street games retailer (game.co.uk), and a UK supermarket (Tesco).

- Digital media software and system drivers such as audio, network, graphics, and motherboard.
- Localised downloads and software from Americas, Europe Eastern, Europe Western, APAC, and Middle East and Africa regions.

- Malware sourced from WCL's collections just prior to the commencement of testing, representing 20,000 distinct samples, including malware captured in WCL's global honeypot network.

WCL also approached some of Haymarket Media group's partners and licensees and requested that they provide (and purchase, where appropriate) software localised for their particular market, and links from which users in their region regularly download software.

Kaspersky Whitelisting - Test Report

Test Methodology

Test Case 01 - Database Coverage (TC01)

TEST OBJECTIVE

This test aims to verify the coverage of the database, both for specific geographic regions, and also for particular areas of software, such as consumer or corporate.

- The % coverage ratio of files associated with specific regions/countries (Eastern Europe, Western Europe, Americas, Middle East and Africa, APAC)
- The % coverage ratio of files associated with the consumer market
- The % coverage ratio of files associated with the corporate market

TEST DESCRIPTION

The combined list of MD5s from WCL's central storage database that housed the test collection was exported into a number of flat text files containing 50,000 MD5s each. They were further broken down into region and then by corporate and consumer groupings. The regions used in the test were as follows:

- Americas
- Western Europe
- Eastern Europe
- Middle-East & Africa
- Asia Pacific

Each of these flat-text files was then parsed against the whitelist database using the interface to the live database supplied by Kaspersky. The returned outputs against each MD5 were saved to a combined log file for analysis, and various

Kaspersky Whitelisting - Test Report

Test Methodology

measurements were also taken, such as the time taken to perform the lookup, and start/finish times for the process. To further aid in this, network traffic captures were taken to provide later verification.

Using various SQL queries, along with in-house analysis tools and scripts, engineers then calculated the total number of MD5s for which data was returned by the whitelist database.

Test Case 02 - Database Fullness (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, scripts were developed that would compile a list of all those MD5s for which data had been returned. Following this, the scripts then extracted all of the data on a per MD5 basis and made a record of how many, if any, 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

Test Methodology

to each returned MD5 so that a judgement on the value and quality of the data could be determined. Specific details of the weightings are detailed in Appendix A.

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

Testing of the database speed was conducted utilising several separate stages. The first considered the independent verification of the lookup time as reported by the database/lookup application. This consisted of a manual verification conducted by a WCL engineer, along with an automatic verification conducted by the scripts that monitored the start and finish times of the associated windows applications as the collections were being parsed. Network traffic captures were also utilised to provide further verification of the timings.

Kaspersky Whitelisting - Test Report

Test Methodology

Following this, the full collections were reprocessed through the database, using the methodology as stated for TC01. This time, however, the test sets were split into groups of both 10,000 and 1,000 MD5s.

The timings for these 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 MD5 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 focussed 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 WCL'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 MD5s that are associated with files contained within WCL's malware collections was compiled, with the criteria for this being that these had been collected just prior to the start of the test. These included samples taken from WCL's

Kaspersky Whitelisting - Test Report

Test Methodology

global honeypot network, and so these files were live and in the wild. Using the methodology that was employed for TC01, each of these MD5s 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 – Additional Services (TC05)

TEST OBJECTIVE

This case aimed to examine and report upon the added functionality that is extended to partners of Kaspersky and corporate consumers.

- Kaspersky whitelisting service (http://www.kaspersky.com/partners/whitelist)
- Kaspersky Trusted service (http://trusted.kaspersky.com)
- Also available on http://www.whitelist.kaspersky.com

The examination of the whitelisting service involved looking at the means by which a partner company can submit upcoming software releases for inclusion into the whitelist, including going through the process itself.

Investigations of the Kaspersky Trusted service considered the process that allows for the provision of a Kaspersky approval logo on a software download page, alongside information relating to the file.

TEST DESCRIPTION

In order to test the Kaspersky Whitelisting Service, WCL created a series of new files

Kaspersky Whitelisting - Test Report

Test Methodology

that were previously unknown to Kaspersky Lab or to their Whitelisting database. Using account information specific to WCL and provided by Kaspersky Lab, each of these files was uploaded to the Whitelisting service FTP server and the upload time noted.

A series of in-house scripts were simultaneously started that would continuously check the database once every 10 seconds, this having been agreed as a reasonable timeframe. These scripts were configured to look for the newly added information related the MD5s of the files that had been uploaded. The timestamp for when this information appeared was recorded on a per file basis.

A subsequent test was then performed that measured the time it takes for Kaspersky Lab to reclassify a file's status once they have been contacted by a customer with a query. To do this, a specific given email address was contacted with a request to reclassify those same files from "clean" to "suspicious". The same scripts used in the earlier test were once again run and configured to record the timestamp at which the classification was seen to have altered.

A validation test was also performed for the use of the Kaspersky Trusted logo within the Kaspersky Trusted service. Using the MD5 information for one of the files supplied earlier in this test case, a web page was constructed and the HTML code provided was included, with the appropriate MD5 and account code information. It was then visually verified that both the Trusted logo and respective Trusted service page were available.

Finally, a series of questionnaires were sent out to existing customers of the service. Each questionnaire was designed to gain an insight as to the overall user experience of the service.

Kaspersky Whitelisting - Test Report

Test Methodology

Test Case 06 – Default Deny Mode (TC06)

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 XP Service Pack 3 (32 bit)
- Windows 7 Embedded Edition (32 bit)
- Windows 7 Home Edition (64 bit)
- Windows 7 Professional (32 bit)
- Windows 7 Enterprise (32-bit)
- Windows 7 Enterprise (64-bit)

Kaspersky Whitelisting - Test Report

Test Results

This section contains the results for all testing conducted as part of this report. Tests are broken down according to each of the Test Cases outlined above, and detailed as follows:

- TC01 - Database Coverage
- TC02 - Database Fullness or quality of data
- TC03 - Database Speed
- TC04 - Database False Rate
- TC05 - Additional Service
- TC06 – Default Deny mode support

Kaspersky Whitelisting - Test Report

Test Results TC01 - Database Coverage

Coverage by Regions and type of software

Region	Consumer Software		
	Files requested	Files detected	Known (%)
Americas	131,355	127,313	**96.92%**
Western Europe	188,860	169,806	**89.91%**
Eastern Europe	14,116	12,428	**88.04%**
Middle East & Africa	5,010	4,414	**88.10%**
Asia & Pacific	41,547	38,804	**93.40%**
All Regions	380,888	352,765	**92.62%**

Table 1.0 – Consumer software coverage by region

Region	Corporate Software		
	Files requested	Files detected	Known (%)
Americas	184,487	180,997	**98.11%**
Western Europe	265,685	243,751	**91.74%**
Eastern Europe	9,935	9,573	**96.36%**
Middle East & Africa	489	419	**85.69%**
Asia & Pacific	2,087	2,072	**99.28%**
All Regions	462,683	436,812	**94.41%**

Table 1.1 – Corporate software coverage by region

Region	Consumer + Corporate Software		
	Files requested	Files detected	Known (%)
Americas	315,842	308,310	**97.62%**
Western Europe	454,545	413,557	**90.98%**
Eastern Europe	24,051	22,001	**91.48%**
Middle East & Africa	5,499	4,833	**87.89%**
Asia & Pacific	43,634	40,876	**93.68%**
All Regions	843,571	789,577	**93.60%**

Table 1.2 – Corporate and Consumer software coverage by region

Kaspersky Whitelisting - Test Report

Test Results TC01 - Database Coverage

The below graphs show overall coverage statistics by region (Figure 1.0) and overall coverage by market segment (Figure 1.1)

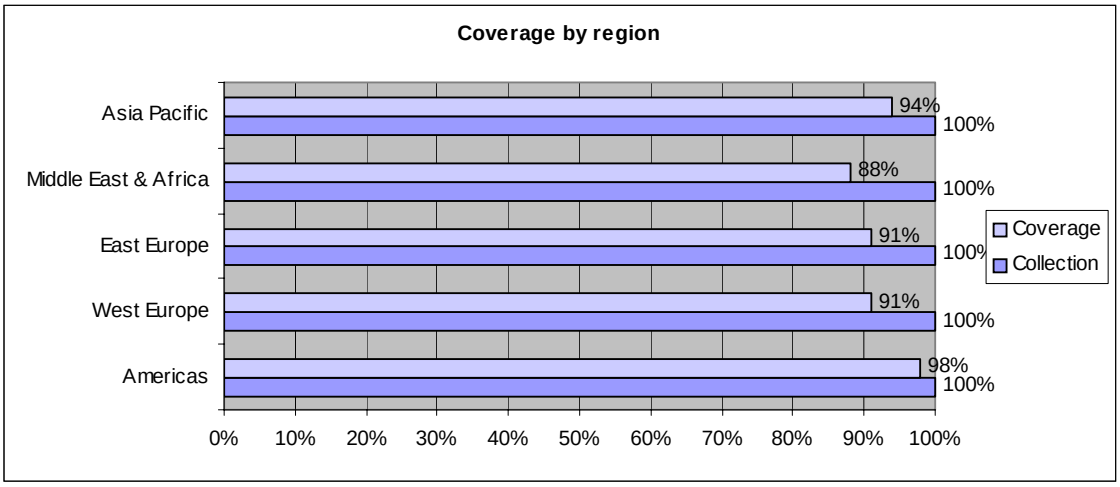

Figure 1.0 – Coverage by geographical region

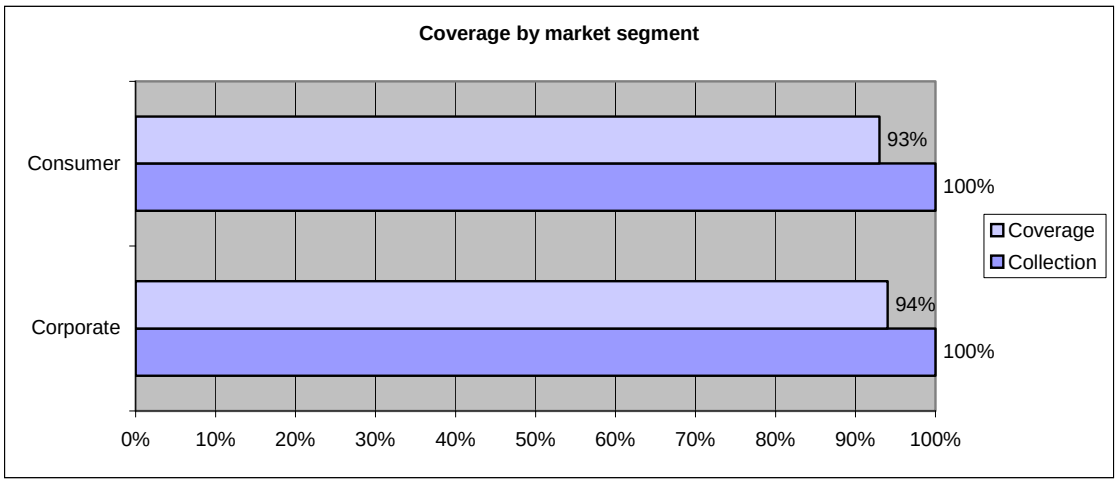

Figure 1.1 – Coverage by geographical region

Kaspersky Whitelisting - Test Report

Test Results TC01 - Database Coverage – File Type

The following table (Table 1.3) lists the database coverage statistics based on specific extensions with a graphical representation in Figure 1.2.

Extension	Files requested	Files identified	Percent Identified
.exe	19694	17291	87.80%
.dll	87627	85778	97.89%
.com	154	150	97.40%
.cab	4600	3129	68.02%
.sys	5669	5461	96.33%
.msi	995	707	71.06%
Other files (.pdf, .gpg, .doc, etc.)	721230	657482	91.16%

Table 1.3 – Coverage by file extension type

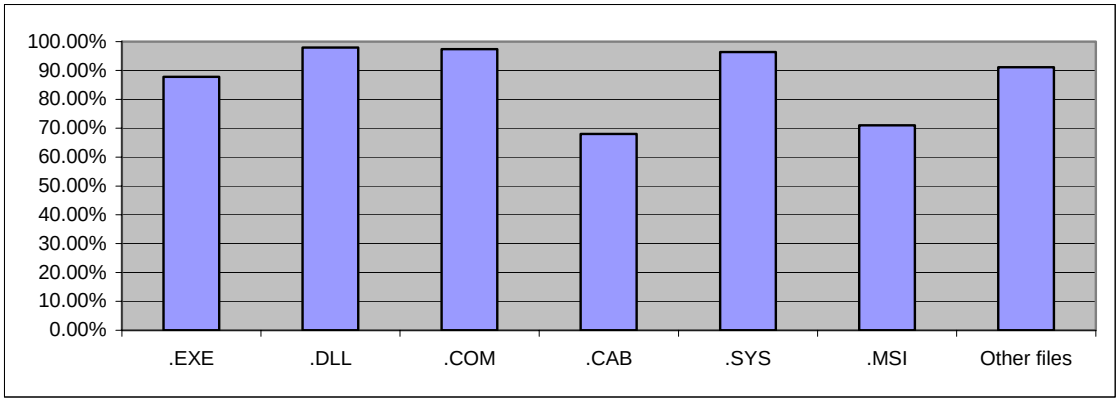

Figure 1.2 – Coverage by file extension type

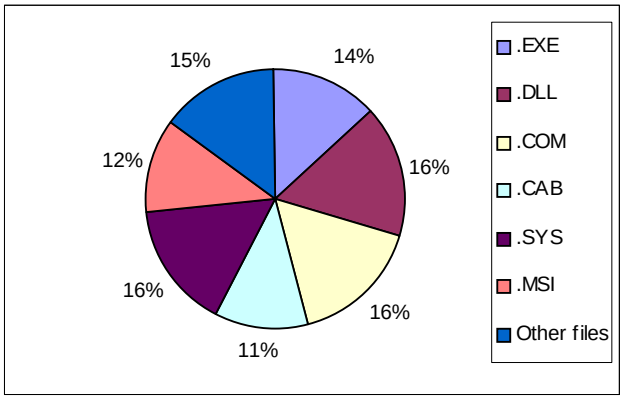

Figure 1.3 – Coverage by file extension type

Kaspersky Whitelisting - Test Report

Test Results TC01 - Database Coverage

TC01 – Result Analysis

When looking at the data for the MD5 test collection, it is clear that the whitelist database provides information, not just for a large number MD5s, but also for a large *variety* of MD5s.

Never does this become more obvious than when looking at MD5s belonging to software downloaded from popular download locations/mirrors that serve the Asia Pacific and Middle East/Africa regions.

MD5 recognition rates remained consistently high throughout all of the tests. The lowest of these, corporate software downloaded from the Middle East & Africa region, still registered an impressive 86% coverage. Of the other categories, the result that probably stands out most is the 98% coverage of all software downloaded from the Americas region.

When looking at individual file types, the traditional Portable Executable (PE) files such as .exe, .dll, and .com all recorded a high coverage rate.

Kaspersky Whitelisting - Test Report

Test Results TC02 - Database Fullness

The following table and graph (table 2.0 and figure 2.0) show the scores for the three main fields of file information based upon the results returned from the database related to the MetaData attached to each of the checksums. A full description of how these scores were arrived at can be found in Appendix A.

These scores are based on data returned only for those files contained in the test suite that are executable (.exe) files.

Data	Weighted percentage score
Expertise	87.17%
Statistics	80.57%
Raw Data	87.17%

Table 2.0 – Database fullness based upon Kaspersky metadata flags - .EXE files only

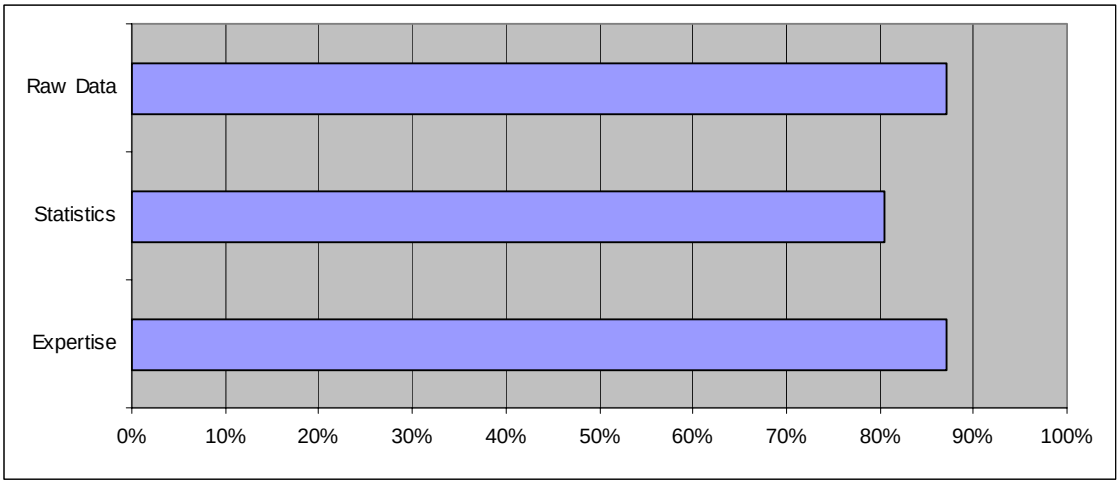

Figure 2.0 – Database fullness based upon Kaspersky metadata flags - .EXE files only

Kaspersky Whitelisting - Test Report

Test Results TC02 - Database Fullness

The following table and graph (table 2.1 and figure 2.1) show the scores for a number of metrics based upon the results returned from the database related to the MetaData attached to each of the checksums. A full description of how these scores were arrived at can be found in Appendix A.

Data	Weighted percentage score		Weighted percentage score
File Data Info	87.23	**KSN info**	78.71
File Product info	72.45	**File Source & Package Info**	72.1
Signatures & Certificates Info	63.73	**Verdict Type & Comment**	87.17
Users Trusted Level	81.21	**Categorization**	47.86
File Geography & Popularity	62.63	**Zone Info**	89.3

Table 2.1 – Database fullness based upon Kaspersky metadata flags - .EXE files only

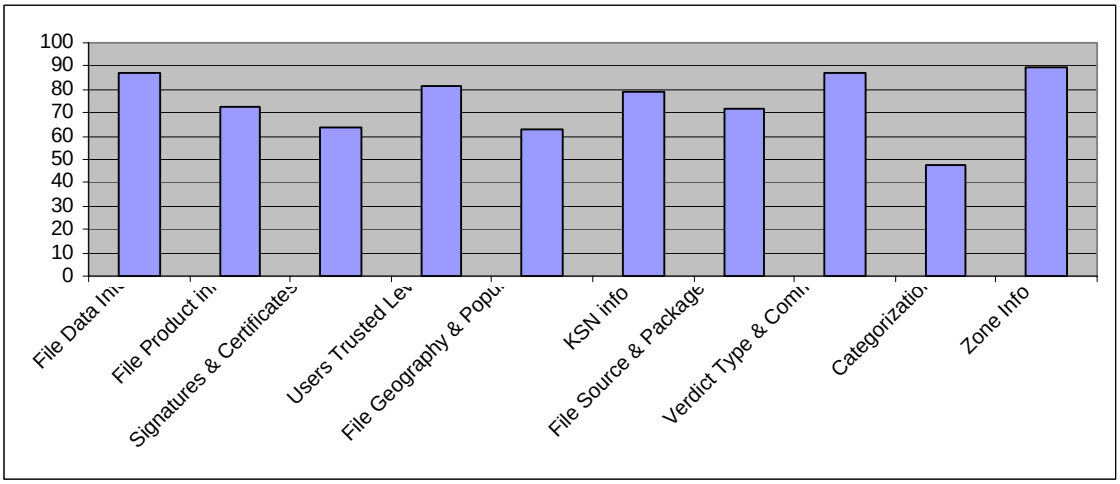

Figure 2.1 – Database fullness based upon Kaspersky metadata flags - .EXE files only.

Kaspersky Whitelisting - Test Report

Test Results TC02 - Database Fullness

The following table and graph (table 2.1 and figure 2.1) show the scores for the three main fields of file information based upon the results returned from the database related to the MetaData attached to each of the checksums. A full description of how these scores were arrived at can be found in Appendix A.

Worth noting with the tables and charts below is that this data is based on all file types included within the test set and that some of the fields, such as File Geography, are related solely to executable files.

Data	Weighted percentage score
Expertise	97.37%
Statistics	88.91%
Raw Data	85.01%

Table 2.0 – Database fullness based upon Kaspersky metadata flags - all files

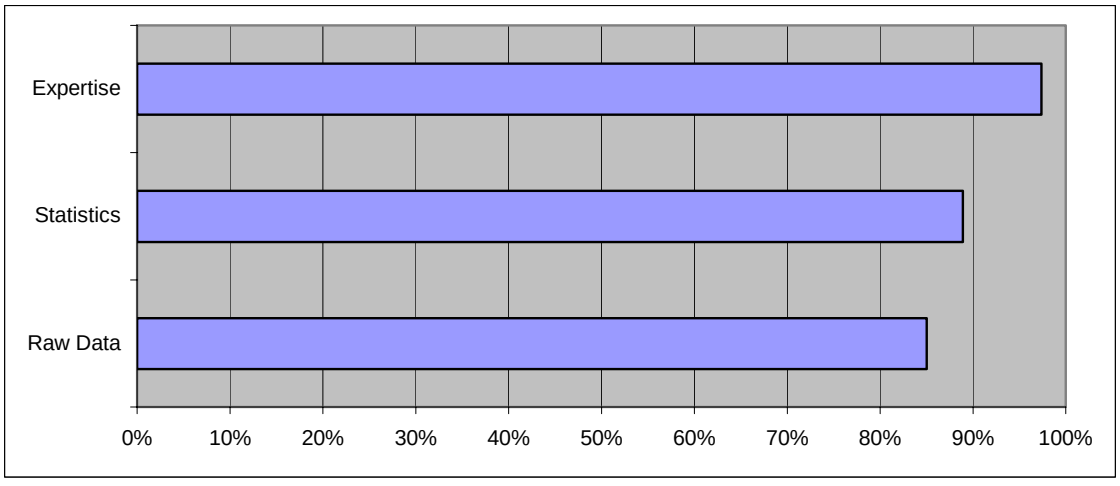

Figure 2.0 – Database fullness based upon Kaspersky metadata flags – all files

Kaspersky Whitelisting - Test Report

Test Results TC02 - Database Fullness

The following table and graph (table 2.1 and figure 2.1) show the scores for a number of metrics based upon the results returned from the database related to the MetaData attached to each of the checksums. A full description of how these scores were arrived at can be found in Appendix A.

Data	Weighted percentage score		Weighted percentage score
File Data Info	97.3	**KSN info**	29.93
File Product info	14.52	**File Source & Package Info**	88.92
Signatures & Certificates Info	63.28	**Verdict Type & Comment**	97.38
Users Trusted Level	3.89	**Categorization**	11.58
File Geography & Popularity	2.47	**Zone Info**	97.43

Table 2.1 – Database fullness based upon Kaspersky metadata flags – all files.

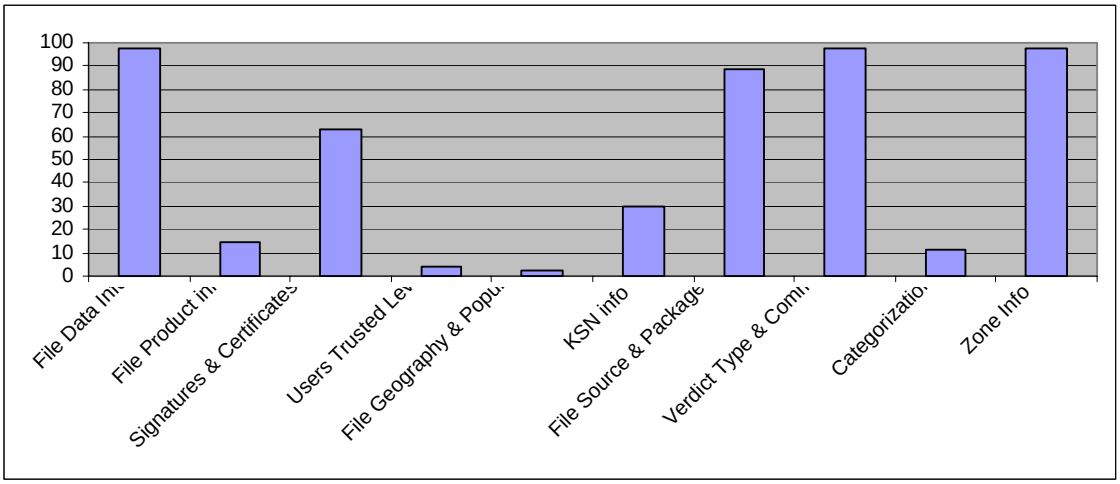

Figure 2.1 – Database fullness based upon Kaspersky metadata flags – all files.

Kaspersky Whitelisting - Test Report

Test Results TC02 - Database Fullness

TC02 – Result Analysis

It can be seen from the above results that, whilst certain areas of the metadata in the database do still require backfilling, the important sections related to the File Data Info, the File Source and Package info, the Verdict Types and Comments, Zone info and Expertise are all well populated – these are the core of the information on which decisions will likely be made within any implementation.

A marked difference can also be noted when comparing the file information provided specifically for executable files.

Kaspersky Whitelisting - Test Report

Test Results TC03 - Database Speed

Whitelisting database reply speed (Grouped by 1,000 MD5s)

The following tables display the time taken for the Whitelist database to respond to verification requests against individual checksums. These are the times recorded by West Coast Labs. The specific application provided by Kaspersky for use in the testing also returned a lookup time as part of its functionality, and the differences between the Kaspersky reported time and the time measured by West Coast Labs were well within the margins of error.

These verifications were conducted across 10 separate runs, each consisting of 1,000 unique MD5s, taking the verification test set to 10,000 unique MD5s in total.

Run of 1000 MD5s	Recorded Time (mm:ss:00)	Run of 1000 MD5s	Recorded Time (mm:ss:00)
1	01:04.10	**6**	00:29.70
2	00:12.60	**7**	00:27.90
3	00:11.70	**8**	00:24.80
4	00:11.20	**9**	00:38.70
5	00:53.90	**10**	00:14.90

Table 3.0 – Recorded times for 1000 unique MD5 lookups (mm:ss:00)

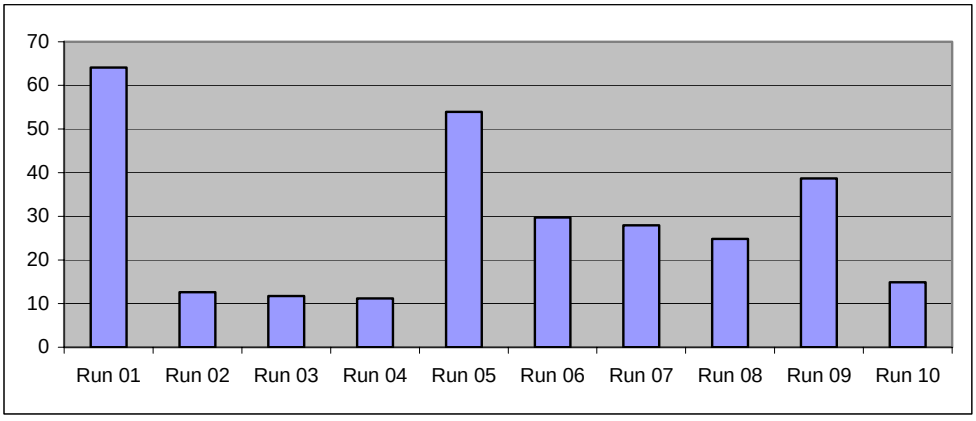

Figure 3.0 – Recorded times for 1000 unique MD5 lookups in seconds

Kaspersky Whitelisting - Test Report

Test Results TC03 - Database Speed - Grouped by 10,000 MD5s

The following graph (figure 3.1) shows the distribution lookup times recorded for the entire MD5 test collection (rather than 10 individual runs of 1000 each) when parsed through the whitelist tool in groups of 10,000.

Average Lookup Time for a group of 10,000 MD5s: 5 **minutes 13 seconds**
Average Lookup Time per MD5 when parsed in groups of 10,000: **0.03 seconds**

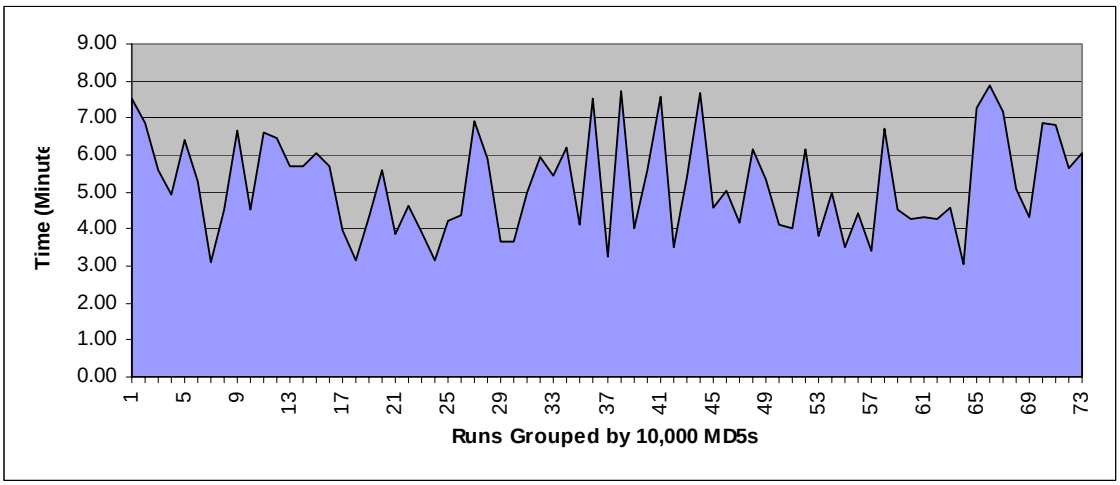

Figure 3.1 – runs of checksum lookups grouped by 10,000 MD5s over entire test collection

This shows the 73 runs grouped against the time taken in minutes - as can be seen, there were very few runs overall that took substantially longer than about 7 minutes to return when querying 10,000 checksums at a time.

Results appearing in the top and bottom 10% of the overall range were discarded in order to avoid skew from possible transient network conditions.

Kaspersky Whitelisting - Test Report

Test Results TC03 - Database Speed – Grouped by 1,000 MD5s

The following graph (figure 3.2) displays the lookup times recorded for the entire MD5 test collection (rather than 10 individual runs when parsed through the whitelist tool in groups of 1,000 – 844 sets of runs.

Average Lookup Time for a group of 1,000 MD5s: **18.5 seconds**
Average Lookup Time per MD5 when parsed in groups of 1,000: **0.02 seconds**

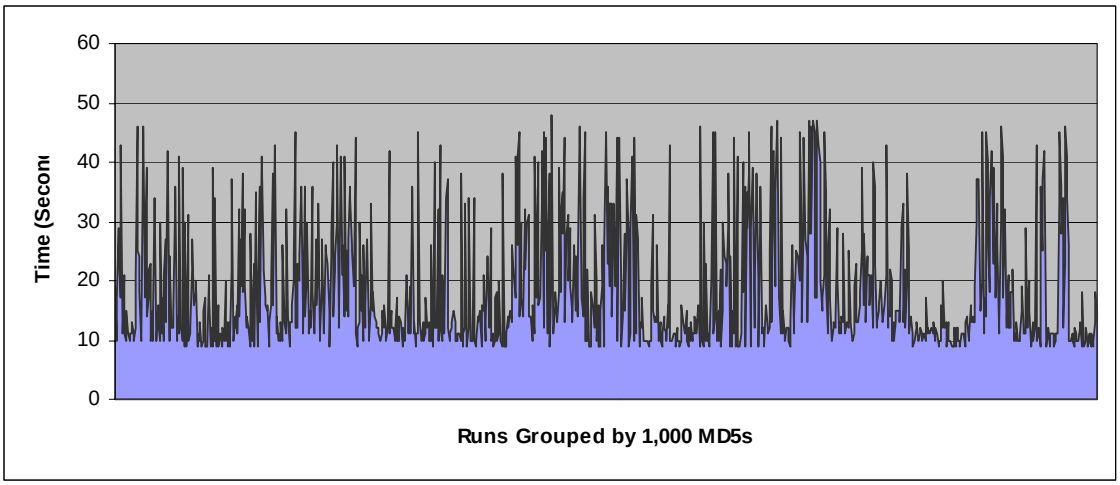

Figure 3.2 – runs of checksum lookups grouped by 1,000 MD5s over entire test collection

Once again, it can be seen that the majority of runs returned very quickly with only a few that took than about 40 seconds longer to return.

Results appearing in the top and bottom 10% of the overall range were discarded in order to avoid skew from possible transient network conditions.

Kaspersky Whitelisting - Test Report

Test Results TC03 - Database Speed – Addition of new files to Whitelist

The following graph (figure 3.3) shows the time taken in the process of the addition of a previously unknown clean file into the whitelist following its submission to Kaspersky for verification.

The average time in this case is just over **1 hour and 13 minutes**.

The second graph (figure 3.4) shows the time required for Kaspersky to respond to the reporting of, and take appropriate actions upon, a reported false positive result.

The average time in this case is just over **1 minute and 50 seconds**.

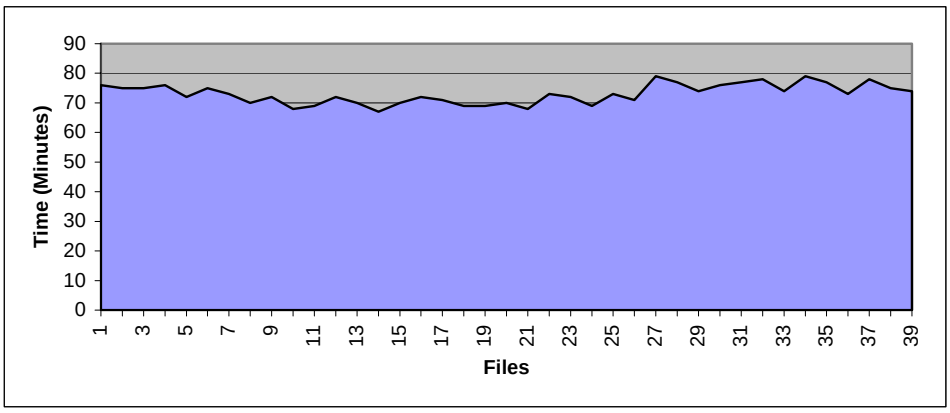

Figure 3.3 – Time taken to add files to whitelist database

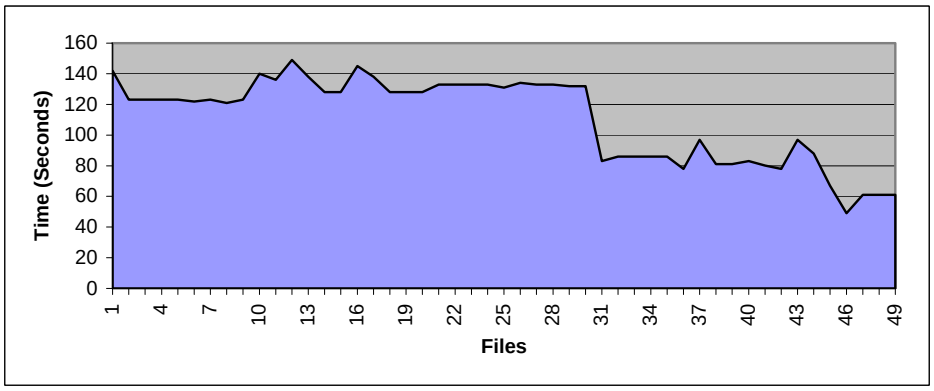

Figure 3.4 – Time taken to change file reputation in whitelist database

Kaspersky Whitelisting - Test Report

Test Results TC03 - Database Speed

TC03 – Database Speed conclusion

When using an Internet-based service, it is important that the response time of the service does not create a bottleneck. These tests have shown that, external network conditions not withstanding, Kaspersky's whitelist database provides rapid responses to MD5 lookup requests, with very few longer lookup times – these could have easily been attributable to transient network conditions.

With an average lookup time of around 0.02 seconds per MD5 3when grouped by 1,000, any delay caused by the lookup is minimal.

However, with a group of 10,000 MD5s, the average lookup time is increased to just over 0.04 seconds. So, if larger numbers of lookups are required, for example in mass installation rollouts to endpoints, so any potential users considering large global enterprise wide deployments would be advised to consider staggering rollouts (likely in a multi-time zone environment anyway).

The verification by WCL of the results provided by the Kaspersky Whitelist database and reported through the logs of the lookup application in terms of time taken to perform these lookups show that the results are broadly similar and well within acceptable margins of error.

For day-to-day lookups of a single file, perhaps an executable installation file for a given program, the average lookup time of approximately two-hundredths of a second is more than reasonable for most corporate networks and applications.

Kaspersky Whitelisting - Test Report

Test Results TC04 - Database False Rate

The following results, expressed as a percentage in Table 4.0, are of MD5s are taken from a test set of 20,000 infected files, and returned with the following verdicts and zone names.

Verdict	Zone Name	Percentage	Note
Clean	Good	0.49%	Incorrectly identified as clean
Infected	Any	96.89%	Correctly identified

Table 4.0 – false positive rates in the database

The remaining 2.62% unaccounted for in the statistics above had no, or minimal, reputation information at the time of testing, and Kaspersky stated that these were internally classified as grey files in terms of metadata as the reputation building process was underway at time of testing.

The following result, expressed as a percentage in Table 4.1, is of MD5s are taken from the wider general test set of all (clean) files used in TC01, and returned with the following verdict and zone names.

Verdict	Zone Name	Percentage	Note
Infected	Any	0%	No misidentifications

Table 4.1 – false positive rates in the database

Kaspersky Whitelisting - Test Report

Test Results TC04 - Database False Rate

Conclusion

The accuracy of the whitelist database, in this instance with regard to malicious files, is high. The key result during this test is the 96.89% detection rate for malware, which is remarkable from a cloud-based service which is not particularly aimed at malware detection, but is designed to work alongside a traditional anti-malware engine. This means that those organisations looking to employ this service should benefit from a significant level of protection afforded by a correctly configured engine using this whitelisting database before the anti-malware engines even need to become involved with files.

Also recorded, and arguably just as significant, is the 0% false-positive result. An ever increasing concern for system administrators is the accidental deletion, blocking, or interference with genuine, or even perhaps vital, system files. Whilst this testing does not guard against the risk of future false-positive entries, based upon these results the whitelisting service appears to introduce no notable increased risk of a False Positive against the wide range of software tested as part of this programme.

Kaspersky Whitelisting - Test Report

Test Results TC05 – Additional Services and Ease of Use

Whitelist Service – http://whitelist.kaspersky.com/whitelist_program

The Kaspersky Whitelisting programme involves cooperation between Kaspersky and software vendors and distributors on regular basis. The overall goal of this programme is to reduce the number of false positives in Whitelist database
In order to use this service, prospective users must follow a very short registration and setup process. After completing the registration form (Figure 5.0), and it being accepted and verified by the Kaspersky Lab White List administrators, the user is provided with an FTP server and login credentials to allow for file uploads.

This FTP server is, in turn, polled approximately every five minutes for the presence of new uploads. If detected, these new files are then downloaded and analysed by Kaspersky Lab using a variety of both manual and automated processes.

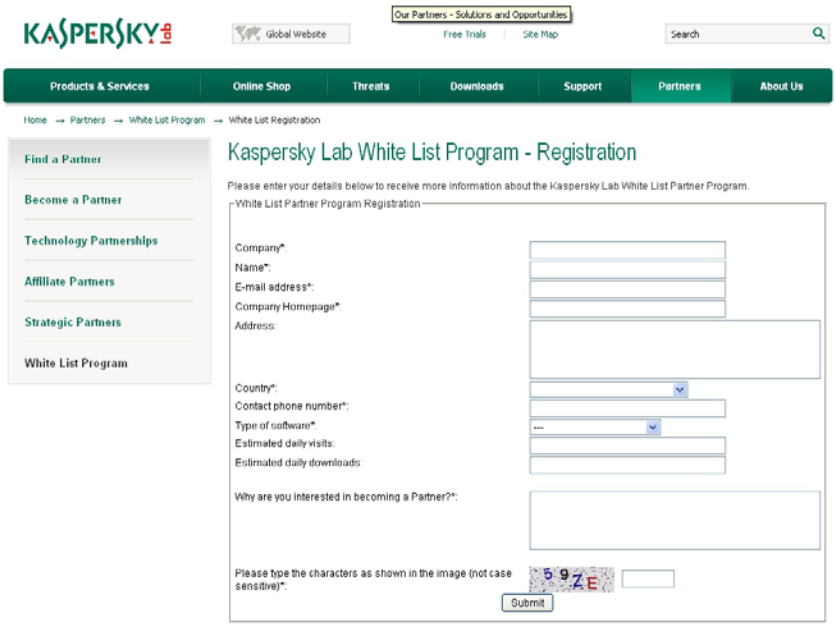

Figure 5.0 – Kaspersky White List Registration Page.

Kaspersky Whitelisting - Test Report

Test Results TC05 – Additional Services and Ease of Use

Should the submitted files be confirmed as clean and valid, they are immediately verified and entered into the whitelist database (if clean), along with all accompanying information and become instantly available.

Throughout the entire analysis process, the user is kept informed of the status of their uploaded files by a series of automated reports. These begin to appear once the files have been downloaded from the FTP server by Kaspersky and culminate in a final email containing the result of the analysis.

Kaspersky Whitelisting - Test Report

Test Results TC05 – Additional Services and Ease of Use

Trusted Service – http://trusted.kaspersky.com/

The Trusted Service provided by Kaspersky Lab allows subscribed partners, who have a valid Whitelist Service account to display the animated Trusted logo shown in Figure 5.1 on the download page for their respective file/executable. This program is valid for Whitelist service partners only

Figure 5.1 – Kaspersky Lab Trusted Logo at various stages throughout the single time animation

Users of the partner's software may then click upon this logo to be taken to the respective page on Kaspersky's website (an example is shown in Figure 5.2 below) in order to verify that the file in question is correct and that the logo is not being falsely used or subverted, as shown in the below image.

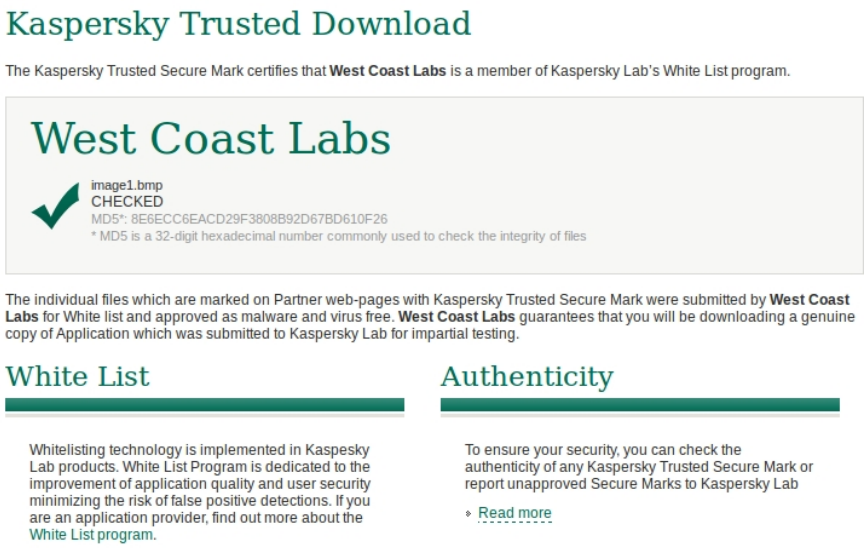

Figure 5.2 – Kaspersky Trusted Download page

Kaspersky Whitelisting - Test Report

Test Results TC05 – Additional Services

It can be seen from Figure 5.2 that the particular partner, file name and MD5 checksum is displayed on the Kaspersky site. The end user can therefore always validate through the use of the checksum that the software they are downloading was classified as clean.

TC05 – Partner Testimonial

As most of this process is carried out within Kaspersky, and therefore not directly verifiable by WCL outside of the verification tests as described above, WCL also contacted a number of existing customers of Kaspersky in order to gain outside opinions of the service.

Their feedback was largely positive, the details of which can be found in Appendix B.

TC05- Results Analysis

At a little over an hour to add new files into the system, the Trusted service will allow for a same-day confirmation and use of the Trusted logo. The process of simply having to upload files to a given FTP address means that the submission of files can be quite easily automated as part of a vendor's existing systems making this a very easy way of having a third party verify the integrity of files in any application.

Although not tested as part of this report, Kaspersky can also receive software directly from an enrolled Partner's sources or ftp server. The Partner provides and xml file or files with URL links to the software sources enclosed and Kaspersky will automatically download it for processing within the framework described above.

Kaspersky Whitelisting - Test Report

Test Results TC06 – Default Deny mode

This particular test case was executed to determine whether the files that were associated with specific operating systems that would be needed to run a Default Deny mode (where only the basic Operating System and necessary drivers are allowed to execute) were included in the database to make this sort of operation possible.

The below results in Table 6.0 (with graphics in Figure 6.0) show the outcomes against the following file types, which are needed to ensure Default Deny mode would work properly such as PE/DLL (.dll, .sys, .ocx, and so on), PE/EXE, COM, CDF, MSI, CAB, MSP, XML/MSC.

Operating System	Percentage of known MD5s
Windows XP Service Pack 3 (32 bit)	99.98%
Windows 7 Embedded Edition (32 bit)	97.89%
Windows 7 Home Edition (64 bit)	98.34%
Windows 7 Professional (32 bit)	95.95%
Windows 7 Enterprise (32-bit)	97.84%
Windows 7 Enterprise (64-bit)	99.28%

Table 6.0 – Default Deny results for specific executable types

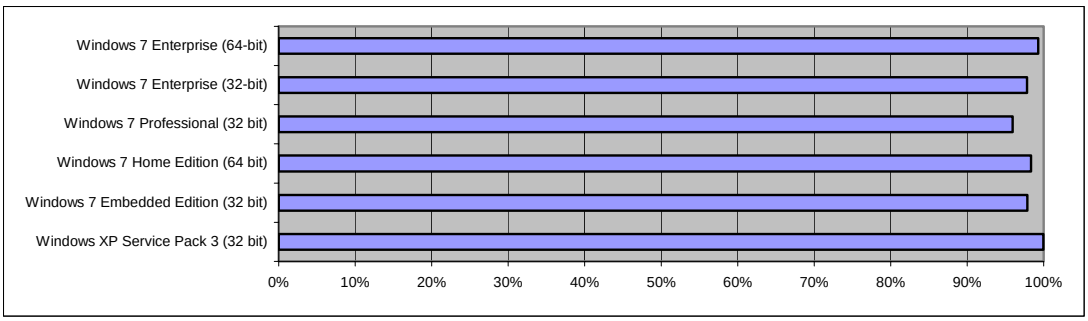

Figure 6.0 – Default Deny results for specific executable types

Kaspersky Whitelisting - Test Report

Test Results TC06 – Default Deny mode

TC06- Results Analysis

Default Deny mode, as a technology, is usually implemented locally on an endpoint host by using a series of flexible categorization rules which are stored on within an endpoint security product (in case of Kaspersky Lab this is Endpoint 8, which was not tested as part of this report).

In Kaspersky's case, these categorization rules use metainformation about the file for classification, categorization and, ultimately a determination as to whether the file should be allowed to run or not. It is therefore important that even software unknown to the Whitelist database is categorized by the endpoint software as well, whilst their model simultaneously ensures that a Default Deny mode deployment is possible without a connection to the cloud database being necessary.

There is no doubt that a Default Deny mode is critically important for network connected hosts, and so Kaspersky Lab also stores data on related software in their Whitelisting database. This functionality means that there is extra reassurance that when the endpoint application checks the data, it has been carefully considered by Kaspersky as to whether software is appropriate for use on any internet connected host.

Perhaps unsurprisingly, it can be seen that the majority of the appropriate files for running a Default Deny mode are in the database and are available for use in under these circumstances – this exactly what is required for those users who are interested in keeping tight control over their systems, for example in a PoS (Point of Sale) type environment.

Kaspersky Whitelisting - Test Report

West Coast Labs' Conclusion

Throughout the testing process, the Kaspersky Lab Whitelist Service has maintained a high degree of responsiveness, accuracy, and coverage.

The coverage of the service (as tested in TC01), both in terms of geographic coverage and market segment, should ensure that even some of the more uncommon pieces of software will be accounted for.

Meanwhile, the value of the information provided for each individual file will allow for an informed decision to be made when deciding to block or allow a file at the gateway level.

However, none of the coverage or file information would be as useful if the service did not also provide a quick response. As the tests in TC03 show, single file lookups are, on average, handled in just 0.02 – 0.04 seconds

All of the above, when coupled with the ease of use in TC05 and the feedback from existing customers, points to a service that should benefit its users and enhance any existing network and content security setups.

Kaspersky Whitelisting - Test Report

Appendix A – Determination of rollup scores for TC-02

The following is the weighting algorithm agreed with Kaspersky for calculating TC-02 and is reproduced from their document.

1. Interpretation of data about objects

In the calculation scheme there are 3 groups of high level. These levels are created in order to reflect importance/weight of metainformation about objects. Clarification of high level groups:

- Raw data – consist of data about attributes and characteristics of objects. It also includes information about digital signatures, certificates, etc. This group is basic level of data about objects. It has minimal informative value.
- Statistics – consist of data about popularity of object in the world, sources and user's trust level. This group accumulates data of informational streams which are generated by user's community (in our case this is KSN- Kaspersky Security Network).
- Expertise –consist of data about confidence zone of object (reputation), functional category and assigned verdict

Decomposition of the high level groups is made according to data which are part of the group. Thus 10 groups were formed and divided between the high level groups:

- Raw data
    - File data info – characteristics of the object
    - File product info – information about product which is received from the object
    - Signatures & Certificates info – information about digital signatures and certificates related with the object
- Statistics
    - Users trusted level – user's trust level to the object
    - File geography & popularity – popularity of the object in the world and popularity among the users

  - KSN info – information about the object from the cloud
  - File source & package info – sources of the object, parent objects and references
- Expertise
  - Verdict type & comment - type and anti-virus verdict description
  - Categorization – functional category of the object
  - Zone info – object zone

Each sub-group is presented by set of knowledge about file:

- File data info
- Signatures & Certificates info
  - MD5 – MD5 hash of the file
  - SHA1 – SHA1 hash of the file
  - Format Type – Type/format of the file
  - Size – File size (bytes)
- File product info
  - OriginalFilename – FVI file original name
  - FileVersion – FVI fileVersion
  - Language – FIV locale language
  - ProductName – FIV product name
  - ProductVersion – FIV product version (Major.Minor.Build.Revision)
  - VendorName – FIV vendor name
- Signatures & Certificates info
  - Signature Status – information about signature presence

- Signature TimeStamp – Time when signature was created
- Is Signature Verified – certificate validity mark
- IsDirectlySigned – direct signature mark
- Is Signature From CAT – mark which means that file is signed via CAT catalogue
- Certificate Discredited – Indication, that given certificate was discredited in WL DB
- Certificate Trusted – certificate signature validity mark
- SerialNumber – Certificate's serial number
- Certificate Issued – Date, when certificate was issued
- Certificate ValidTo (Expires) – Date, starting which the certificate becomes invalid
- Certificate Vendor (Subject) – Manufacturer's name, mentioned in certificate
- Publisher (Issuer) – Issuer's name

- Users trusted level
  - Trusted Groups percent
  - Low Restricted percent
  - High Restricted percent
  - Untrusted percent
  - File geography & popularity
  - Country Sharing Code
  - Country Sharing Percent
  - File popularity for Last 2 Weeks
  - File popularity for Last Day
  - File popularity for Last Month
  - File popularity for Last Week

  - Total File popularity
- Cloud-based info
  - Cloud First Request Time
  - Cloud User Count
  - Time Added
  - Last Scan Time
  - Last Zone Change Time
- File source & package info
  - FileSource Name
  - URL
  - MD5
  - Original Name
  - Signature Status
  - Time Added
  - SHA1
  - Size
  - Format Type
- Verdict type & comment
  - Verdict Comment
  - VerdictType
- Categorization
  - Categorization
  - Zone info

- Zone info

2. Calculation scheme

Scheme goal- to estimate importance/value of data about objects which is proposed by service developer.

The scheme is based on weights usage which presents importance of the weighted element (attribute) within considered sub-group. Distribution of file's attributes to high level groups (Raw data, Statistics, Expertise) and then to sub-groups allows making decomposition of analyzed elements of data. It also allows structuring it from general to particular and provides opportunity to precisely estimate the weight of each informational element.

Thus all information about the object should be presented within partitioning described in point 1. After that each element and group receives a weight.

The scheme includes 2 parts:

- Calculation of figures for high level groups
- Calculation of figures for its sub-groups

3. Calculation of figures for high level group

Calculation of figures for high level group (Raw data, Statistics, Expertise) is achieved by sum of weights of all elements (attributes) of group which are presented in Whitelisting service reply. Then calculated sum is submitted to input of threshold function. This function can have value 0 (if sum is less than half of absolute weight of group (AW, which is equal 1)). This function can also have value 1 (if sum is more or equal to half of AW). This operation should be made for each file. And final sum will present target figure. Division of final sum into number of positive WL service replies (number of known MD5) will present weighted figure of coverage in % (for each high level group)

4. Calculation of figures for sub-group

Calculation of figures for sub-group (File data info, File product info, Signatures & Certificates info, Users trusted level, File geography & popularity, KSN info, File source & package info, Verdict type &

comment, Categorization, Zone info) is achieved by sum of weights of all elements of group (for each group separately) which are presented in Whitelisting service reply. Then calculated sum is submitted to input of threshold function. This function can have value 0 (if sum is less than half of absolute weight of group (AW, which is equal 1)). This function can also have value 1 (if sum is more or equal to half of AW). This operation should be made for each file. And final sum will present target figure. Division of final sum into number of positive WL service replies (number of known MD5) will present weighted figure of coverage in % (for each high level group)

Kaspersky Whitelisting - Test Report

Appendix B – Customer Feedback Questionnaires

Customer Feedback #1 – Gamona.de (Trusted Service)

Question #1 - scale of 1- 10: How would you rate the Trusted service as a whole? **8**

Question #2 - scale of 1- 10: If used, how would you rate the response time of the service? **8**

Question #3 – scale of 1-10: If used, how would you rate its ease of use? **7**

Question #4 – comment: If used, please comment on your experience with the service e.g. how long you've used it, if you've found it efficient, if you believe it's helped verify the security of your uploaded content, been of benefit to your business, etc.

"We've been using the Kaspersky Trusted Service since August 2010. It's a great benefit for us to show ours users the quality of the files and it's highly accepted. The only improvement we see would be an API to exchange the responses on a much easier way then via ZIP files."

Kaspersky Whitelisting - Test Report

Appendix B – Customer Feedback Questionnaires

Customer Feedback #2- Hewlett Packard (Whitelisting)

Question #1 - scale of 1- 10 : How would you rate the whitelist service as a whole?

10 – The process is easy to work with and very responsive

Question #2 - scale of 1- 10 : If used, how would you rate the file information provided by the database?

8 – provides adequate information

Question #3 – scale of 1- 10 : If used, how would you rate the response time of the database?

10 – Excellent response time….

Question #4 – scale of 1-10 : If used, how would you rate the accuracy of the information provided by the database?

9 – I have found only 1 error in the past. This is very reliable overall

Question #5 – scale of 1-10 : If used, how would you rate the geographical coverage of the database? i.e. information on files from various regions

N/a = Not reviewed or used

Question #6 – scale of 1-10 : If used, how would you rate the file-type coverage of the database? I.e. executables, images, system files, etc

10 – covers all the file types we have and that we submit.

Kaspersky Whitelisting - Test Report

Appendix B – Customer Feedback Questionnaires

Customer Feedback #2 – Hewlett Packard (Trusted Service)

Question #1 - scale of 1- 10 : How would you rate the Trusted service as a whole?

10 – excellent, both for us and our customers...

Question #2 - scale of 1- 10 : If used, how would you rate the response time of the service?

10 - excellent

Question #3 – scale of 1-10 : If used, how would you rate its ease of use?

9 – very good

Question #4 – comment : If used, please comment on your experience with the service e.g. how long you've used it, if you've found it efficient, if you believe it's helped verify the security of your uploaded content, been of benefit to your business, etc

"The Kaspersky team with their whitelisting and trusted services have been extremely responsive and helpful regarding our software compatibility and ensuring our software is properly reported as safe. As our s/w engineers have made changes and evolved our software the K. services has allowed complete s/w recognition and feedback. In the case where our s/w engineers created a new process which was deemed a risk, the Kaspersky team worked with our s/w engineers to resolve the problems.

These services are definitely not stand alone, but supported by very competent individuals who really work to make their solutions the best possible.

It is a real pleasure working with them!"

Kaspersky Whitelisting - Test Report

Appendix B – Customer Feedback Questionnaires

Customer Feedback #3 – VideoLAN organisation (Whitelisting)

Question #1 - scale of 1- 10 :How would you rate the whitelist service as a whole?

9

Question #3 – scale of 1- 10 : If used, how would you rate the response time of the database?

9

Question #6 – scale of 1-10 : If used, how would you rate the file-type coverage of the database? I.e. executables, images, system files, etc.

9

Kaspersky Whitelisting - Test Report

Appendix B – Customer Feedback Questionnaires

Customer Feedback #3– VideoLAN organisation (Trusted Service)

Section 2 – Kaspersky Trusted Service

Question #1 - scale of 1- 10 : How would you rate the Trusted service as a whole?

8

Question #2 - scale of 1- 10 : If used, how would you rate the response time of the service?

8

Question #3 – scale of 1-10 : If used, how would you rate its ease of use?

9

Question #4 – comment : If used, please comment on your experience with the service e.g. how long you've used it, if you've found it efficient, if you believe it's helped verify the security of your uploaded content, been of benefit to your business, etc.

"It seems very simple to use and great for us; saving us a lot of time."

Kaspersky Whitelisting - Test Report

West Coast Labs Disclaimer

While West Coast Labs is dedicated to ensuring the highest standard of security product testing in the industry, it is not always possible within the scope of any given test to completely and exhaustively validate every variation of the security capabilities and/or functionality of any particular product tested and/or guarantee that any particular product tested is fit for any given purpose.Therefore, the test results published within any given report should not be taken and accepted in isolation.

Potential customers interested in deploying any particular product tested by West Coast Labs are recommended to seek further confirmation that the said product will meet their individual requirements, technical infrastructure and specific security considerations.All test results represent a snapshot of security capability at one point in time and are not a guarantee of future product effectiveness and security capability.

West Coast Labs provide test results for any particular product tested, most relevant at the time of testing and within the specified scope of testing and relative to the specific test hardware, software, equipment, infrastructure, configurations and tools used during the specific test process.

West Coast Labs is unable to directly endorse or certify the overall worthiness and reliability of any particular product tested for any given situation or deployment.

Kaspersky Whitelisting - Test Report

Revision History

Issue	Description of Changes	Date Issued
1.0	Cleared for public release	14/12/11

USA SALES

T +1 (949) 870 3250

EUROPE SALES

T +44 (0) 2920 548400

CHINA, KOREA, JAPAN, TAIWAN SALES

T +86 1 343 921 7464

REST OF THE WORLD SALES

T +44 (0) 2920 548400

CORPORATE OFFICES AND TEST FACILITIES

US Headquarters and Test Facility

West Coast Labs

16842 Von Karman Avenue, Suite 125,

Irvine, California, CA92606, USA

T +1 (949) 870 3250, **F** +1 (949) 251 1586

European Headquarters and Test Facility

West Coast Labs

Unit 9, Oak Tree Court, Mulberry Drive

Cardiff Gate Business Park, Cardiff CF23 8RS, UK

T +44 (0) 2920 548400, **F** +44 (0) 2920 548401

Asia Headquarters and Test Facility

A2/9 Lower Ground floor, Safdarjung Enclave,

Main Africa Avenue Road, New Delhi 110 029, India.

T +91 (0) 11 4602 0622, **F** +44 (0) 11 4602 0633

E info@westcoast.com

W www.westcoastlabs.com