Kaspersky Internet Security 2013 Test Report

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

Date of the report: August 31st, 2012, last update: August 31st, 2012

Executive Summary

In June and July 2012, AV-Test performed a review of the new Kaspersky Internet Security 2013. The product has been tested against the full set of AV-TEST tests: Protection, Repair and Usability. To perform the test runs, a clean Windows 7, SP1 (64 bit) image (June) and a clean Windows XP, SP3 (32 bit) image (July) was used on several identical PCs. On this image, the security software was installed and then the individual tests have been carried out.

Kaspersky Internet Security 2013 performed very well in all of the test categories on both operating systems and achieved the best possible results in several of the tests, always being better than the industry average.

Products Tested

The testing occurred in June and July 2012. AV-Test used the latest releases available at the time of the test of the following products:

- Kaspersky Internet Security 2013 (Program version 13.0.0.3370)

Methodology and Scoring

Platform

All tests have been performed on identical PCs equipped with the following hardware:

- Intel Xeon Quad-Core X3360 CPU
- 4 GB Ram
- 500 GB HDD (Western Digital)
- Intel Pro/1000 PL (Gigabit Ethernet) NIC

The operating system was Windows 7 Ultimate Service Pack 1(64 bit) with only those hotfixes that were part of SP1 as well as all patches that were available on May 1st2012 and Windows XP SP3 (32 bit) with only those hotfixes that were part of SP3 as well as all patches that were available on June 1st2012

Testing methodology

The tests have been carried out following the three AV-TEST categories: Protection, Repair and Usability.

Protection

We test the protective effect of security solutions by installing them on a non-infected system and examining how they respond to malware threats. We do so by simulating a variety of attack scenarios such as the threat of e-mail attachments, infected websites or malicious files that have been transferred from external storage devices. When carrying out these tests, AV-TEST takes the entire functionality of the protection program into account.

Repair

The repair performance of products is analyzed using a system that is already infected. We evaluate the products' ability to remove active malware and to restore other system changes as well as its performance when detecting and removing specially hidden malware (rootkits).

Usability

We investigate the influence that security software has on the usability of the system and the system interferences that occur, for example: warning messages, general messages and blockages, false positives during system scans and the computer slowing down while the software is being used.

For a detailed description of the methodology please refer to http://www.av-test.org/en/tests/test-modules/

Samples

June Test

1. BLOCKING OF "REAL WORLD" ATTACKS: 51 URLs, 3 Mails

2. DETECTION OF "ZOO" MALWARE: 129063 malicious files

3. DETECTION OF PREVALENT MALWARE: 2500 malicious files

4. FALSE POSITIVE TESTING (STATIC SET OF FILES): 372810 clean files

6. SYSTEM DISINFECTION / REMEDIATION TESTING: 43 malicious files

7. DETECTION AND REMOVAL OF ACTIVELY RUNNING ROOTKITS: not tested

8. DYNAMIC (BEHAVIOUR-BASED) DETECTION OF MALWARE: 10 malicious files

9. FALSE POSITIVE PREVENTION DURING THE DYNAMIC MALWARE DETECTION: 24 clean programs

July Test

1. BLOCKING OF "REAL WORLD" ATTACKS: 45 URLs

2. DETECTION OF "ZOO" MALWARE: 126077 malicious files

3. DETECTION OF PREVALENT MALWARE: 2500 malicious files

4. FALSE POSITIVE TESTING (STATIC SET OF FILES): 366791 clean files

6. SYSTEM DISINFECTION / REMEDIATION TESTING: 27 malicious files

7. DETECTION AND REMOVAL OF ACTIVELY RUNNING ROOTKITS: 14

8. DYNAMIC (BEHAVIOUR-BASED) DETECTION OF MALWARE: 10 malicious files

9. FALSE POSITIVE PREVENTION DURING THE DYNAMIC MALWARE DETECTION: 22 clean programs

All tested samples have been collected and analyzed by AV-TEST. Samples used for the tests 2, 3, 4, 6 and 7 have been collected in the 4 weeks before start of the test (June test: Files have been collected during May. July test: Files have been collected during June). Samples used for the other tests have been collected at the day of the test.

Test Results

The first category is Protection, which consists of four individual tests:

- Blocking of “Real World” attacks tests the full product (dynamic and static protection, e.g. signatures, behavior-based detection, URL blocking, exploit blocking etc.) against certain real threats (e.g. malicious URLs and Emails)
- Detection of “Zoo” Malware and Detection of prevalent malware: This tests the static detection (signatures and heuristics) against a big set of inactive, recent malware files

- Dynamic detection of malware: This tests the behavior-based detection (and to some extent the static detection as well) against a small number of active malware threats

With these different test approaches it is possible to get a pretty accurate picture of the overall protection capabilities of the product. When looking at the results it can be seen that Kaspersky achieved perfect scores (100%) for several tests and was always better or equal than the industry average calculated of all 28 tested products in each month.

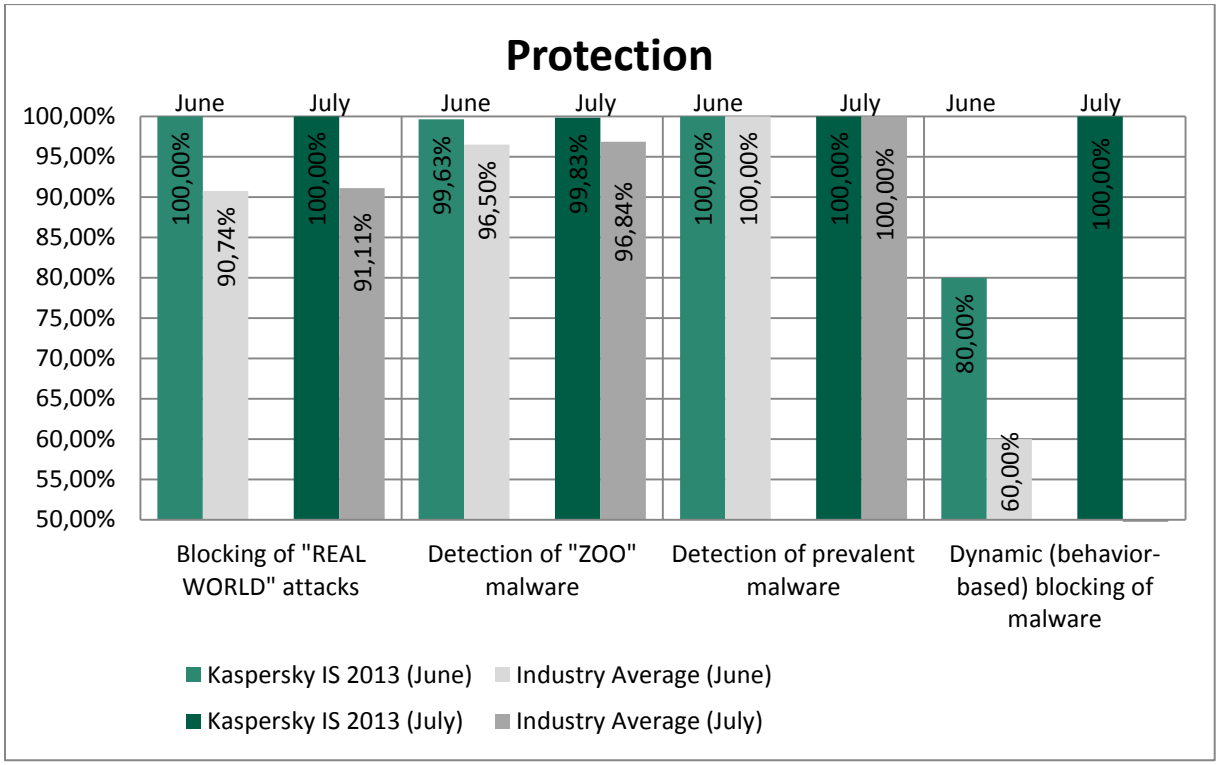

Figure 1: Protection

The most important test is the first one, Blocking of “Real World” attacks. The products have to use all of their protection features (static, dynamic, URL blocking etc.) to detect and stop the threat. Kaspersky successfully detected and stopped all threats in the test, both malicious URLs as well as malicious e-mails. The industry average was only at around 90% here, which is a pretty big difference. The results of the individual feature tests explain why Kaspersky scores so well. Both the detection of Zoo malware as well as of prevalent malware show very good results. The industry average in case of Zoo malware is around 3% lower than the Kaspersky result. The same is true for the dynamic blocking of malware. Kaspersky scores 80% resp. 100% in the two months and both of these results are way higher than the average of the other products, which was just 60%. Since Kaspersky scores very good results in the individual feature tests, which are always higher than the industry average it is no surprise that their real-world performance is also outstanding when combining all the protection features against current real threats.

The next test category is Repair in which the security software has to clean an infected system from malware. Two different test sets are used here. The first contains usual malware samples while the second set contains malware that uses rootkit techniques which are still a challenge for many products. Figure three shows the results of Kaspersky as well as the industry average for the different tests. Please note that there are only average results for July, since no test has been performed in

June for the other products. Also there are no rootkit results in June for Kaspersky, because there were no working, recent rootkits for Windows 7 SP1 64-bit available at that time.

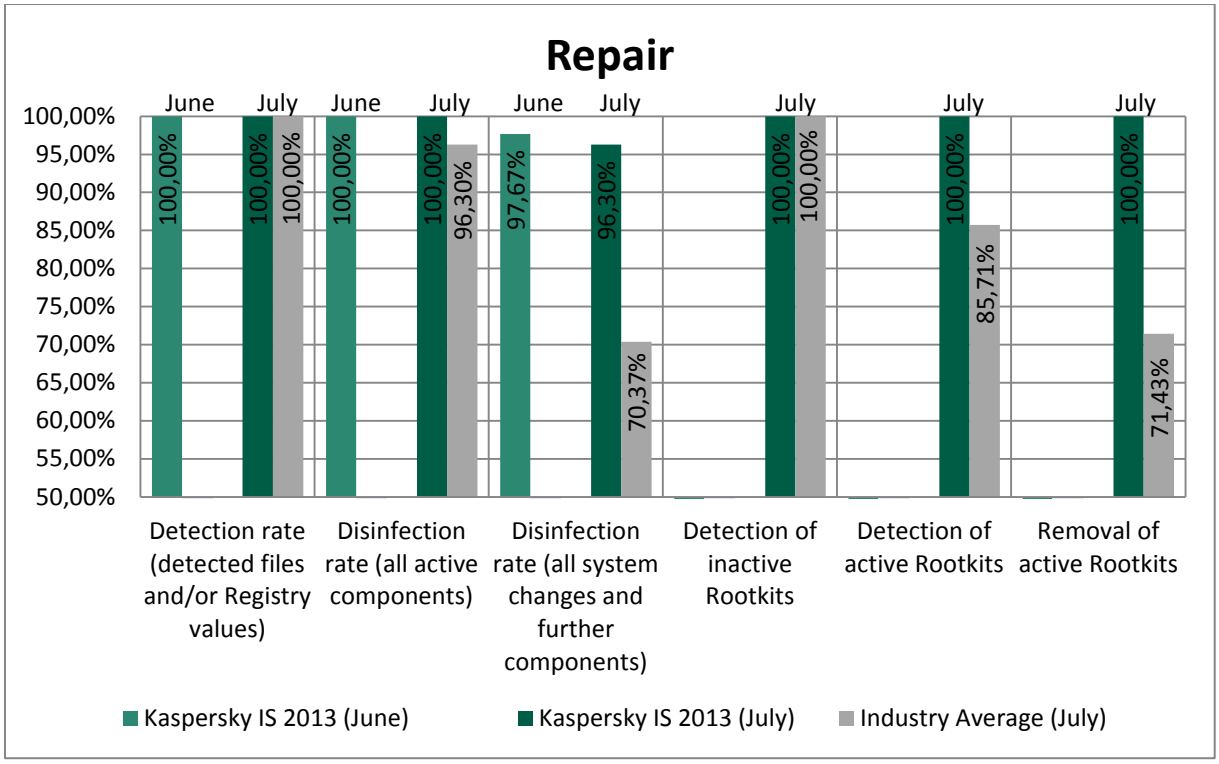

Figure 2: Repair

Kaspersky was able to detect all active malware as well as rootkit infections and successfully disable them. The industry average for detection of normal malware is also at 100% but only around 86% of the active rootkit infections were detected on average. The industry average for removal was also far worse than the Kaspersky result. Normal malware was successfully disabled in 96% and rootkits only in 71%. Kaspersky even managed to completely clean the malware (including further system changes that are not per se malicious but may still be bothersome) in 98% resp. 96%, while the industry average is only at 70% here. With these results Kaspersky Internet Security 2013 is far ahead of many other products.

The final test category takes a look at the impact on the usability of the system. Three different attributes of the security software are covered here:

- How much does the software slow-down typical actions on the system
- How many false alarms and warnings are triggered during a system scan
- How many false alarms and warnings are triggered during the usage of the system

All of these things have an impact on the usability of the system and ideally the security software would not disturb the user at all. There was no single false alarm during the usage of the system (installing and using over 20 different wide-spread software products) by Kaspersky. The industry average is at one for the blocking of programs during installation or usage. There was one false warning in June and one false warning in July during the system scan of clean files by Kaspersky. This is still a very good result as the industry average is at 3 (June) resp. 5 (July). When it comes to the slow-down of the system by the security software, Kaspersky was slightly heavier than the industry

average with an impact of 16 compared to 15. Lower numbers mean less impact and are therefore better.

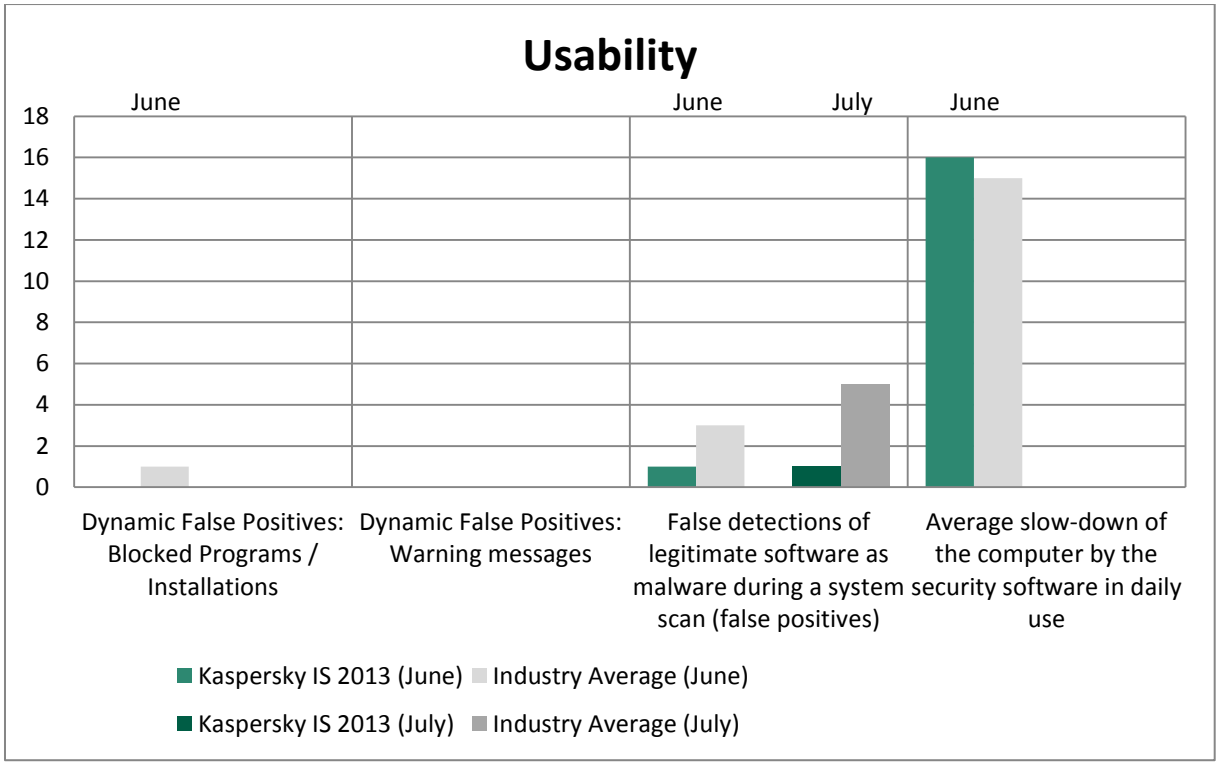

Figure 3: Usability

Despite the excellent protection and repair capabilities of Kaspersky which are far better than the average, it triggered nearly no false positives and is only very slightly heavier than the industry average.

Summarized, Kaspersky Internet Security 2013 is a very good allround product, without any weak spot, but with many strong points and providing results that are far better than the industry average.