



Anti-Malware Testing Standards Organization

AMTSO REVIEW ANALYSIS COMMITTEE FINAL REPORT

SUBJECT: DENNIS TECHNOLOGY LABS “PC VIRUS PROTECTION 2010 II” TEST REPORT

Review Published: 26-Oct-2009

Review Analysis proposed by: Simon Edwards, Dennis Technology Labs

Review Analysis Approved by Review Analysis Board: 6-May-2010

Review Analysis Committee:

David Harley, ESET

David Perry, Trend Micro

John Hawes, Virus Bulletin

Jong Purisima, Webroot

Chairperson and liaison: Alice Decker, Trend Micro

FINDINGS ON COMPLIANCE WITH AMTSO PRINCIPLES

Principle #1

Testing must not endanger public

The test was performed without creation of new malware and samples used during the test were not made publicly available. During gathering and validation of samples some degree of external exposure was unavoidable, but this was closely monitored and manually interrupted at the first sign of malicious activity. These measures were mentioned briefly in the report and described in more depth to the committee, and were considered more than reasonable precautions to avoid unnecessary risk and protect the community.

The committee found that the test complied with Principle #1.

Principle #2

Testing must be unbiased

The test was sponsored or commissioned by the vendors of one of the products under test, but the tester was apparently given complete independence in the methodology design and implementation. The test environment, the selection of samples and products, and the configuration and operation of products appeared to be well balanced and not to favour any particular vendor or product.

The report contained incomplete information on the configuration of the products in the test – the committee was informed that all products used their default settings and were given access to all external resources required for full operation. While this may be deduced from context we would advise testers to include full and explicit details of configuration protocols as a standard component of any test report. More details of sample selection criteria may also form a useful addition to reports.

The committee found that the test complied with Principle #2.

Principle #3

Testing should be reasonably open and transparent

The test report was found to be reasonably detailed. It contained at least basic information on the solutions tested, although it might have been useful to have more detailed data on product versions, and also on how the products were obtained for the test (whether submitted by vendors or downloaded/purchased without vendor knowledge or approval). A reasonable level of information was also provided on the testing environments used, on how samples were obtained, validated and presented during the tests, on the setup and operation of the products, and on the interpretation of results.

The committee found that the test complied with Principle #3.

Principle #4

The effectiveness and performance of anti-malware products must be measured in a balanced way.

Some differences were observed in the capabilities of the solutions tested, and the committee debated the selection of free products in comparison to suites even when all vendors offer full suite solutions. However, the choice of products is discussed and justified in the report, and all products showed themselves to offer sufficiently similar functionality to warrant direct comparison.

All products were tested in an equal manner and, while some subjectivity may have influenced the design of the final scoring system, the system used seemed reasonable, was clearly described and was applied evenly to all solutions.

The committee found that the test complied with Principle #4.

Principle #5

Testers must take reasonable care to validate whether test samples or test cases have been accurately classified as malicious, innocent or invalid.

The report details some of the steps taken to check the samples used were appropriate, and the committee was provided with further details of these measures. From this evidence it seems clear that reasonable care was taken in both the selection and validation of samples to ensure accurate classification.

The committee found that the test complied with Principle #5.

Principle #6

Testing methodology must be consistent with the testing purpose.

The report makes the objective of the test clear from the outset, and provides reasonable details of the methodology implemented; along with further details provided to the committee, this approach appears to support the stated purpose. The decision to use default settings throughout is intended to reflect the assumed norm among users of consumer-grade products, and the committee debated the appropriateness of using default settings in some circumstances, particularly when sample sets include 'grey' material which may be approached differently by different vendors. In this case however, the use of defaults appears to be appropriate given the selection of samples and the test methodology.

The committee found that the test complied with Principle #6.

Principle #7**The conclusions of the test must be based on the test results**

The report contained a large amount of data on specific test cases and results obtained from visual observation, but the absence of internal information on product logging and analysis of test systems meant that in some cases the results were rather difficult for the reader to interpret accurately. More details on the data gathered but not published were given to the committee in discussion with the tester, and the difficulties involved in displaying all the data in an easily-digestible manner were clear.

In drawing conclusions, the report did not appear to omit, misinterpret, or otherwise distort the results obtained, and drew logical conclusions based on the full set of data. The conclusions followed the selected interpretation system accurately and fairly reflected the stated intentions of the test.

The committee found that the test complied with Principle #7.

Principle #8**Test results should be statistically valid**

The results as presented provided ample information on the samples used and the relative performance of products in the test. While there were some areas of the report open to misinterpretation, it appeared to accurately apply all results recorded in the calculation of final ratings.

The type of test methodology used does not readily allow for extremely large and broad selections of test samples, which would give a more accurate reflection of products' true protective capabilities against the entire malware threat. However, the sample size was considered respectable for this type of test, and the results accurately reflected the performance of the products against the samples used.

The committee found that the test complied with Principle #8.

Principle #9**Vendors, testers and publishers must have an active contact point for testing-related correspondence.**

No information was found in the report concerning interaction with the vendors of the products tested, however the test body is a well-known and active member of the AMTSO group, provides ample contact information on their website and responded promptly and helpfully to all committee communications. Furthermore no issues were reported by any of the vendors participating in the test during the consultation period.

The committee found that the test complied with Principle #9.