westcoast labs

September 2008

McAfee

Anti-Malware Detection Rates

Comparative Testing

McAfee Anti-Malware Detection Rates Comparative Testing

Vendor Details

Vendor Name:

McAfee

Vendor Address:

Dr.Solomons Software Ltd, Alton House, Gatehouse Way, Buckinghamshire, Aylesbury, HP19 8YD

Vendor Telephone Number: Guy Roberts, Avert Labs, 0789 423 0095

Product: McAfee Anti-Malware solution and competitor products

WCL Corporate Offices and Test Facilities

US 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

Test Facilities also in Hong Kong and Sydney, Australia.

Date: 8th September 2008 **Issue**: 1.3

Author: Michael Parsons

Contact Telephone Number: +44 (0) 2920 548 400

McAfee Anti-Malware Detection Rates Comparative Testing

Contents

Introduction 4

Products tested 5

Test Structure 6

Test Methodology 7

Test Results 9

Conclusion 11

West Coast Labs Disclaimer 12

McAfee Anti-Malware Detection Rates Comparative Testing

Introduction

Following discussions between McAfee and West Coast Labs (WCL), a comparative test of anti-malware products was prepared.

WCL evaluated the detection rates of 10 retail Anti-Malware products over a large number of malware samples provided by both WCL (50,000+ samples) and McAfee (100,000+ samples). Each sample set was analysed and reported on separately so as not to skew any results, although combined results were also calculated. WCL also provided a collection of clean files for False Positive testing.

The primary objectives of these tests were to evaluate and validate the On Demand scanning detection rates of the 9 Anti-Malware solutions with new detection technology currently under development by McAfee.

All testing was conducted at West Coast Labs' UK test facilities in Cardiff during the month of May of 2008.

McAfee Anti-Malware Detection Rates Comparative Testing

Products Tested

The Products included in the test programme were as follows:

- McAfee VirusScan 12.1 with Artemis technology
- AhnLab Internet Security 2008 7.6.1.1
- Avira AntiVirus 8.1.00.295
- ESET NOD 32 AntiVirus 3.0.650.0
- Kaspersky AntiVirus 7.0.0.125
- Microsoft OneCare 2.0.2500.22
- Rising AntiVirus 2008 20.42.40
- Sophos AntiVirus 7.3.0
- Symantec Internet Security 15.5.0.23
- Trend Internet Security Professional 2008 16.10.1106

All products were updated on 2nd May 2008.

McAfee Anti-Malware Detection Rates Comparative Testing

Test Structure

The overall test program facilitated meaningful evaluation of detection rates over a large number of samples for those products chosen by McAfee.
The samples were split between McAfee supplied and WCL supplied.

The WCL supplied samples consisted of current malware with selections taken from the WCL sample sets including WCL's global honeynet.

The WCL samples were selected from those collected over a 12 month period preceding the testing.

The McAfee sample was selected from collections provided by other AV companies to represent a global distribution of malware threats assembled from all regions worldwide.

WCL also produced a small sample set which was added to both the McAfee and WCL malware test suites, to measure False Positive detection rates.

McAfee Anti-Malware Detection Rates Comparative Testing

Test Methodology

Each product was installed using base options onto a clean image of Windows Vista Home Edition. The products were then updated on the same day to the latest patch version available on that day.

The malware collections were then subjected to On Demand Scans (ODS) in accordance with the appropriate procedure for each product. Two scans were run for each product, the first using default settings and the second designed to effect the maximum possible detection by that particular product.

Each machine was isolated from the Internet during the testing with the exception of the McAfee product (featuring the Artemis technology which was under development at the time this test was conducted), which required full access to the Internet to check against the McAfee servers.

McAfee Anti-Malware Detection Rates Comparative Testing

Test Methodology (Contd.)

Results are reported on as percentages against the complete sample range in each test suite. To produce accurate results, three procedures were followed:

- Files reported detected were divided by the number of files scanned, giving a % detection rate.
- A check was then made that the difference between the total number of files scanned and the reported deletions tallied with the remainder of the files in the directory.
- A separate count was made of those samples that had been detected as false positives.

McAfee Anti-Malware Detection Rates Comparative Testing

Test Results

False Positive Detection

No files were falsely identified as being malware.

WCL collection

A total of 51263 unique files were supplied by West Coast Labs for this test.

Detection rates were recorded under default detection settings and also under maximum detection settings.

	Default detection		Maximum detection	
Sophos	50158	97.84%	50158	97.84%
Avira	49518	96.60%	49639	96.83%
McAfee	49459	96.48%	49459	96.48%
Kaspersky	46872	91.43%	47566	92.79%
Symantec	46452	90.62%	46452	90.62%
ESET	43564	84.98%	44449	86.71%
Trend	42961	83.81%	42961	83.81%
Microsoft	41972	81.88%	41972	81.88%
AhnLab	36827	71.84%	36827	71.84%
Rising	34799	67.88%	34799	67.88%
Industry Average	44258.2	86.34%	44428.2	86.67%

McAfee Anti-Malware Detection Rates Comparative Testing

Test Results (Contd.)

McAfee collection
A total of 105324 unique files supplied by McAfee were used for this test. Other samples provided were removed from the collection as being duplicated within the WCL collection.

Detection rates were recorded under both default and maximum detection settings.

	Default detection			**Maximum detection**	
Avira	105222	99.90%	Avira	105254	99.93%
McAfee	105158	99.84%	McAfee	105158	99.84%
Sophos	104242	98.97%	Sophos	104242	98.97%
Microsoft	104158	98.89%	Microsoft	104158	98.89%
Symantec	104055	98.80%	Symantec	104055	98.80%
Rising	103325	98.10%	ESET	103398	98.17%
ESET	103144	97.93%	Rising	103325	98.10%
Kaspersky	102454	97.28%	Kaspersky	102908	97.71%
Trend	102032	96.87%	Trend	102032	96.87%
AhnLab	93603	88.87%	AhnLab	93603	88.87%
Industry Average	102739.3	97.54%	Industry Average	102813.3	97.62%

McAfee Anti-Malware Detection Rates Comparative Testing

Test Results (Contd.)

Combined collection (weighted average)

A total of 156587 unique files were used for the two tests. This shows the combined results.

	Default detection			Maximum detection	
Avira	154740	98.82%	Avira	154893	98.92%
McAfee	154617	98.74%	McAfee	154617	98.74%
Sophos	154400	98.60%	Sophos	154400	98.60%
Symantec	150507	96.12%	Symantec	150507	96.12%
Kaspersky	149326	95.36%	Kaspersky	150474	96.10%
ESET	146708	93.69%	ESET	147847	94.42%
Microsoft	146130	93.32%	Microsoft	146130	93.32%
Trend	144993	92.60%	Trend	144993	92.60%
Rising	138124	88.21%	Rising	138124	88.21%
AhnLab	130430	83.30%	AhnLab	130430	83.30%
Industry Average	146997.5	93.88%	Industry Average	147241.5	94.03%

McAfee Anti-Malware Detection Rates Comparative Testing

Conclusion

McAfee's new technology proved its abilities, producing very creditable results. It detected over 96% of the files in the WCL collection and over 99% of those in the McAfee collection. Of the other products, only Avira surpassed its detection rates in both collections, with Sophos outdoing it in one but not in the other.

Comparative detection rates were generally higher in the McAfee collection than in the WCL collection, and were probably influenced by the respective origins of those collections.

McAfee Anti-Malware Detection Rates Comparative Testing

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.

Revision History

Issue	Description of Changes	Date Issued
1.0	McAfee Anti-Malware Detection Rates Comparative Testing	29th May 2008
1.1	McAfee Anti-Malware Detection Rates Comparative Testing	3rd July 2008
1.2	Renaming and relocation of results as agreed	3rd September 2008
1.3	Artemis name reinstated	8th September 2008

westcoast labs

US SALES
T +1 (717) 243 5575

EUROPE SALES
T +44 (0) 2920 548400

CHINA SALES
T +86 1 343 921 7464

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

Test Facilities also in Hong Kong and Sydney, Australia

E info@westcoast.com
W www.westcoastlabs.com