McAfee Advanced Threat Defense Test

A test commissioned by Intel Security and performed by AV-TEST GmbH

Date of the report: July 10, 2014

Executive Summary

During May and June 2014 AV-TEST performed a test of the McAfee Advanced Threat Defense appliance to determine its malware detection capabilities. The appliance showed great performance detecting 99.96% overall and no less than 99.5% in any single tested malware category. It also had a minimum of false positive detections at 0.01%.

Overview

With the increasing number of threats that are being released and are spreading through the Internet these days, the risk of being infected is increasing as well. A few years back there were new viruses released every few days. This has now grown to several thousand new threats per hour.

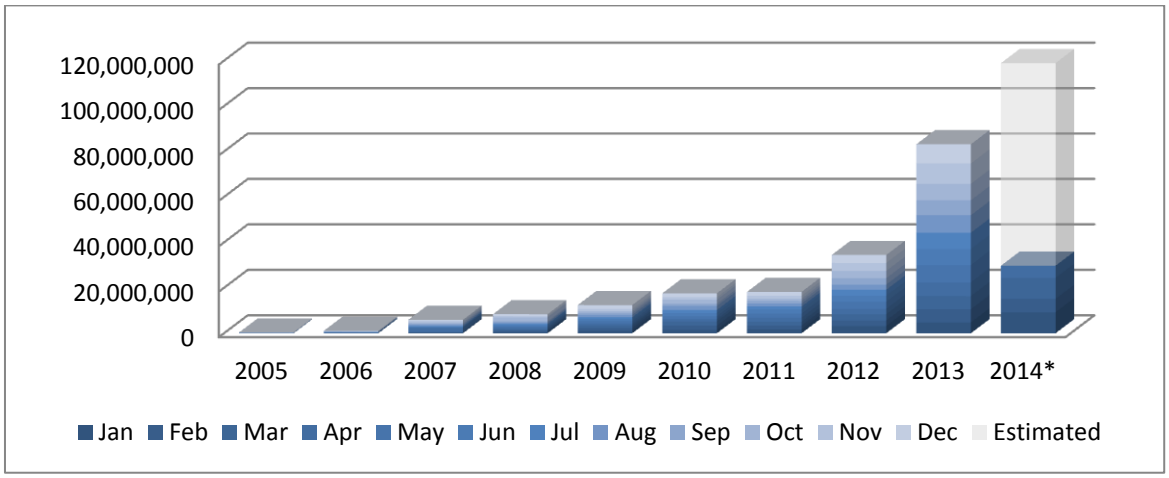

Figure 1: New samples added per year

In 2000, AV-TEST received more than 170,000 new samples; but by 2013 the number of new samples grew to more than 80,000,000. The number of new samples received during 2014 continues to grow with over 20 million new samples already in the first quarter. This growth is seen in Figure 1.

The enormous number of samples makes it impossible to create a valid signature for each file, especially when care is needed to avoid false positives. If a unique signature was needed for each file (e.g. by using a hash like SHA256), the signature databases grow too large to be usable. On the other hand, if the signatures are made too generic, so that a single signature could identify all files of a malware family, the risk is high that clean files would be erroneously matched as well, causing a higher false positive rate.

In the last few years new detection techniques were developed to handle this problem, including behavioral analysis and sandboxing techniques. The McAfee Advanced Threat Defense appliance combines all of these advanced detection techniques, making it a comprehensive tool for malware protection and analysis.

Products Tested

Product	Version
McAfee Advanced Threat Defense	3.0.4.83.38479

Table 1: Product tested

An Intel Security engineer assisted AV-TEST in the setup of the test environment.

Methodology and Setup

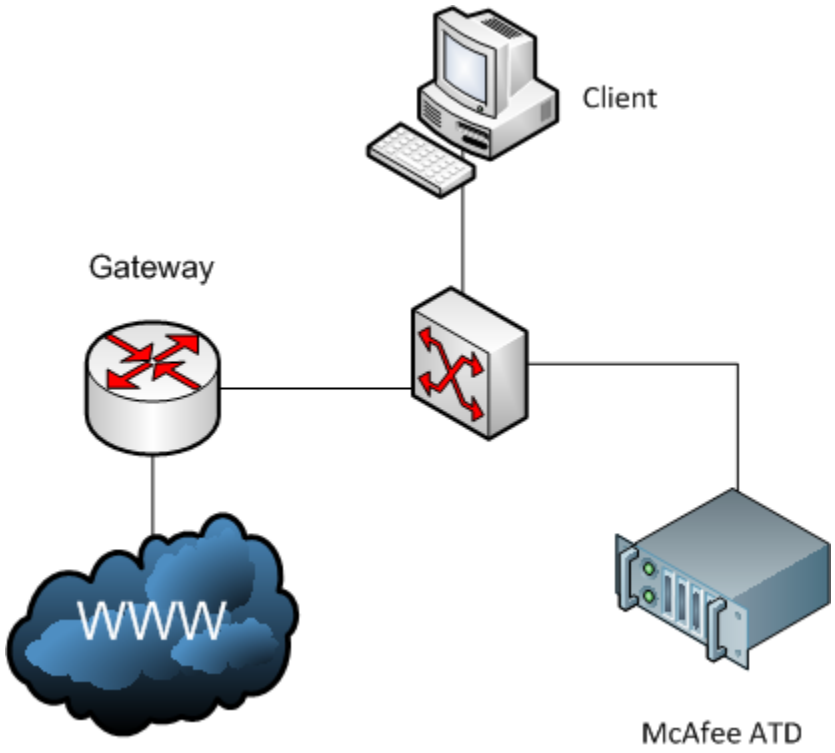

Figure 2: Test environment scheme

As the McAfee Advanced Threat Defense appliance is not capable of downloading URLs on its own (it would typically partner with an IPS or web gateway for this) it was connected to a client PC, which used the REST interface of the appliance to upload the test samples for analysis. Each sample was uploaded one by one and the appliance had several seconds to analyze the sample. McAfee Advanced Threat Defense includes several detection methods, including static and dynamic techniques. Many files were detected in less computationally expensive methods, meaning results returned in less than a second and dynamic analysis was not needed to convict.

Samples

The samples used in this test consisted of the AV-TEST reference set of 12,132 prevalent malware samples; 131,871 malware zoo samples; 4,752 malicious PDF documents; and 7,616 malicious Microsoft Office documents to determine the detection capabilities, as well as 96,722 clean files for false positive testing.

Test Results

Malware Detection

Using multiple analysis techniques the McAfee Advanced Threat Defense appliance performed well over all malware categories with an overall detection rate of more than 99.96%.

The detailed results are listed in Table 2.

Sample Set	Number of Samples	Detected Samples	Detection Rate
Prevalent Malware	12,132	12,125	99.94%
Zoo Malware	131,871	131,851	99.98%
PDF Documents	4,752	4,731	99.56%
Microsoft Office Documents	7,616	7,608	99.89%
Overall	**156,371**	**156,315**	**99.96%**

Table 2: Malware detection results

False Positives

A high detection rate is only good in combination with a low false positive rate. Therefore AV-TEST uploaded 96,722 clean files to the McAfee Advanced Threat Defense appliance to determine its false positive rate.

Only 5 files were flagged with the highest malware score of 5 points and 2 files were flagged with a malware score of 3 points. The malware score indicates the risk of a file. Every file with a score above 2 points is considered unwanted or malicious.

The detailed results are listed in Table 3.

Sample Set	Number of Samples	Detected Samples	Detection Rate
False Positives	96,722	7	0.01%

Table 3: False positive test results

Conclusion

The McAfee Advanced Threat Defense appliance from Intel Security is a flexible extension to a corporate security infrastructure as it is highly effective in identifying advanced malware. It can be directly integrated with several Intel Security products, including McAfee Network Security Platform, McAfee Web Gateway, and McAfee Email Gateway.

Copyright © 2014 by AV-TEST GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web http://www.av-test.org