McAfee Network Security Platform 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 conducted an evaluation of the McAfee Network Security Platform appliance to determine its real signature-less detection capabilities. In order to accomplish this, McAfee Network Security Platform was configured with all available detection capabilities (both signatures and signature-less) enabled and subjected to an extensive battery of malware. McAfee Network Security Platform was then immediately reconfigured to disable IPS signatures, so only signature-less capabilities remained, and was then subjected to the same battery of malware. AV-TEST saw no significant difference in the detection rates between these different configurations.

Overview

With the increasing number of threats that are being released and spreading through the Internet these days, the danger of getting infected is increasing as well. A few years back, a new virus was released only once every few days. Today, several thousand new threats are released per hour.

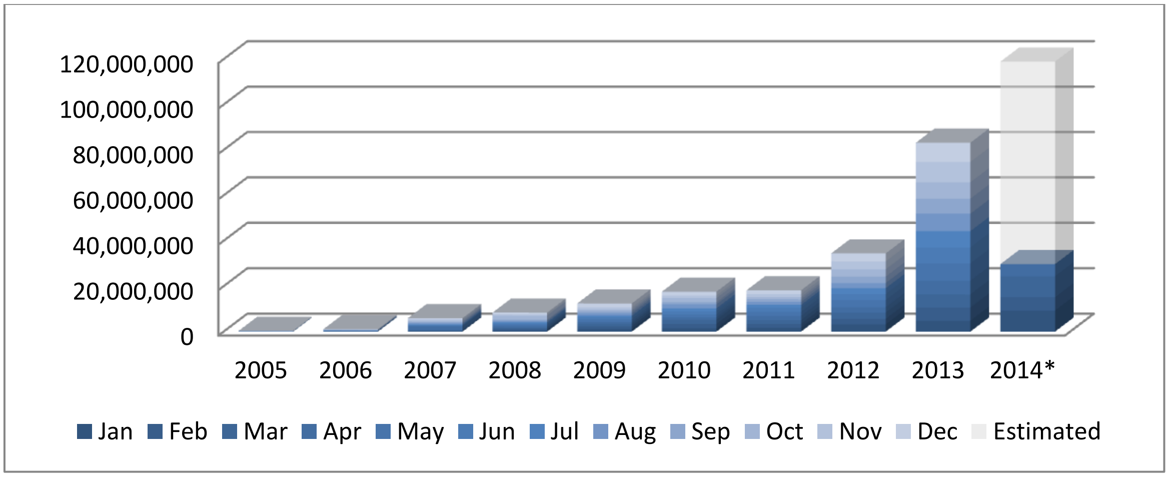

Figure 1: New samples added per year

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. The growth of these numbers is displayed in Figure 1.

The McAfee Network Security Platform is designed with extensible modules, like the Network Threat Behavioral Analysis appliance or the Advanced Threat Defense appliance, in order to support the latest detection technologies and defend against the increasing number of cyber attacks.

Products Tested

Product	Version
McAfee Network Security Platform	8.1.3.10
McAfee Advanced Threat Defense	3.0.4.83.38479

Table 1: Products tested

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

Methodology and Setup

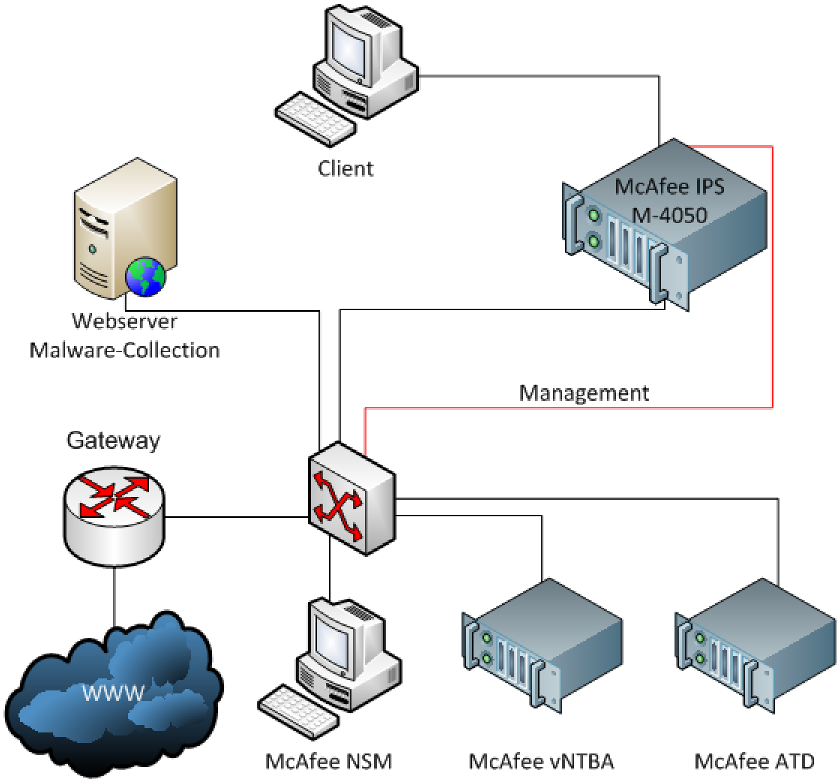

Figure 2: Test environment scheme

The complete setup consisted of a McAfee IPS M-4050 appliance, a McAfee Network Security Manager server, a McAfee Network Threat Behavioral Analysis appliance and a McAfee Advanced Threat Defense appliance. The test sets were stored on a local web server. The client made HTTP GET requests to each malware sample on the web server. The requests were transparently passed through the IPS appliance, which analyzed the response – the sample download.

The platform was configured with two protection policies. The first policy tested had all available IPS signatures enabled (policy 1 – all IPS signatures enabled) and the second policy had all IPS signatures disabled (policy 2 – IPS signatures disabled). Static malware signatures were always active to enable the forwarding of files to all signature-less engines (not pattern matching signatures). The policies were tested one after the other.

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

The malware detection rates of both tested policies were equal. Table 2 shows the detailed results which were achieved with both policies. With at least 99.6% in all categories the detection rates are very good, independently from the type of malware which was tested.

Sample Set	Number of Samples	Detected Samples	Detection Rate
All IPS Signatures enabled	**156,371**	**156,339**	**99.98%**
Prevalent Malware	*12,132*	*12,129*	*99.98%*
Zoo Malware	*131,871*	*131,865*	*99.995%*
PDF Documents	*4,752*	*4,736*	*99.66%*
Microsoft Office Documents	*7,616*	*7,609*	*99.91%*
IPS Signatures disabled	**156,371**	**156,339**	**99.98%**
Prevalent Malware	*12,132*	*12,129*	*99.98%*
Zoo Malware	*131,871*	*131,865*	*99.995%*
PDF Documents	*4,752*	*4,736*	*99.66%*
Microsoft Office Documents	*7,616*	*7,609*	*99.91%*

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 passed 96,722 clean files through the Network Security Platform appliance to determine its false positive rate.

In Policy 1 (all IPS signatures enabled) only 4 files triggered a false positive, with the highest malware score of 6 points and 3 files triggered a false positive with a malware score of 4 points. In Policy 2 (IPS signatures disabled) only 2 files triggered a false positive with a malware score of 6 points.

The malware score indicates the risk of a file. Every file with a score above 3 points is considered unwanted or malicious.

The detailed results are listed in Table 3.

Sample Set	Number of Samples	Detected Samples	Detection Rate
All IPS Signatures enabled	96,722	7	0.01%
IPS Signatures disabled	96,722	2	0.00%

Table 3: False positive test results

Conclusion

The McAfee Network Security Platform from Intel Security is a modular and extensible solution for a corporate security infrastructure. Though we endorse following Intel Security's recommendation not to run for extended periods of time with IPS signatures disabled, this test shows that McAfee Network Security Platform's signature-less capabilities alone (IPS signatures disabled) are able to detect the majority of malware samples in the network with a minimum of false positives.