Proactive Rootkit Protection Comparison Test

A test commissioned by McAfee and performed by AV-TEST GmbH

Date of the report: February 25th, 2013

Executive Summary

In January 2013, AV-TEST performed a comparative review of McAfee Deep Defender, Microsoft System Center Endpoint Protection and Symantec Endpoint Protection to determine their capabilities to pro-actively protect against kernel-mode and MBR rootkits, so called day zero attacks. Two individual tests have been performed. The first was a test that used frozen updates (from October 1st 2012) to perform the test against 48 rootkits that were discovered after that date. The second test was done with disabled on-access components, so that only behavioral detection was in place against 48 rootkits as well.

To perform the test runs, a clean Windows 7 image was used on several identical PCs. On this image, the security software was installed. Access to the cloud was disabled for all products, in order to prevent any static detection and test the protection against new, unknown threats for which there is no signature. The rootkits have then been executed and any detections from the security product were noted. In Test 2, not only the detection but also the protection/remediation has been tested. If a disinfection/blocking routine was started, then this was executed as part of the test as well. Finally the resulting system state has been captured to determine whether the rootkit was successfully blocked.

While 'retrospective' tests are not always considered a wholly accurate form of testing, they do nonetheless provide a simulation of zero day proactive protection and are much simpler to run in a controlled manner than attempting to discover and test zero day threats (especially rootkits) as they are delivered into the wild. As such, this style of test can provide a useful baseline for information purposes.

The result of this test shows, that the pro-active approach of McAfee Deep Defender is capable of providing a very good level of protection against kernel-mode and MBR rootkits. It detected and successfully blocked all 48 tested rootkits in the test. None of the other products was able to match this result. See details of the test results in the table below.

	Reference	McAfee Deep Defender	Microsoft System Center Endpoint Protection	Symantec Endpoint Protection
Detected rootkits (Test 1)	48	48	40	32
Detected rootkits (Test 2)	48	48	Not tested	20
Remediated rootkits (Test 2)	48	48	Not tested	18

Overview

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

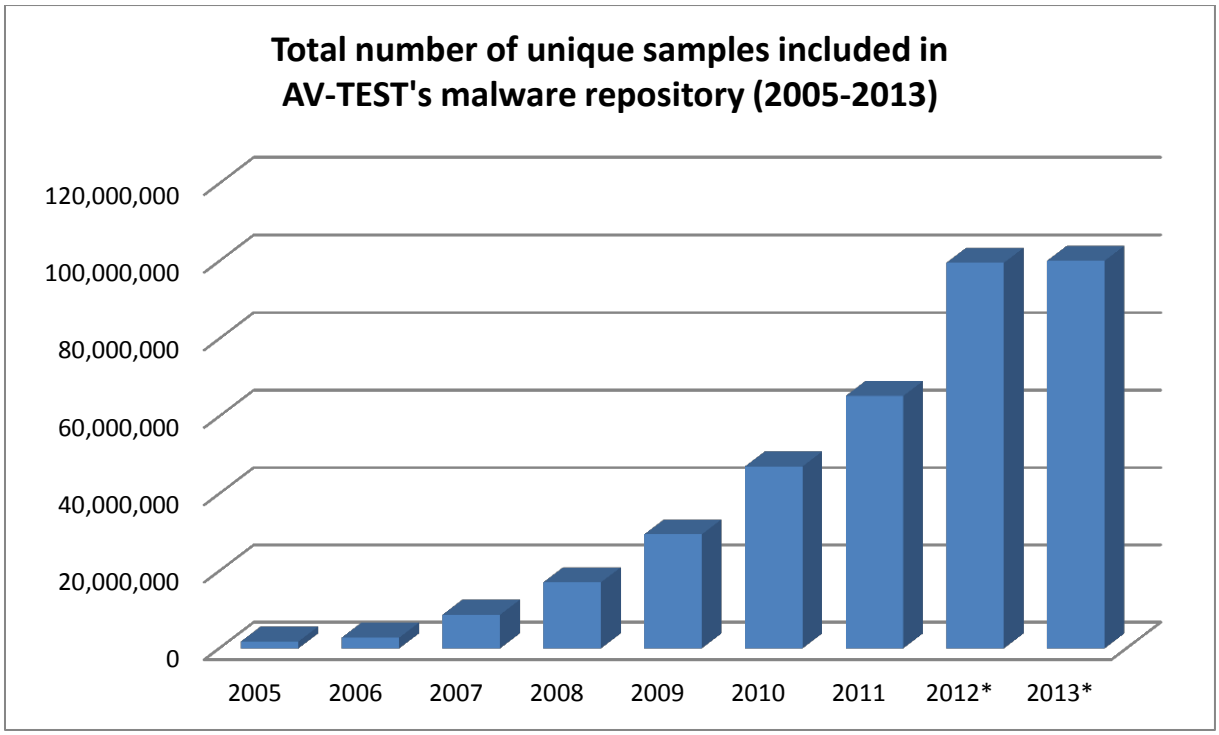

Figure 1: New samples added per year

In early 2013 the AV-TEST collection of malware exceeded 100.000.000 unique samples and the growth rates are getting worse and worse. In the year 2000, AV-TEST received more than 170,000 new samples, and in 2010 and 2011, the number of new samples grew to nearly 20,000,000 samples each. The numbers continue to grow with about 35 million new files in 2012 alone.

These growth rates clearly show the need for pro-active protection measures, as static protection is not good enough to protect against all threats. This is especially important for rootkits, since it becomes a lot harder to detect them once they are successfully installed on the system. McAfee Deep Defender is a product that aims to protect here using McAfee DeepSAFE technology operating beyond the operating system, designed to detect, block and remediate advanced stealth attacks.

Products Tested

The testing occurred in January 2013. AV-TEST used the latest releases available at the time of the test of the following products:

- McAfeeDeep Defender 1.5.0.399
- Microsoft System Center 2012 Endpoint Protection
- Symantec Endpoint Protection 12.1

Methodology and Scoring

Platform

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

- Intel i7-3770 3,4Ghz CPU
- 16 GB DDR3 1600-Ram
- 480 GB SATA III SSD (Intel)

The operating system was Windows 7 Ultimate, SP1 in default settings.

Testing methodology

General

1. **Clean system for each sample**. The test systems should be restored to a clean state before being exposed to each malware sample.
2. **Physical Machines**. The test systems used should be actual physical machines. No Virtual Machines were used.
3. **Product Cloud/Internet Connection**. Products were not allowed to query to cloud (in order to prevent static detection).
4. **Product Configuration**. All products were run with their default, out-of-the-box configuration, despite for Test 2 where the on-access detection has been switched off.
5. **Sample Cloud/Internet Accessibility**. If the malware uses the cloud/Internet connection to reach other sites in order to download other files and infect the system, care should be taken to make sure that the cloud access is available to the malware sample in a **safe** way such that the testing network is not under the threat of getting infected.
6. **Allow time for sample to run**. Each sample should be allowed to run on the target system for 10 minutes to exhibit autonomous malicious behavior. This may include initiating connections to systems on the internet, or installing itself to survive a reboot.

The procedures below are carried out on all tested programs and all test cases at the same time in order to ensure that all protection programs have the exact same test conditions. If a test case is no longer working or its behavior varies in different protection programs (which can be clearly determined using the Sunshine analyses), the test case is deleted. This ensures that all products were tested in the exact same test scenarios. All test cases are solely obtained from internal AV-TEST sources and are always fully analyzed by AV-TEST. We never resort to using test cases or analyses provided by manufacturers or other external sources.

Test 1

1. The products are installed and signatures are dated back to October 1st 2012. Products are started up using standard/default settings.
2. AV-TEST attempts to execute the rootkit with Administrator rights
3. If execution is blocked, this is documented
4. If execution is not blocked, the system will be rebooted
5. If further detections occur this will be documented
6. If no detection occurred it is verified that the rootkit successfully infected the system

Test 2

1. The products are installed and updated. Products are started with disabled on-access protection.
2. AV-TEST attempts to execute the rootkit with Administrator rights
3. If execution is blocked, this is documented
4. If execution is not blocked, the system will be rebooted
5. If further detections occur this will be documented
6. If no detection occurred it is verified that the rootkit successfully infected the system
7. If there was a detection it is documented whether the rootkit was successfully disabled/blocked

The malware set for both tests consisted of 48 kernel-mode and MBR rootkits collected in the time frame between October 1st and January 31st. The 48 rootkits were from 23 different families.

Test Results

The results of the first test (Figure 2) show that McAfee Deep Defender was able to detect all 48 rootkits used in the test, while Microsoft failed to detect 8 out of them and Symantec didn't detect 15.

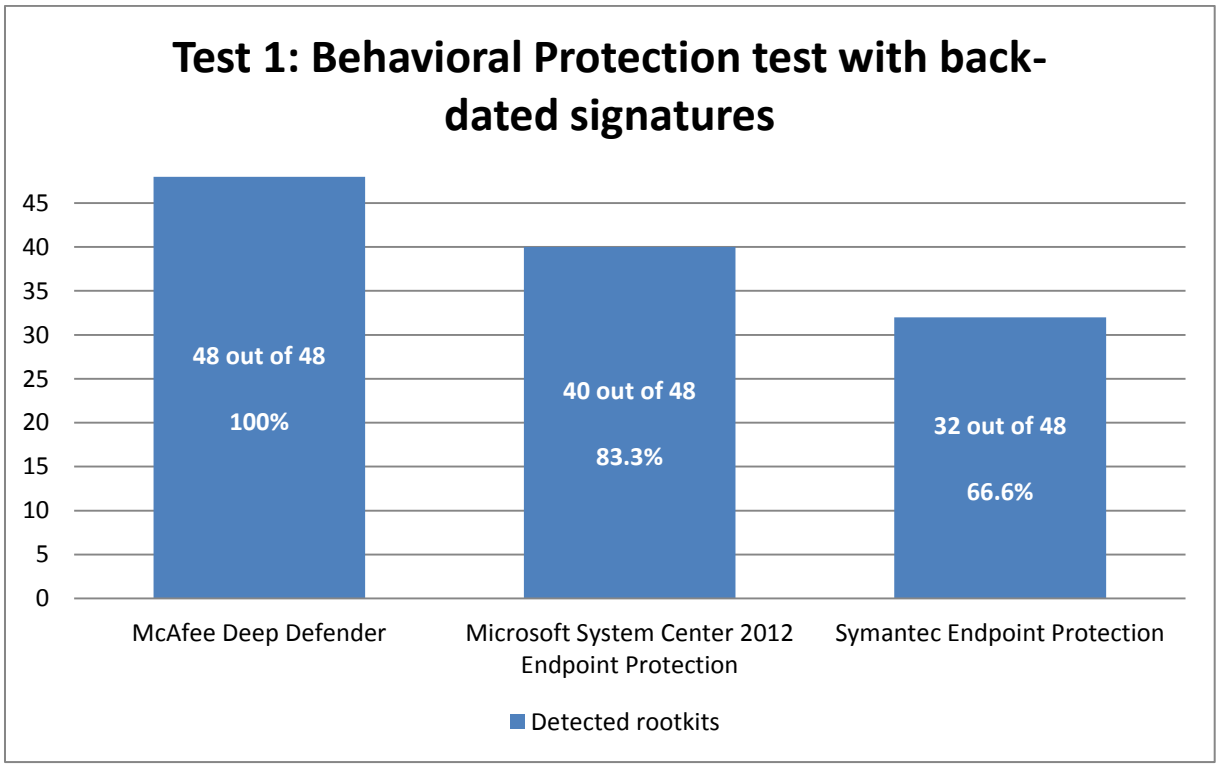

Figure 2: Test 1 Behavioral Protection test with back-dated signatures

These results show that the pro-active (non signature dependent) approach of Deep Defender is indeed capable of providing a very good detection level against current high profile rootkits. The results of Microsoft and Symantec also show where these products have their strengths. Microsoft relies a lot on generic signatures (which allow detection of samples from the same family, even without prior knowledge of all specific samples) and is able to detect 40 out of 48 rootkits even if they haven't seen them before thanks to their generic signatures. Symantec on the other hand relies a lot on cloud lookups and reputation. Since this was not allowed during the test, their results are lower than Microsoft's. The detections that occurred were partly because of generic signatures, but heuristic and behavioral detections as well.

The results of test 2 show a similar picture. Deep Defender again is able to detect against all 48 rootkits. Symantec managed to detect 20 rootkits. The problem for Symantec is again that they rely a lot on their cloud which was not allowed in this test. So these detections are solely from heuristic/behavioral components. While the cloud adds another layer of security and helps in many cases, it may not be available all the time. Either because there are problems on the vendor side, in the local network or because the malware disables or limits access to the internet. It was not possible to include the Microsoft product in this test, since it is not possible to just disable the on-access guard and leave the behavior guard enabled.

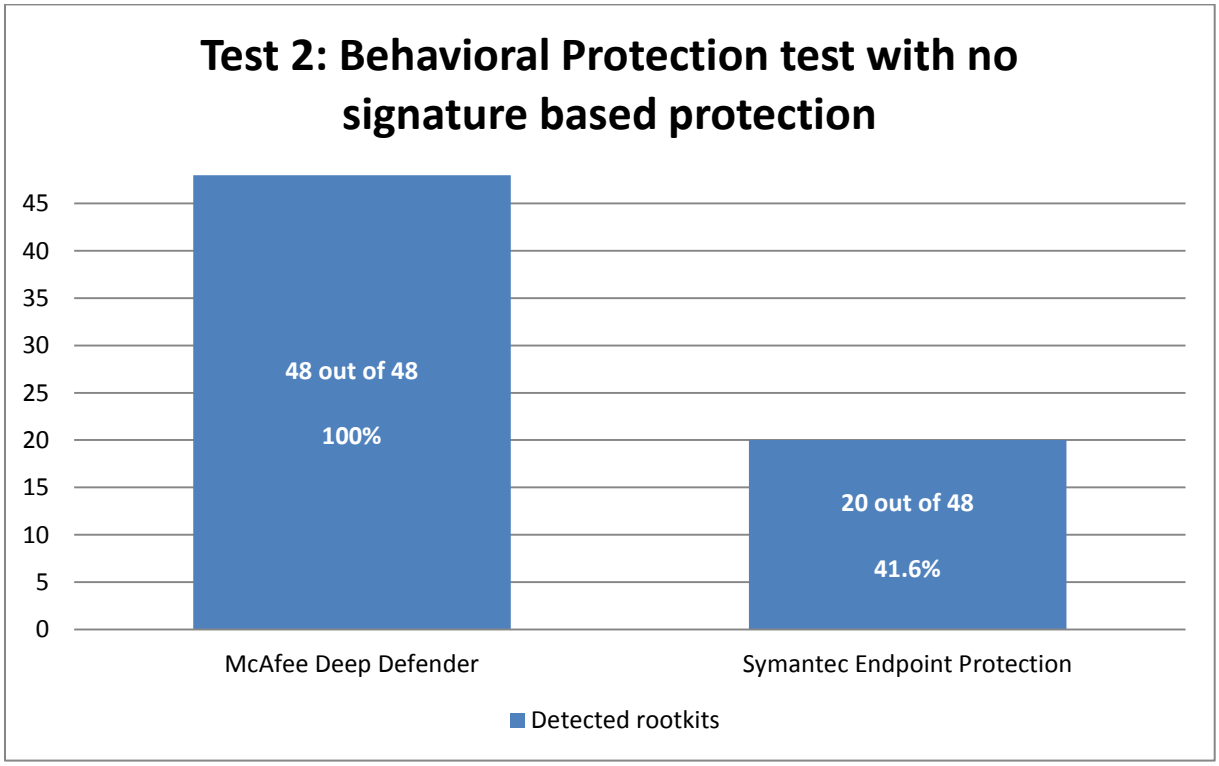

Figure 3: Test 2 Behavioral Protection test with no signature based protection (Detection)

Further to the detection part it was also checked whether the installation of the rootkit was indeed prevented resp. if the detection took place after the installation if the the rootkit was successfully disabled. The results are shown in Figure 4.

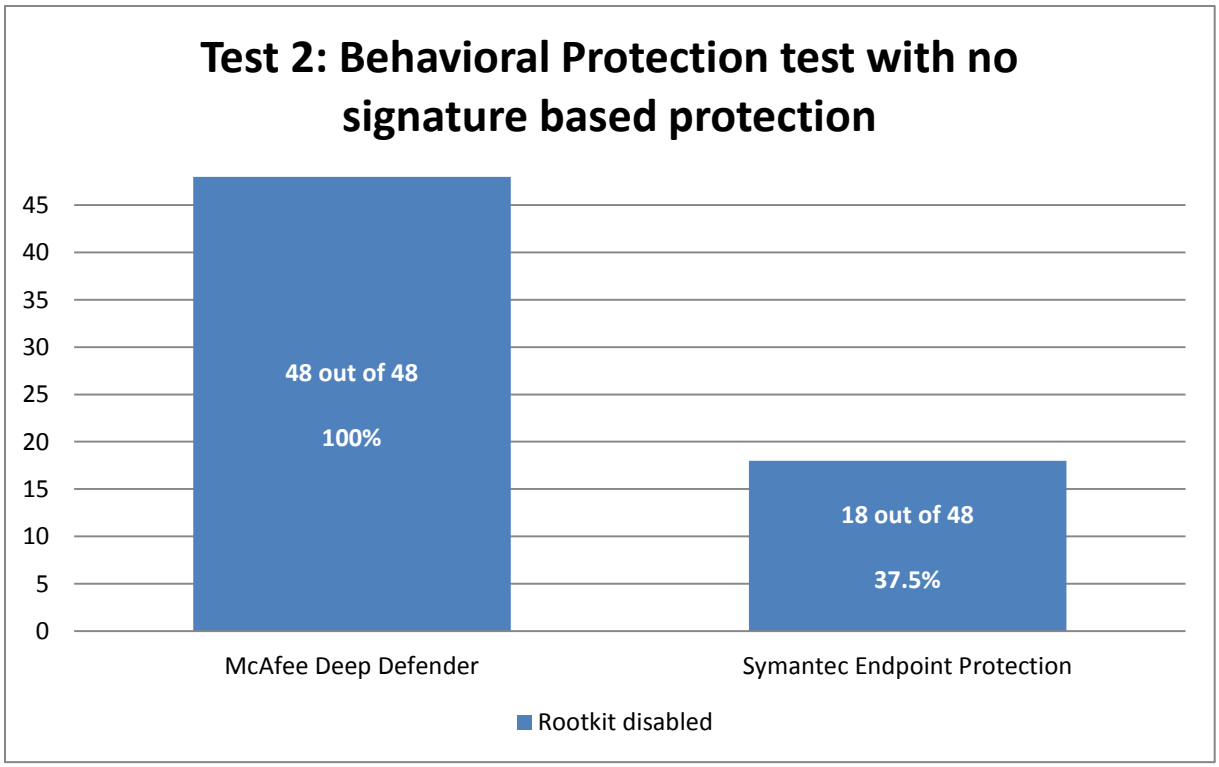

Figure 4: Test 2 Behavioral Protection test with no signature based protection (Removal)

McAfee was able to successfully block/remediate all rootkits that they detected. For McAfee several detections took place during the installation of the rootkit, which is more difficult to deal with, but Deep Defender still managed to block/remediate all tested rootkits. In case of Symantec two detected rootkits were not successfully disabled. This is because the behavioral detection took place during or after installation where the rootkit already has control over the system and this makes it more difficult to deal with the threats.

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version
McAfee	Deep Defender	1.5.0.399
Microsoft	Microsoft System Center 2012 Endpoint Protection	2.2.903.0
Symantec	Symantec Endpoint Protection	12.1.2015.2015