Webroot SecureAnywhere AntiVirus Malware Detection Certification

Q4 2016

Contents

Introduction 3
Executive Summary 3
Tests Employed 4
Malware sample types used to conduct the tests 5
Full Spectrum Test Results 6
Appendix 1 7
Methodology Used in the Webroot SecureAnywhere AntiVirus Certification 7

Introduction

This assessment measured the ability of a security product to protect an endpoint from a live infection, and, in the event of a system being compromised, the time taken to detect the infection and remediate the system.

The methodology employed in this test maps more closely to Real World use, and although it may not be a 100% accurate model of how an "average" system is used, it gives a more realistic assessment of a security product's ability to detect and remediate an infected endpoint.

This test deals with the full spectrum of malware like trojans, backdoors, ransomware, PUAs, financial malware and "other" malware are used.

MRG Effitas is a member of AMTSO (Anti-Malware Testing Standards Organization, Inc.)

Executive Summary

Webroot SecureAnywhere AntiVirus 9.0.13.62 was tested in this report.

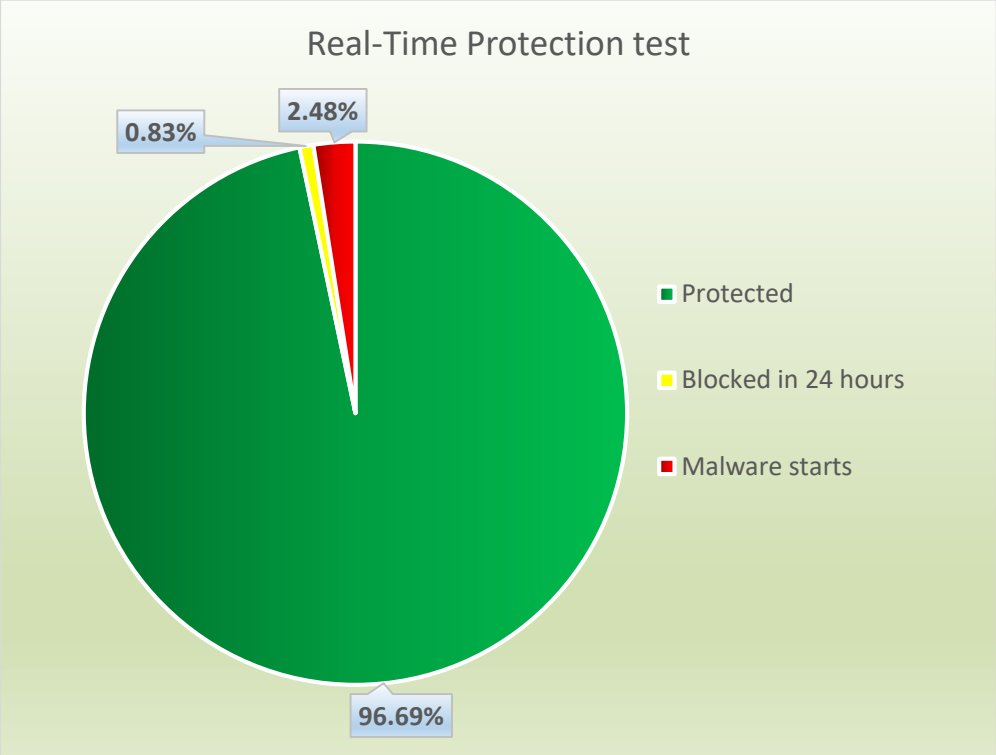
In total, 363 live malware has been tested.

MRG Effitas certifies the ability of Webroot SecureAnywhere AntiVirus to detect malware.

Test date: 11 November 2016 – 21 December 2016.

Certificate number: 2016122101

This certificate is valid until: 2017 December 21



Tests Employed

For us, a product's ability to block initial infection (although critical in most cases) is not the only metric that matters. One also needs to measure the time taken for the security product to detect malware on a system and remediate it.

When conducting these tests, we tried to simulate normal user behaviour. We are aware that a "Real World" test cannot be conducted by a team of professionals inside a lab because we understand how certain types of malware work, how malware attacks and how such attacks could be prevented. Simulating normal user behaviour means that we paid special attention to all alerts given by security applications. A pass was given only when alerts were straightforward and clearly suggested that malicious action should be blocked.

In this assessment, we ran the following test:

In the Wild - Full Spectrum Test

Approximately 50% of the malicious URLs used in this test were compromised legitimate websites which served malware. We believe that such URLs pose the greatest danger to users as this is the place where they least expect to get infected. 10% of the URLs pose as fake porn websites serving visitors with various types of malware. The remaining 40% of the URLs come from our regular honeypots or, in case of ransomware and financial malware in particular, we used URLs from newly-discovered distribution sites.

Malware delivered by URLs used in this test can be considered as Zero Day in the true meaning of that phrase. This posed a great challenge to all participants as new variant samples such as Locky (Ransomware) TeslaCrypt (Ransomware), Dridex (Banking Trojan) and many others caused most damage.

It is our opinion that Ransomware currently poses the greatest threat to users, for this reason we choose to use more URLs serving this threat than before.

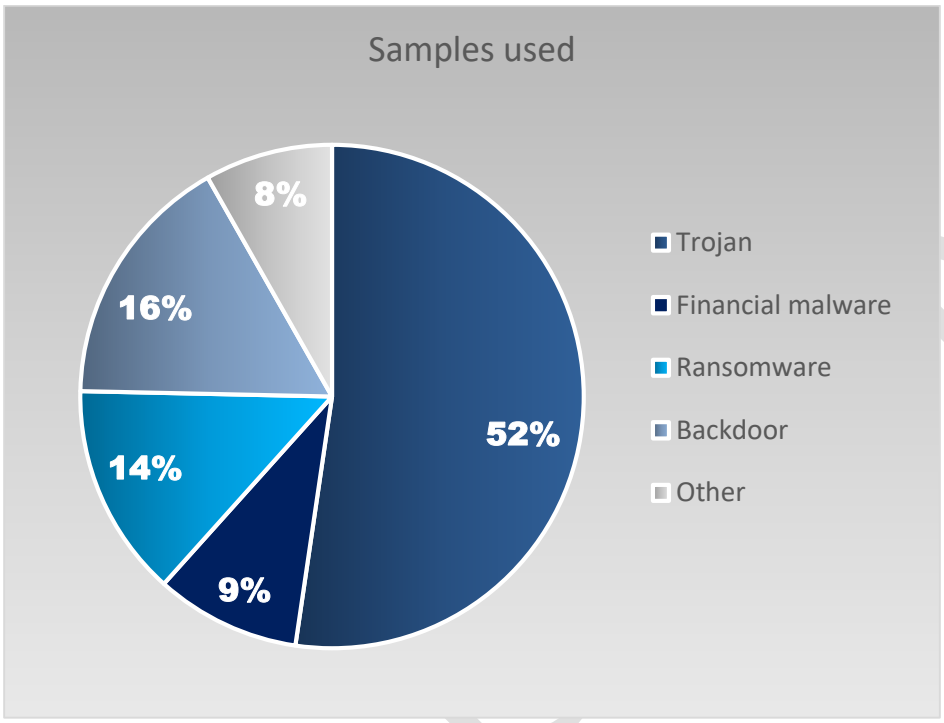
Because of the wide spectrum of malware used in this project and the freshness of the samples, we used a smaller set than usual.

Our testing environment supports the use of VM aware malware, this is the reason why we were able to use more sophisticated threats which wouldn't run on Virtual Machines.

10% of the threats used in this test were introduced to the system via USB flash memory sticks. These samples came originally from live URLs, but inside archives.

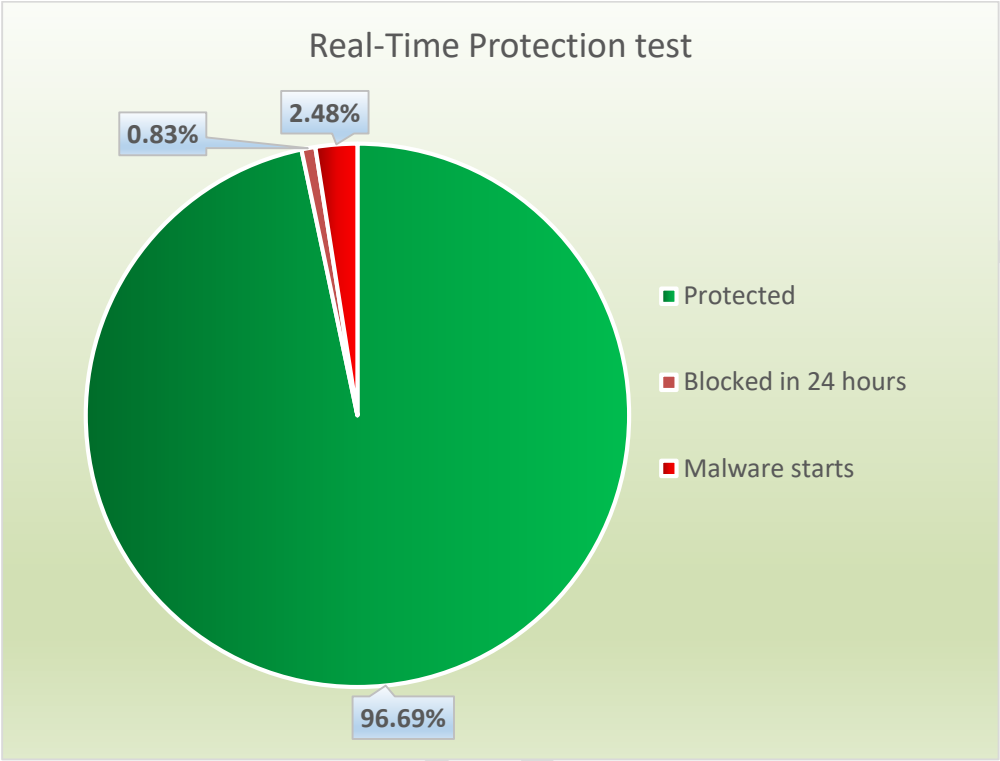
Testing was conducted as per the methodology detailed in Appendix 1. In total, 363 live ITW samples were used. The stimulus load comprised the following: 189 trojans, 59 backdoors, 35 financial malware samples, 49 ransomware samples, and 31 others.

Malware sample types used to conduct the tests.



Full Spectrum Test Results

The table below shows the initial detection rates of the security product.



Appendix 1
Methodology Used in the Webroot SecureAnywhere AntiVirus Certification

Methodology used in the assessment:

1. Windows 10 64 bit operating system was installed on a virtual machine[i], all updates were applied and third party applications installed and updated according to our "Average Endpoint Specification"[ii]
2. An image of the operating system was created.
3. A clone of the imaged systems was made for the security applications used in the test.
4. An individual security application was installed using default settings[iii] on each of the systems created in 3. and then, where applicable, updated.
5. A clone of the system as at the end of 4. was created.
6. Each live URL test was conducted by:
    a. Downloading a single malicious binary from its native URL using Microsoft Edge to the desktop, closing Microsoft Edge and then executing the binary.
    b. The security application blocked the URL where the malicious binary was located.
    c. The security application detected and blocked the malicious binary whilst it was being downloaded to the desktop.
    d. The security application detected the malicious binary when it was executed according to the following criteria:

        It identified the binary as being malicious and either automatically blocked it or postponed its execution and warned the user that the file was malicious and awaited user input.
7. The system under test was deemed to have been infected if:

    The security application failed to detect or block the binary at any stage in 6. and allowed it to be executed.
8. Testing on infected systems continued for 24 hours. The system was rescanned once, exactly 24 hours after the system was compromised.
9. Remediation performance of an application was determined by manual inspection of the system in contrast to its pre-infected state and not by the logs and reports of the security application itself.[iv]
10. Testing was conducted with all systems having internet access.
11. Each individual test for each security application was conducted from a unique IP address.
12. All security applications were fully-functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.
13. All testing was conducted during Q4 2016.
14. As no user initiated scans were involved in this test, applications relied on various technologies to detect, block and remediate threats. Some of these technologies were: background scanning, startup scanning, scheduled scanning, system monitors, etc. A scheduled scan was used only if enabled by default.

[i] VM hardware spec is 4GB RAM & 2 core processor.
[ii] AES includes Adobe Flash, Reader, Java, Microsoft Office 2010, Edge & VLC Player. All Microsoft components were fully updated; all third-party components were out of date by three months.
[iii] During installation of the security application, if an option to detect PUAs was given, it was selected.
[iv] This is because in some instances, an application will claim to have removed an infection, but actually failed to do so and was still active on the system.