

Proactive Security Challenge report

June 11, 2009

Tested product: Malware Defender 2.2.2
Product vendor: TorchSoft
Testing platform: Windows XP Service Pack 3
Number of tests: 84

Level reached: 10+
Total score: **89 %**

Introduction

This report presents results of *the Tested product* in the series of tests known as [Proactive Security Challenge](#). All the information regarding these tests, testing methodology and scoring system is available on [the website of this project](#). Reports of the commercial testing usually contain results of all available levels, reports of the public testing usually contain results of the first level and the following levels up to the highest level reached by the tested product. Public testing results are always published on the project's website, while the results of commercial testing are published only after the consent of the paying customer. The total score is always calculated as if the report was public.

Note that the number of levels, the number of tests or even the tests implementation may change. The report's results are valid at the day of the report's release and are not guaranteed to be valid after that day.

Testing results

Level 1

Level up: 50 %
Product's score: 100 %

Test name	Result	Comment
Breakout2	100 %	PASSED
Coat	100 %	PASSED
ECHOTest	100 %	PASSED
Kill1	100 %	PASSED
Kill2	100 %	PASSED
Leaktest	100 %	PASSED
Tooleaky	100 %	PASSED
Wallbreaker1	100 %	PASSED
Yalta	100 %	PASSED

Level 2

Level up: 50 %

Product's score: 100 %

Test name	Result	Comment
AWFT1	100 %	PASSED
DNSstest	100 %	PASSED
Ghost	100 %	PASSED
Jumper	100 %	PASSED
Kill3	100 %	PASSED
Kill3b	100 %	PASSED
Kill6	100 %	PASSED
Wallbreaker3	100 %	PASSED
Wallbreaker4	100 %	PASSED

Level 3

Level up: 50 %

Product's score: 90 %

Test name	Result	Comment
AWFT3	100 %	PASSED
AWFT4	100 %	PASSED
DNSstester	0 %	FAILED
Kernel1	100 %	PASSED
Kill3f	100 %	PASSED
Kill4	100 %	PASSED
Kill7	100 %	PASSED
SSS2	100 %	PASSED
Suspend1	100 %	PASSED
Thermite	100 %	PASSED

Level 4

Level up: 50 %
Product's score: 100 %

Test name	Result	Comment
CopyCat	100 %	PASSED
CPIL	100 %	PASSED
CPILSuite1	100 %	PASSED
Kernel1b	100 %	PASSED
Keylog1	100 %	PASSED
Kill3e	100 %	PASSED
Kill8	100 %	PASSED
Kill9	100 %	PASSED
SSS	100 %	PASSED
Suspend2	100 %	PASSED

Level 5

Level up: 50 %
Product's score: 100 %

Test name	Result	Comment
Breakout1	100 %	PASSED
CPILSuite2	100 %	PASSED
Crash1	100 %	PASSED
Crash2	100 %	PASSED
Crash3	100 %	PASSED
Crash4	100 %	PASSED
Kernel2	100 %	PASSED – See the further notes at the end of the report.
Kernel3	100 %	PASSED
Keylog2	100 %	PASSED
Kill3c	100 %	PASSED
Kill3d	100 %	PASSED
VBStest	100 %	PASSED

Level 6

Level up: 50 %

Product's score: 85 %

Test name	Result	Comment
CPILSuite3	100 %	PASSED
Crash5	100 %	PASSED
Crash6	100 %	PASSED
DDEtest	100 %	PASSED
ECHOTest2	0 %	FAILED
FireHole	100 %	PASSED
Flank	0 %	FAILED
Kernel4	100 %	PASSED
Keylog3	100 %	PASSED
Keylog4	100 %	PASSED
Kill10	100 %	PASSED
Kill11	100 %	PASSED
Runner	100 %	PASSED

Level 7

Level up: 50 %

Product's score: 72 %

Test name	Result	Comment
BITStest	0 %	FAILED
FireHole2	100 %	PASSED
Keylog5	100 %	PASSED
Keylog6	100 %	PASSED
Kill12	100 %	PASSED
OSfwbypass	0 %	FAILED
Runner2	100 %	PASSED
Schedtest	100 %	PASSED
SSS3	50 %	FAILED – Unwanted system reboot was not prevented.

Level 8Level up: **50 %**Product's score: **63 %**

Test name	Result	Comment
Kernel4b	100 %	PASSED
Kernel5	100 %	PASSED
Keylog7	100 %	PASSED
Kill5	100 %	PASSED
NewClass	0 %	FAILED – See the further notes at the end of the report.
Schedtest2	0 %	FAILED – See the further notes at the end of the report.
SockSnif	0 %	FAILED
SSS4	100 %	PASSED

Level 9Level up: **50 %**Product's score: **50 %**

Test name	Result	Comment
Crash7	0 %	FAILED
Driver Verifier	100 %	PASSED

Level 10Level up: **100 %**Product's score: **100 %**

Test name	Result	Comment
BSODhook	100 %	PASSED
ShadowHook	100 %	PASSED

Further notes

Malware Defender passes Kernel2 test because the user has a chance to block the attack in a popup window, which contains the name of the driver to be loaded. However, the information provided in the popup window by Malware Defender may mislead the user because verified Microsoft system application "services.exe" is mentioned as the source process. However, Malware Defender fails NewClass when its code is slightly modified not to use "cmd.exe" to run "explorer.exe" but to run Internet Explorer directly. In this case, Malware Defender does not protect against the test's technique but it fights only its specific implementation. Similarly, Malware Defender fails Schedtest2.