Proactive Security Challenge report

August 27, 2011

Tested product: **BitDefender Internet Security 2011 14.0.30.357**
Product vendor: BitDefender
Testing platform: Windows XP Service Pack 3, Internet Explorer 8
Number of tests: 148

Level reached: 10+
Total score: **97 %**

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

Number of tests: **12**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun1	100 %	**PASSED**
Autorun3	100 %	**PASSED**
Breakout2	100 %	**PASSED**
Coat	100 %	**PASSED**
ECHOtest	100 %	**PASSED**
FileDel2	100 %	**PASSED**
Kill1	100 %	**PASSED**
Kill2	100 %	**PASSED**

Leaktest	100 %	**PASSED**
Tooleaky	100 %	**PASSED**
Wallbreaker1	100 %	**PASSED**
Yalta	100 %	**PASSED**

Level 2

Number of tests: **16**
Level up: **50 %**
Product's score: **94 %**

Test name	Result	Comment
Autorun12	100 %	**PASSED**
Autorun2	100 %	**PASSED**
Autorun20	100 %	**PASSED**
Autorun30	100 %	**PASSED**
AWFT1	100 %	**PASSED**
DNStest	100 %	**PASSED**
FileMov2	100 %	**PASSED**
Ghost	100 %	**PASSED**
HostsBlock	100 %	**PASSED**
Jumper	100 %	**PASSED**
Kill3	100 %	**PASSED**
Kill3b	100 %	**PASSED**
Kill6	100 %	**PASSED**
RegDel1	0 %	**FAILED**
Wallbreaker3	100 %	**PASSED**
Wallbreaker4	100 %	**PASSED**

Level 3

Number of tests: **17**
Level up: **50 %**
Product's score: **88 %**

Test name	Result	Comment
Autorun16	100 %	**PASSED**
Autorun24	100 %	**PASSED**
Autorun31	100 %	**PASSED**
Autorun4	100 %	**PASSED**

AWFT3	100 %	**PASSED**
AWFT4	100 %	**PASSED**
DNStester	100 %	**PASSED**
FileRep1	100 %	**PASSED**
Kernel1	100 %	**PASSED**
Kill3f	100 %	**PASSED**
Kill4	100 %	**PASSED**
Kill7	100 %	**PASSED**
RegSet1	0 %	**FAILED**
SSS2	0 %	**FAILED** – See the further notes at the end of the report.
Suspend1	100 %	**PASSED**
Thermite	100 %	**PASSED**
Wallbreaker2	100 %	**PASSED**

Level 4

Number of tests: **20**
Level up: **50 %**
Product's score: **95 %**

Test name	Result	Comment
Autorun14	100 %	**PASSED**
Autorun17	100 %	**PASSED**
Autorun26	100 %	**PASSED**
Autorun36	100 %	**PASSED**
Autorun37	100 %	**PASSED**
Autorun6	100 %	**PASSED**
Autorun9	100 %	**PASSED**
CopyCat	100 %	**PASSED**
CPIL	100 %	**PASSED**
CPILSuite1	100 %	**PASSED**
FileRep2	100 %	**PASSED**
Inject2	100 %	**PASSED**
Inject3	100 %	**PASSED**
Kernel1b	100 %	**PASSED**
Keylog1	100 %	**PASSED**
Kill3e	100 %	**PASSED**
Kill8	100 %	**PASSED**
Kill9	100 %	**PASSED**
SSS	0 %	**FAILED** – See the further notes at the end of the report.

Suspend2	100 %	**PASSED**

Level 5

Number of tests: **20**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun15	100 %	**PASSED**
Autorun18	100 %	**PASSED**
Autorun21	100 %	**PASSED**
Autorun28	100 %	**PASSED**
Autorun5	100 %	**PASSED**
Breakout1	100 %	**PASSED**
CPILSuite2	100 %	**PASSED**
Crash1	100 %	**PASSED**
Crash2	100 %	**PASSED**
Crash3	100 %	**PASSED**
Crash4	100 %	**PASSED**
FileWri1	100 %	**PASSED**
Kernel2	100 %	**PASSED**
Kernel3	100 %	**PASSED**
Keylog2	100 %	**PASSED**
Kill3c	100 %	**PASSED**
Kill3d	100 %	**PASSED**
RegDel2	100 %	**PASSED**
Svckill	100 %	**PASSED**
VBStest	100 %	**PASSED**

Level 6

Number of tests: **20**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun22	100 %	**PASSED**
Autorun25	100 %	**PASSED**
Autorun27	100 %	**PASSED**

Autorun29	100 %	**PASSED**
Autorun32	100 %	**PASSED**
Autorun7	100 %	**PASSED**
CPILSuite3	100 %	**PASSED**
Crash5	100 %	**PASSED**
Crash6	100 %	**PASSED**
DDEtest	100 %	**PASSED**
ECHOtest2	100 %	**PASSED**
FileWri2	100 %	**PASSED**
FireHole	100 %	**PASSED**
Flank	100 %	**PASSED**
Kernel4	100 %	**PASSED**
Keylog3	100 %	**PASSED**
Keylog4	100 %	**PASSED**
Kill10	100 %	**PASSED**
Kill11	100 %	**PASSED**
Runner	100 %	**PASSED**

Level 7

Number of tests: **20**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun10	100 %	**PASSED**
Autorun19	100 %	**PASSED**
Autorun33	100 %	**PASSED**
Autorun35	100 %	**PASSED**
Autorun8	100 %	**PASSED**
BITStest	100 %	**PASSED**
Crash4b	100 %	**PASSED**
FileDel1	100 %	**PASSED**
FileMov1	100 %	**PASSED**
FileWri3	100 %	**PASSED**
FireHole2	100 %	**PASSED**
Inject1	100 %	**PASSED**
Keylog5	100 %	**PASSED**
Keylog6	100 %	**PASSED**
Kill12	100 %	**PASSED**

OSfwbypass	100 %	**PASSED**
RegAcc1	100 %	**PASSED**
Runner2	100 %	**PASSED**
Schedtest	100 %	**PASSED**
SSS3	100 %	**PASSED**

Level 8

Number of tests: **16**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun11	100 %	**PASSED**
Autorun13	100 %	**PASSED**
Autorun23	100 %	**PASSED**
Autorun34	100 %	**PASSED**
FileDel3	100 %	**PASSED**
FileOpn1	100 %	**PASSED**
FileOpn2	100 %	**PASSED**
Kernel4b	100 %	**PASSED**
Kernel5	100 %	**PASSED**
Kernel5b	100 %	**PASSED**
Keylog7	100 %	**PASSED**
Kill5	100 %	**PASSED**
NewClass	100 %	**PASSED**
Schedtest2	100 %	**PASSED**
SockSnif	100 %	**PASSED**
SSS4	100 %	**PASSED**

Level 9

Number of tests: **5**
Level up: **50 %**
Product's score: **80 %**

Test name	Result	Comment
Crash7	0 %	**FAILED**
Driver Verifier	100 %	**PASSED**
FileAcc1	100 %	**PASSED**

FileCtl1	100 %	**PASSED**
FileWri4	100 %	**PASSED**

Level 10

Number of tests: **2**
Level up: **100 %**
Product's score: **100 %**

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

Further notes

BitDefender failed SSS2 and SSS tests because its protection relies on the specific implementations of these tests. BitDefender does not protect against techniques of these tests. This was proved using slightly modified versions of these tests.

Although BitDefender passes many tests, the usability of the BitDefender's application behavior control is questionable. The problem with BitDefender is that in case of many techniques it gives absolutely no or very poor information about what is going on. Just a simple Allow/Block pop-up window is displayed without any or few details about the action to be blocked. Moreover, in case of many actions, “blocking an action” with BitDefender actually terminates the offending process instead of blocking the particular action. This also lowers the effectiveness of BitDefender's protection.