

Proactive Security Challenge 64 report

January 13, 2012

Tested product: **Comodo Internet Security Premium 5.9.219863.2196**
Product vendor: Comodo Security Solutions, Inc.
Testing platform: Windows 7 Service Pack 1, Internet Explorer 9
Number of tests: 110

Level reached: 11
Total score: **94 %**

Introduction

This report presents results of *the Tested product* in the series of tests known as [Proactive Security Challenge 64](#). All the information regarding these tests, the testing methodology and the scoring system is available on the website of this project.

Publicly available reports published on the project website contain results of the testing on the first level and the following levels up to the highest level reached by the tested product. Private reports for commercial based testing usually include results of tests on all levels regardless the level reached by the tested product. 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' implementations may change. The report results are valid at the day of the report's release and are not guaranteed to be valid after that day for any future version of the product or the testing suite.

How to interpret results

With its methodology Proactive Security Challenge 64 covers only some of many aspects that are relevant to the security of desktop computers running Windows OS. By no means the results presented in the reports or on the project's website should be interpreted as overall measure of the tested products quality or security. This project is strictly focused on testing features related to application-based security model and behavior blocking, sometimes such features of a security product are referred to as proactive protection features or HIPS features.

Proactive Security Challenge 64 especially does not evaluate the quality of non-behavioral pattern based or heuristic anti-virus or anti-malware scanning engines. It is also not designed to evaluate products that are built to protect only a single part of the system or just a few selected applications – this includes various Internet browser security add-ons, sandboxes or virtualizations, for example.

More information about methodology of testing and interpretation of results can be found on the project's website. All users of the this report are strongly encouraged to read further information on the project's website in order to avoid misinterpretations of the presented results.

Testing results

Level 1

Number of tests: **10**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun12	100 %	PASSED
Autorun3	100 %	PASSED
Autorun9	100 %	PASSED
Coat	100 %	PASSED
FileDel2	100 %	PASSED
Kill1	100 %	PASSED
Kill2	100 %	PASSED
Leaktest	100 %	PASSED
Tooleaky	100 %	PASSED
Yalta	100 %	PASSED

Level 2

Number of tests: **10**
Level up: **50 %**
Product's score: **90 %**

Test name	Result	Comment
Autorun15	100 %	PASSED
Autorun31	100 %	PASSED
Autorun7	100 %	PASSED
ECHOtest	100 %	PASSED
FileWri1	0 %	FAILED
Jumper	100 %	PASSED
Kill4	100 %	PASSED
Schedtest	100 %	PASSED
Suspend1	100 %	PASSED
Wallbreaker4	100 %	PASSED

Level 3

Number of tests: **10**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun10	100 %	PASSED
Autorun4	100 %	PASSED
AWFT4	100 %	PASSED
ECHOTest2	100 %	PASSED
FileDel1	100 %	PASSED
HostsBlock	100 %	PASSED
Keylog3	100 %	PASSED
Kill6	100 %	PASSED
RegDel1	100 %	PASSED
Suspend2	100 %	PASSED

Level 4

Number of tests: **10**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun19	100 %	PASSED
Autorun20	100 %	PASSED
Autorun37	100 %	PASSED
Crash1	100 %	PASSED
FileMov1	100 %	PASSED
Keylog4	100 %	PASSED
Kill9	100 %	PASSED
ProxyTest	100 %	PASSED
SSS2	100 %	PASSED
VBStest	100 %	PASSED

Level 5

Number of tests: **10**
Level up: **50 %**
Product's score: **90 %**

Test name	Result	Comment
Autorun24	100 %	PASSED
Autorun26	100 %	PASSED
Autorun29	100 %	PASSED
CopyCat	100 %	PASSED
Crash2	100 %	PASSED
DDExec	100 %	PASSED
FileWri2	0 %	FAILED – See the further notes at the end of the report.
Keylog7	100 %	PASSED
RegSet1	100 %	PASSED
Schedtest2	100 %	PASSED

Level 6

Number of tests: **10**
Level up: **50 %**
Product's score: **90 %**

Test name	Result	Comment
Autorun25	100 %	PASSED
Autorun28	100 %	PASSED
Autorun36	100 %	PASSED
Breakout1	100 %	PASSED
Crash3	100 %	PASSED
FileWri3	0 %	FAILED
FireHole2	100 %	PASSED
Inject2	100 %	PASSED
Keylog5	100 %	PASSED
SSS3	100 %	PASSED

Level 7

Number of tests: **10**
Level up: **50 %**
Product's score: **90 %**

Test name	Result	Comment
Autorun17	100 %	PASSED
Autorun23	100 %	PASSED
Autorun41	100 %	PASSED
Crash4	100 %	PASSED
FileCtl1	0 %	FAILED
FireHole	100 %	PASSED
Keylog6	100 %	PASSED
Kill8	100 %	PASSED
RegDel2	100 %	PASSED
Svckill	100 %	PASSED

Level 8

Number of tests: **10**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun38	100 %	PASSED
Autorun5	100 %	PASSED
Autorun8	100 %	PASSED
Crash5	100 %	PASSED
DDEtest	100 %	PASSED
FileDel3	100 %	PASSED
Flank	100 %	PASSED
NewClass	100 %	PASSED
Runner2	100 %	PASSED
SSS4	100 %	PASSED

Level 9

Number of tests: **10**
Level up: **50 %**
Product's score: **100 %**

Test name	Result	Comment
Autorun34	100 %	PASSED
Autorun43	100 %	PASSED
CPILSuite2	100 %	PASSED
Crash6	100 %	PASSED
DNStester	100 %	PASSED
FileMov2	100 %	PASSED
FileRep1	100 %	PASSED
Keylog1	100 %	PASSED
Kill12	100 %	PASSED
Schedtest3	100 %	PASSED

Level 10

Number of tests: **10**
Level up: **50 %**
Product's score: **80 %**

Test name	Result	Comment
Autorun39	100 %	PASSED
Autorun44	100 %	PASSED
Cliplog	100 %	PASSED
FileOpn2	100 %	PASSED
Inject1	0 %	FAILED – See the further notes at the end of the report.
Keylog2	100 %	PASSED
Kill3e	100 %	PASSED
OSfwbypass	100 %	PASSED
RegAcc1	100 %	PASSED
SockSnif	0 %	FAILED

Level 11

Number of tests: **10**
Level up: **100 %**
Product's score: **90 %**

Test name	Result	Comment
Autorun40	100 %	PASSED
Autorun42	100 %	PASSED
BITStest	100 %	PASSED
FileAcc1	0 %	FAILED
FileRep2	100 %	PASSED
Kill3f	100 %	PASSED
Kill5	100 %	PASSED
Schedtest4	100 %	PASSED
Screenlog	100 %	PASSED
WFPblock	100 %	PASSED

Further notes

All tests were executed outside the Comodo Internet Security's sandbox.

A minor modification of the FileWri2 test is needed in order to prove that Comodo Internet Security fails the test.

Comodo Internet Security failed Inject1 because it does not protect against the technique of this test. The protection was effective only against the specific implementation of this test. This was proved using a slightly modified version of Inject1.