

Proactive Security Challenge 64 report

December 1, 2011

Tested product: **Jetico Personal Firewall 2.1.0.10.2451**
Product vendor: Jetico Inc. Oy.
Testing platform: Windows 7 Service Pack 1, Internet Explorer 9
Number of tests: 110

Level reached: 10
Total score: **59 %**

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: **90 %**

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	0 %	FAILED

Level 2

Number of tests: **10**
Level up: **50 %**
Product's score: **60 %**

Test name	Result	Comment
Autorun15	100 %	PASSED
Autorun31	0 %	FAILED
Autorun7	100 %	PASSED
ECHOtest	0 %	FAILED
FileWri1	100 %	PASSED
Jumper	100 %	PASSED
Kill4	100 %	PASSED
Schedtest	0 %	FAILED – See the further notes at the end of the report.
Suspend1	100 %	PASSED
Wallbreaker4	0 %	FAILED – See the further notes at the end of the report.

Level 3

Number of tests: **10**
Level up: **50 %**
Product's score: **70 %**

Test name	Result	Comment
Autorun10	100 %	PASSED
Autorun4	100 %	PASSED
AWFT4	100 %	PASSED
ECHOTest2	0 %	FAILED
FileDel1	100 %	PASSED
HostsBlock	100 %	PASSED
Keylog3	0 %	FAILED
Kill6	100 %	PASSED
RegDel1	0 %	FAILED
Suspend2	100 %	PASSED

Level 4

Number of tests: **10**
Level up: **50 %**
Product's score: **60 %**

Test name	Result	Comment
Autorun19	100 %	PASSED
Autorun20	100 %	PASSED
Autorun37	100 %	PASSED
Crash1	100 %	PASSED
FileMov1	100 %	PASSED
Keylog4	0 %	FAILED
Kill9	100 %	PASSED
ProxyTest	0 %	FAILED – See the further notes at the end of the report.
SSS2	0 %	FAILED
VBStest	0 %	FAILED – See the further notes at the end of the report.

Level 5

Number of tests: **10**
Level up: **50 %**
Product's score: **60 %**

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

Level 6

Number of tests: **10**
Level up: **50 %**
Product's score: **70 %**

Test name	Result	Comment
Autorun25	100 %	PASSED
Autorun28	100 %	PASSED
Autorun36	100 %	PASSED
Breakout1	100 %	PASSED
Crash3	100 %	PASSED
FileWri3	100 %	PASSED
FireHole2	100 %	PASSED
Inject2	0 %	FAILED – See the further notes at the end of the report.
Keylog5	0 %	FAILED
SSS3	0 %	FAILED

Level 7

Number of tests: **10**
Level up: **50 %**
Product's score: **70 %**

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

Level 8

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

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	0 %	FAILED – See the further notes at the end of the report.
SSS4	100 %	PASSED

Level 9

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

Test name	Result	Comment
Autorun34	100 %	PASSED
Autorun43	0 %	FAILED
CPILSuite2	0 %	FAILED – See the further notes at the end of the report.
Crash6	100 %	PASSED
DNStester	0 %	FAILED
FileMov2	100 %	PASSED
FileRep1	100 %	PASSED
Keylog1	0 %	FAILED
Kill12	100 %	PASSED
Schedtest3	0 %	FAILED – See the further notes at the end of the report.

Level 10

Number of tests: **10**
Level up: **50 %**
Product's score: **30 %**

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

Level 11

Number of tests: **10**
Level up: **100 %**
Product's score: **NOT REACHED**

Further notes

Jetico failed Wallbreaker4, Schedtest, Schedtest2 and Schedtest3 because it does not prevent scheduling new tasks and manipulating trusted processes. Despite the current implementation of these tests and Jetico's "indirect relativeness" protection, the tests can be simply modified to schedule the attack after the reboot when the "indirect relativeness" protection is no longer effective.

Jetico failed ProxyTest because it is not able to prevent modification of proxy settings. Its "indirect relativeness" protection is effective only before reboot. Similarly, Jetico failed the DDExec test.

Jetico failed VBStest because it was able to protect only against the specific implementation of this test. Jetico does not protect against the technique of this test. This was proved using a slightly modified version of VBStest. Similarly, Jetico failed Inject2, Inject1, Runner2 and CPILSuite2 tests.

Although Jetico passes many tests, it is sometimes unusable if an action of a malicious program is blocked. It often happens with Jetico that the system must be rebooted to be usable again – e.g. the user can surf the web again. In case of a malware attack the usability of the system with Jetico might be quite low.