

# Proactive Security Challenge report

March 15, 2010

**Tested product:** Jetico Personal Firewall 2.1.0.7.2412  
**Product vendor:** Jetico Inc. Oy  
**Testing platform:** Windows XP Service Pack 3, Internet Explorer 8  
**Number of tests:** 148

**Level reached:** 4  
**Total score:** **28 %**

## 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:** 92 %

Test name	Result	Comment
Autorun1	100 %	<b>PASSED</b>
Autorun3	100 %	<b>PASSED</b>
Breakout2	100 %	<b>PASSED</b>
Coat	100 %	<b>PASSED</b>
ECHOTest	100 %	<b>PASSED</b>
FileDel2	0 %	<b>FAILED</b>
Kill1	100 %	<b>PASSED</b>
Kill2	100 %	<b>PASSED</b>

Leaktest	100 %	<b>PASSED</b>
Tooleaky	100 %	<b>PASSED</b>
Wallbreaker1	100 %	<b>PASSED</b>
Yalta	100 %	<b>PASSED</b>

## Level 2

**Number of tests:** 16  
**Level up:** 50 %  
**Product's score:** 56 %

Test name	Result	Comment
Autorun12	100 %	<b>PASSED</b>
Autorun2	100 %	<b>PASSED</b>
Autorun20	0 %	<b>FAILED</b>
Autorun30	0 %	<b>FAILED</b>
AWFT1	100 %	<b>PASSED</b>
DNStest	100 %	<b>PASSED</b>
FileMov2	0 %	<b>FAILED</b>
Ghost	100 %	<b>PASSED</b>
HostsBlock	0 %	<b>FAILED</b>
Jumper	0 %	<b>FAILED</b> – See the further notes at the end of the report.
Kill3	100 %	<b>PASSED</b>
Kill3b	100 %	<b>PASSED</b>
Kill6	100 %	<b>PASSED</b>
RegDel1	0 %	<b>FAILED</b>
Wallbreaker3	100 %	<b>PASSED</b>
Wallbreaker4	0 %	<b>FAILED</b> – See the further notes at the end of the report.

## Level 3

**Number of tests:** 17  
**Level up:** 50 %  
**Product's score:** 71 %

Test name	Result	Comment
Autorun16	0 %	<b>FAILED</b>
Autorun24	0 %	<b>FAILED</b>
Autorun31	0 %	<b>FAILED</b>
Autorun4	100 %	<b>PASSED</b>

AWFT3	100 %	<b>PASSED</b>
AWFT4	100 %	<b>PASSED</b>
DNSStester	100 %	<b>PASSED</b>
FileRep1	0 %	<b>FAILED</b>
Kernel1	100 %	<b>PASSED</b>
Kill3f	100 %	<b>PASSED</b>
Kill4	100 %	<b>PASSED</b>
Kill7	100 %	<b>PASSED</b>
RegSet1	0 %	<b>FAILED</b>
SSS2	100 %	<b>PASSED</b>
Suspend1	100 %	<b>PASSED</b>
Thermite	100 %	<b>PASSED</b>
Wallbreaker2	100 %	<b>PASSED</b>

**Level 4**

**Number of tests:** 20  
**Level up:** 50 %  
**Product's score:** 45 %

Test name	Result	Comment
Autorun14	0 %	<b>FAILED</b>
Autorun17	0 %	<b>FAILED</b>
Autorun26	0 %	<b>FAILED</b>
Autorun36	100 %	<b>PASSED</b>
Autorun37	0 %	<b>FAILED</b>
Autorun6	0 %	<b>FAILED</b>
Autorun9	0 %	<b>FAILED</b>
CopyCat	100 %	<b>PASSED</b>
CPIL	100 %	<b>PASSED</b>
CPILSuite1	100 %	<b>PASSED</b>
FileRep2	0 %	<b>FAILED</b>
Inject2	0 %	<b>FAILED</b>
Inject3	0 %	<b>FAILED</b>
Kernel1b	100 %	<b>PASSED</b>
Keylog1	0 %	<b>FAILED</b>
Kill3e	100 %	<b>PASSED</b>
Kill8	100 %	<b>PASSED</b>
Kill9	100 %	<b>PASSED</b>
SSS	0 %	<b>FAILED</b>

---

Suspend2	100 %	<b>PASSED</b>
----------	-------	---------------

### Level 5

Level up: 50 %  
Product's score: **Not reached**

### Level 6

Level up: 50 %  
Product's score: **Not reached**

### Level 7

Level up: 50 %  
Product's score: **Not reached**

### Level 8

Level up: 50 %  
Product's score: **Not reached**

### Level 9

Level up: 50 %  
Product's score: **Not reached**

### Level 10

Level up: 100 %  
Product's score: **Not reached**

## Further notes

Regardless the indirect access to network alert, Jetico failed Jumper test because it did not block rewriting Internet Explorer's start page. If Jumper is terminated before the user starts Internet Explorer's process, the browser is redirected without any alert. Similarly, Jetico failed Wallbreaker4. If Wallbreaker4 is terminated just after new task is scheduled the browser is redirected to the target page.

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