# Proactive Security Challenge report

August 19, 2011

**Tested product**: **ZoneAlarm Extreme Security 2012 10.0.250.000**
**Product vendor**: Check Point Software Technologies Ltd.
**Testing platform**: Windows XP Service Pack 3, Internet Explorer 8
**Number of tests**: 148

**Level reached**: 9
**Total score**: **72 %**

## 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**: **83 %**

| Test name | Result | Comment |
|---|---|---|
| Autorun1 | 100 % | PASSED |
| Autorun3 | 100 % | PASSED |
| Breakout2 | 100 % | PASSED |
| Coat | 100 % | PASSED |
| ECHOtest | 100 % | PASSED |
| FileDel2 | 0 % | FAILED |
| Kill1 | 100 % | PASSED |
| Kill2 | 100 % | PASSED |

| | | |
|---|---|---|
| Leaktest | 100 % | PASSED |
| Tooleaky | 0 % | FAILED |
| Wallbreaker1 | 100 % | PASSED |
| Yalta | 100 % | PASSED |

## Level 2

**Number of tests:** 16
**Level up:** 50 %
**Product's score**: 69 %

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

## Level 3

**Number of tests:** 17
**Level up:** 50 %
**Product's score**: 76 %

| 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 | 0 % | FAILED |
| Kernel1 | 100 % | PASSED |
| Kill3f | 0 % | FAILED |
| Kill4 | 100 % | PASSED |
| Kill7 | 100 % | PASSED |
| RegSet1 | 100 % | PASSED |
| SSS2 | 0 % | FAILED |
| Suspend1 | 100 % | PASSED |
| Thermite | 100 % | PASSED |
| Wallbreaker2 | 0 % | FAILED |

## Level 4

**Number of tests:** **20**
**Level up:** **50 %**
**Product's score**: **90 %**

| 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 | 0 % | FAILED |
| Inject2 | 100 % | PASSED |
| Inject3 | 100 % | PASSED |
| Kernel1b | 100 % | PASSED |
| Keylog1 | 100 % | PASSED |
| Kill3e | 100 % | PASSED |
| Kill8 | 100 % | PASSED |
| Kill9 | 100 % | PASSED |
| SSS | 0 % | FAILED |

| | | |
|---|---|---|
| Suspend2 | 100 % | PASSED |

## Level 5

**Number of tests:** 20
**Level up:** 50 %
**Product's score:** 75 %

| Test name | Result | Comment |
|---|---|---|
| Autorun15 | 100 % | PASSED |
| Autorun18 | 100 % | PASSED |
| Autorun21 | 100 % | PASSED |
| Autorun28 | 100 % | PASSED |
| Autorun5 | 0 % | FAILED |
| Breakout1 | 100 % | PASSED |
| CPILSuite2 | 100 % | PASSED |
| Crash1 | 100 % | PASSED |
| Crash2 | 100 % | PASSED |
| Crash3 | 100 % | PASSED |
| Crash4 | 100 % | PASSED |
| FileWri1 | 0 % | FAILED |
| Kernel2 | 100 % | PASSED |
| Kernel3 | 100 % | PASSED |
| Keylog2 | 100 % | PASSED |
| Kill3c | 0 % | FAILED |
| Kill3d | 0 % | FAILED |
| RegDel2 | 0 % | FAILED |
| Svckill | 100 % | PASSED |
| VBStest | 100 % | PASSED |

## Level 6

**Number of tests:** 20
**Level up:** 50 %
**Product's score:** 85 %

| Test name | Result | Comment |
|---|---|---|
| Autorun22 | 100 % | PASSED |
| Autorun25 | 0 % | FAILED |
| Autorun27 | 100 % | PASSED |

| | | |
|---|---|---|
| Autorun29 | 100 % | PASSED |
| Autorun32 | 100 % | PASSED |
| Autorun7 | 100 % | PASSED |
| CPILSuite3 | 100 % | PASSED |
| Crash5 | 100 % | PASSED |
| Crash6 | 0 % | FAILED |
| DDEtest | 100 % | PASSED |
| ECHOtest2 | 100 % | PASSED |
| FileWri2 | 0 % | FAILED |
| FireHole | 100 % | PASSED |
| Flank | 100 % | PASSED |
| Kernel4 | 100 % | PASSED |
| Keylog3 | 100 % | PASSED |
| Keylog4 | 100 % | PASSED |
| Kill10 | 100 % | PASSED |
| Kill11 | 100 % | PASSED |
| Runner | 100 % | PASSED – See the further notes at the end of the report. |

## Level 7

**Number of tests:** **20**
**Level up:** **50 %**
**Product's score**: **65 %**

| Test name | Result | Comment |
|---|---|---|
| Autorun10 | 100 % | PASSED |
| Autorun19 | 100 % | PASSED |
| Autorun33 | 100 % | PASSED |
| Autorun35 | 100 % | PASSED |
| Autorun8 | 0 % | FAILED |
| BITStest | 0 % | FAILED |
| Crash4b | 100 % | PASSED |
| FileDel1 | 0 % | FAILED |
| FileMov1 | 0 % | FAILED |
| FileWri3 | 0 % | FAILED |
| FireHole2 | 100 % | PASSED |
| Inject1 | 100 % | PASSED |
| Keylog5 | 100 % | PASSED |
| Keylog6 | 100 % | PASSED |
| Kill12 | 100 % | PASSED |

| | | |
|---|---|---|
| OSfwbypass | 100 % | PASSED |
| RegAcc1 | 100 % | PASSED |
| Runner2 | 100 % | PASSED – See the further notes at the end of the report. |
| Schedtest | 0 % | FAILED |
| SSS3 | 0 % | FAILED |

## Level 8

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

| Test name | Result | Comment |
|---|---|---|
| Autorun11 | 100 % | PASSED |
| Autorun13 | 100 % | PASSED |
| Autorun23 | 100 % | PASSED |
| Autorun34 | 0 % | FAILED |
| FileDel3 | 0 % | FAILED |
| FileOpn1 | 0 % | FAILED |
| FileOpn2 | 0 % | FAILED |
| Kernel4b | 100 % | PASSED |
| Kernel5 | 100 % | PASSED |
| Kernel5b | 0 % | FAILED |
| Keylog7 | 100 % | PASSED |
| Kill5 | 100 % | PASSED |
| NewClass | 0 % | FAILED |
| Schedtest2 | 0 % | FAILED |
| SockSnif | 0 % | FAILED |
| SSS4 | 100 % | PASSED |

## Level 9

**Number of tests:** 5
**Level up:** 50 %
**Product's score**: 20 %

| Test name | Result | Comment |
|---|---|---|
| Crash7 | 0 % | FAILED |
| Driver Verifier | 0 % | FAILED |
| FileAcc1 | 0 % | FAILED |

| | | |
|---|---|---|
| FileCtl1 | 0 % | **FAILED** |
| FileWri4 | 100 % | **PASSED** |

### Level 10

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

## Further notes

Technically, ZoneAlarm passed Runner and Runner2 tests because popup queries were displayed and the user was given chances to block the attacks. However, the queries asked about the original Internet Explorer accessing the Internet. It could be assumed that common users would allow the actions.