

# [Full-Disclosure] Presentation: Bypassing client application protection techniques with notepad

*Source:* <http://www.derkeiler.com/Mailing-Lists/Full-Disclosure/2004-10/1101.html>

---

*From:* 3APA3A (3APA3A\_at\_SECURITY.NNOV.RU)

*Date:* 10/28/04

To: full-disclosure@lists.netsys.com  
Date: Thu, 28 Oct 2004 16:56:48 +0400

Topic: Bypassing client application protection techniques

Category: Protection bypass

Affected products:

CheckPoint VPN-1(TM) & FireWall-1(R) NG with Application Intelligence (R55) HFA 9

Microsoft Windows XP SP2

Agnitum Outpost Pro 2.1, 2.5

Tiny Firewall Pro v6.0.100

ZoneAlarm Pro with Web Filtering v4.5.594

BlackICE PC Protection 3.6

Kerio Personal Firewall 4.0

WRQ ATGuard 3.2

Authors:

offtopic, <offtopic@mail.ru>

3APA3A, <3APA3A@security.nnov.ru>

Original link:

<http://www.security.nnov.ru/advisories/bypassing.asp>

Special thanks to Igor U. Miturin for testing and coordinating Checkpoint issues, to Checkpoint for cooperation, to Agnitum for "opossum" topic public debates and some ideas.

Disclaimer:

</SARCASM>

This article is neither attempt to teach scriptkiddies to write trojans nor attempt to create one by authors. It's a call to security community to activate discussion on protection techniques for Internet client application security. Yes, we want to fire a flame. We apologies we did not contacted vendors on many issues they may consider as security vulnerabilities in their products. We believe, to solve discussed problem instead of fixing illustrating PoCs, all products must be architecturally changed, not patched. Before architectural change any schoolboy with scripting skills can get access to corporate network protected by advertised product. We share a point of view, this should not be treated as product vulnerability.

<SARCASM>  
<APPLAUSE />  
(yes, pedram).

## 1. Introduction

### 1.1 Front end security

Last years were revolutionary for network services infrastructure security. In addition to more secure and stable operation systems and services, we've got a lot of industrial solutions – stateful firewalls with level 7 inspection, intrusion detection and intrusion prevention systems, reliable clusters and distributed solutions to fight DDoS attacks... And we got actually nothing in the field of client application protection. Security of client network app