



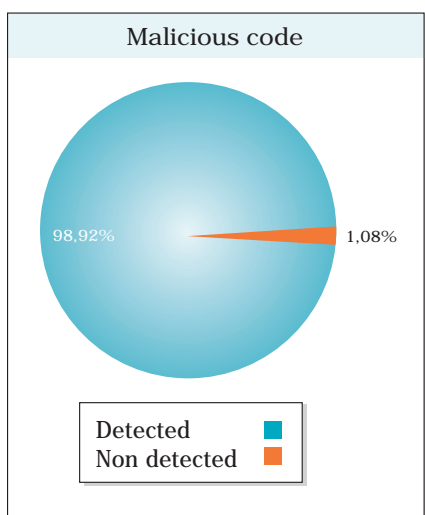
Icsa Labs tests TruPrevent™ Technologies

ICSA Labs determined that TruPrevent™ Technologies developed by Panda Software and present in their commercial antivirus provides a significant level of protection against common malicious code threats, without significantly impacting the performance or interfering with legitimate users of the system tested.



Detection & Prevention

ICSA Labs tested TruPrevent™'s ability to protect against 93 examples of malicious code, and found that in 98.92% of the cases, TruPrevent™ was able to block the spread of the malicious code beyond the infection point. Malware samples used in the test were selected to provide representatives from several categories of malicious code threats, and included Adware, Backdoors, Trojans and both Win32 and Visual Basic Script-based worms.



ICSA Labs designed the test scenario to simulate the case where the resident antivirus software does not have signatures for the malware against which it is being tested. Panda Software Supplied ICSA Labs with a specially prepared antivirus signature file which was only capable of detecting EICAR test string, and which contained no additional virus signatures. ICSA Labs installed this special pav.sig file and then disabled the automatic update feature to prevent this special file from being overwritten. With the antivirus software suite in this state, the only protection offered is by the TruPrevent™ Technologies.

ICSA Labs executed the malware on our designated infection point and monitored all network traffic, the infection point, and other non-protected hosts on our test bed network to determine if the malware successfully spread beyond our infection point. This test was not designed to determine if TruPrevent™ could prevent the malware from installing on infection point, but to determine if it could prevent the malware from propagating beyond the infection point.

Out of 93 malware samples, tested, 92 were properly detected and blocked and 1 was not, a success rate of 98.92%. Testing conducted at the ICSA Labs facility indicated that under certain specific conditions, TruPrevent™ did not block the propagation of Plexus.C. When the tests were repeated at Panda's facility, TruPrevent™ appeared to block Plexus.C. ICSA Labs was not able to repeat this inconsistency.

False Positives

ICSA Labs conducted an extensive test of the base operating system (Windows XP Professional), along with typical user installed extensions, enhancements, commercial and freely available applications. We performed typical user tasks within this system, including registering and installing updates in the Operating System, installing, registering (where applicable), updating and using applications, and exercising the system on the Internet through the use of Web Browsers, File Sharing, Gaming and other applications in an attempt to cause the TruPrevent™ Technologies to inappropriately block legitimate activity. After extensive efforts to do so, we were not able to record a single instance of the evaluated software inappropriately blocking legitimate activity.

ICSA Labs conducted baseline tests using Microsoft Windows XP SP1a and a number of widely available applications to ensure that the test system was functioning correctly. ICSA Labs then re-installed the operating system, installed Panda Titanium Antivirus 2004 with TruPrevent™ and exercised the system according to the test plan in an attempt to generate false positive alerts. ICSA Labs was not able to document an instance where the Panda Titanium 2004 with TruPrevent™ inappropriately altered or blocked software we were installing or using.

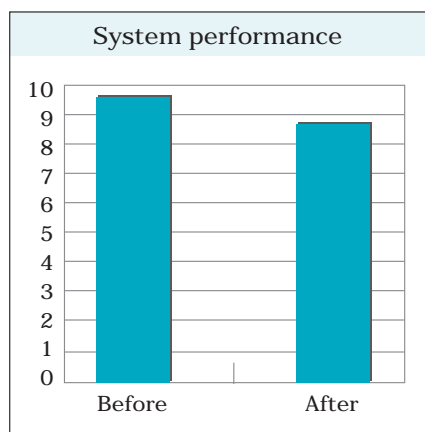
ICSA Labs designed the test scenario to simulate the case where a typical user has purchased a new computer with both the operating system and Panda software pre-installed by the manufacturer. Our test plan was designed to duplicate the actions the user would normally take under these circumstances: registering and updating the operating system, installing, registering, using and updating software applications in several categories, upgrading a video card and installing the appropriate driver software, etc. our detailed test sequence was designed to represent those activities which a normal home or office user would perform.

Applications installed and ran

MS Messenger
Firefox
Acrobat Reader
WinRar
Office 2003 Pro
Kazaa
Yahoo! Messenger
WinAmp
Unreal 2004
Windows Media Player
Shockwave Flash player
WinZip
OpenOffice
BitTorrent
AOL Instant Messenger
Trillian Instant Messenger
Realplayer

Performance Impact

ICSA Labs evaluated the performance impact of the TruPrevent™ using PC Magazine's Business Winstone™ 2004 version 1.0.1. We were able to measure and document a low level of degradation in the performance of the system tested, which performed well and remained responsive throughout all tests.



Business Winstone® installs a suite of commercial business software applications and uses them to perform typical business activities while measuring the systems overall performance. The system performance is evaluated 5 times per iteration of the benchmark suite, and reported arbitrary units called Winstones®. ICSA Labs repeated each run of the benchmark software 4 times to ensure there was no variance in the results.

Given the speed of the system used in the tests and the level of degradation we measured, is it doubtful that a user would perceive any degradation or object the performance of the system while protected. When weighed against the significant level of protection offered by TruPrevent™ and the lack of observed interference with legitimate uses of the system, we believe the performance impact to be negligible.



ICSA Labs
Bent Creek Blvd., Suite 200
Mechanicsburg, PA 17050

Panda Europe Headquarters
Ronda de Poniente, 19
Tres Cantos
Madrid - Spain
Phone: +34 91 806 37 00
E-mail : info@pandasoftware.com

Panda USA Headquarters
N. Maryland, Suite 303
P.O. Box 10578
Glendale, CA 91209
Phone: +00 1 818 543 6901
E-mail : info.usa@pandasoftware.com

The information contained in this document represents the current view of Panda Software, S.L. on the issues discussed herein as of the date of publication. This document is for informational purposes only. Panda Software, S.L. makes no warranties, express or implied, in this document.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Panda Software, S.L.

Panda Software, S.L. may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Panda Software, S.L. the furnishing of this document does not give you any license to these patents, trademarks, copyrights or other intellectual property.