Factsheet October 2013

Real-World Protection Test

Whole Product Dynamic

Real-World Protection Test

Language: English
October 2013

Last Revision: 13th November 2013

www.av-comparatives.org

Introduction

This fact sheet[1] is a short overview of the Whole Product Dynamic Real-World Protection Test results of October 2013. The detailed overall result reports (covering four months each) are released in July and December. Each of the overall result reports will also contain a false alarm test and will award the products based on their overall scores during the respective four-month period. **For more information about this Real-World Protection Test, please read the details and previous test reports available on http://www.av-comparatives.org**

Tested Cases

Our Real-World Protection Test is currently the most comprehensive and complex test available, using a large number of test cases. This year, we are running this test under Microsoft Windows 7 Home Premium 64 Bit SP1 with up-to-date third-party software (such as Adobe Flash, Adobe Acrobat Reader, Java, etc.). Due to this, finding working exploits and running malware is more challenging than e.g. under Microsoft Windows XP with unpatched/vulnerable third-party applications.

Over the year we evaluate tens of thousands malicious URLs. Unfortunately, many of these have to be discarded for various reasons. We remove duplicates such as the same malware hosted on different domains or IP addresses, sites already tested, "grey" or non-malicious sites/files, and malware/sites disappearing during the test.

In September we had **1092** valid malicious URLs, of which **565** test cases (exploits) were not able to compromise the chosen system/applications because of the patch level. This means that the vulnerabilities in the third-party applications on the system were already patched and the exploits could therefore not deliver their malicious payload. Users should be aware that by always keeping their system and third-party applications up-to-date/patched, they can dramatically decrease the risk posed by exploits.

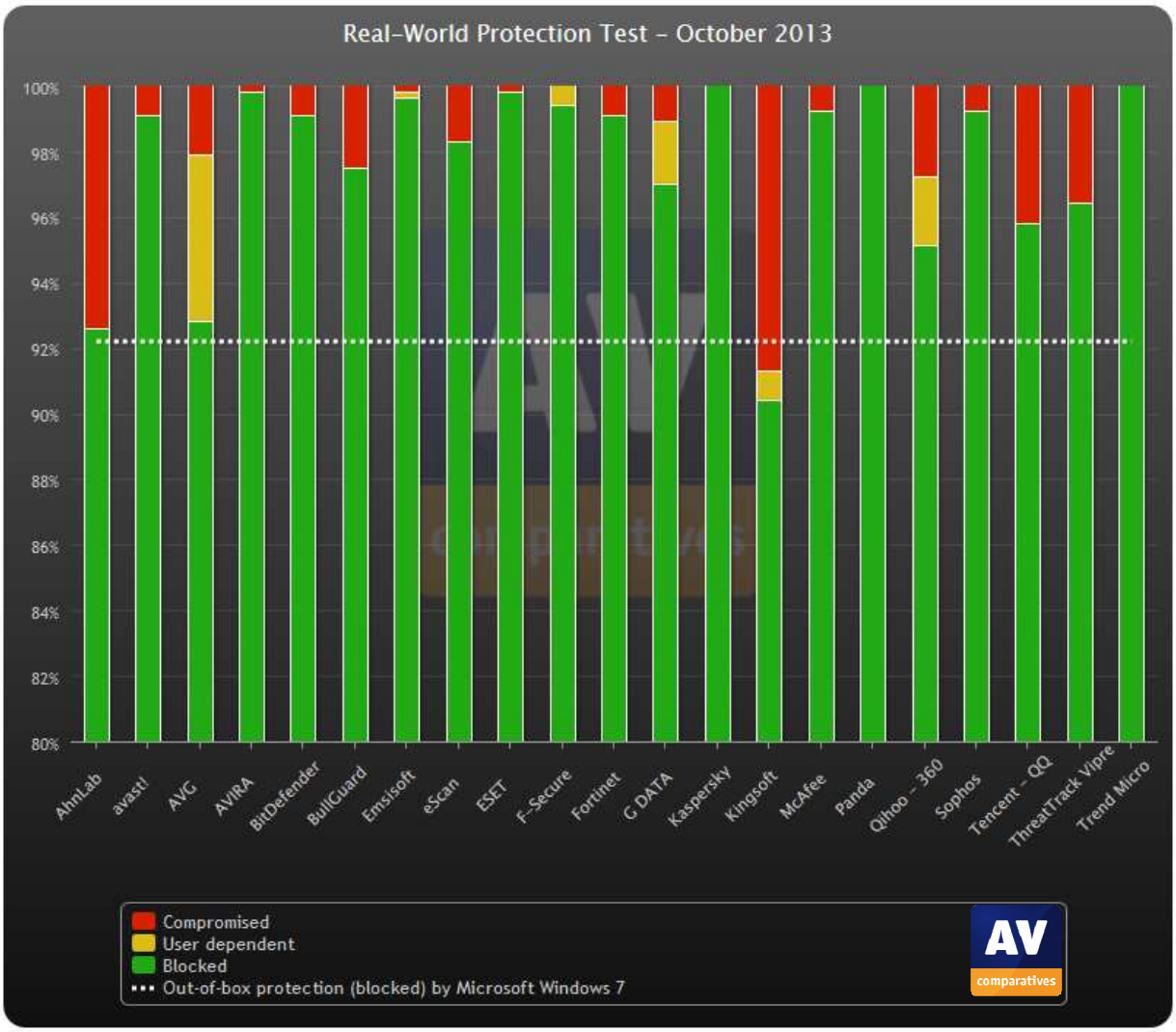
The results are based on the test set of **527** live test cases (malicious URLs found in the field), consisting of working exploits (i.e. drive-by downloads), URLs pointing directly to malware, and a few malicious files from email attachments. The latter are downloaded and executed via webmail. Thus exactly the same infection vectors are used as a typical user would experience in everyday life. The test-cases used cover a wide range of current malicious sites and provide insights into the protection given by the various products (using **all** their protection features) while surfing the web.

The following products (latest version available at time of testing) were tested: AhnLab V3 Internet Security 8.0, avast! Free Antivirus 9.0, AVG Internet Security 2014, AVIRA Internet Security 2014, Bitdefender Internet Security 2014, BullGuard Internet Security 2014, Emsisoft Anti-Malware 8.1, eScan Internet Security 14.0, ESET Smart Security 7.0, F-Secure Internet Security 2014, Fortinet FortiClient 5.0, G DATA Internet Security 2014, Kaspersky Internet Security 2014, Kingsoft Internet Security 2013, McAfee Internet Security 2014, Microsoft Security Essentials 4.3, Panda Cloud Free Antivirus 2.2, Qihoo 360 Security 4.2, Sophos Endpoint Security 10.3, Tencent QQ PC Manager 8.1, ThreatTrack Vipre Internet Security 2014 and Trend Micro Internet Security 2014.

[1] The full detailed report will be released in December.

Graph of protection

Every month (from March to June and from August to November) we update the charts on our website showing the protection rates of the various tested products over the various months. The interactive charts can be found on our website[2]. The chart below shows only the protection scores for the month of OCTOBER 2013 (527 test cases).



Microsoft's out-of-box protection: 92.2% (non-competitive)

The graph above shows the test results against the "out-of-box" malware protection provided by Microsoft Windows. In Windows 8, this is provided by Windows Defender, which is pre-installed by default with the operating system. The equivalent in Windows 7 is Microsoft Security Essentials, which is not pre-installed, but can easily be added for free as an option via the Windows Update service.

We would like to point out that while some products were able to reach 100% protection rates in a test, it does not mean that these products will always protect against all threats on the web. It just means that they were able to block 100% of the widespread malicious samples used in a test.

[2] http://chart.av-comparatives.org/chart1.php

Copyright and Disclaimer

This publication is Copyright © 2013 by AV-Comparatives e.V. ®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives e.V., prior to any publication. AV-Comparatives e.V. and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives e.V. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data. AV-Comparatives e.V. is a registered Austrian Non-Profit-Organization.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

AV-Comparatives e.V. (November 2013)