Factsheet April 2014

Real-World Protection Test

Whole Product Dynamic

Real-World Protection Test

Language: English
April 2014

Last Revision: 14th May 2014

www.av-comparatives.org

Introduction

This fact sheet[1] is a short overview of the Whole-Product Dynamic Real-World Protection Test results of April 2014. 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 contain the awards the products reached 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 in-the-field working exploits and running malware is much more challenging than e.g. under Microsoft Windows XP with unpatched/vulnerable third-party applications.

Over the year we evaluate several 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. Many malicious URLs carrying 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.

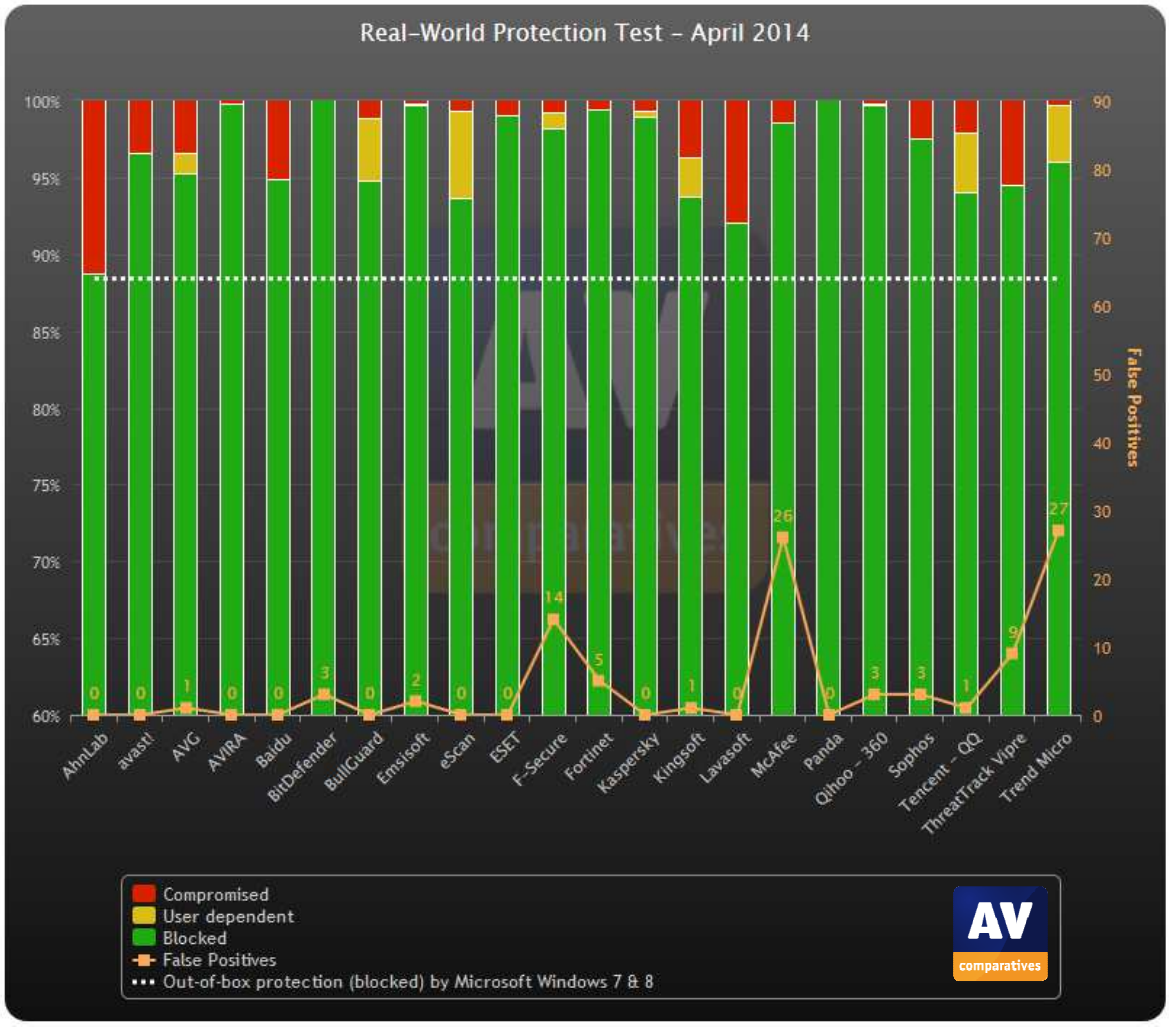
The results are based on the test set of **1030** live test cases (malicious URLs found in the field), consisting of working exploits (i.e. drive-by downloads), URLs pointing directly to malware, and a few malicious files from email attachments. The latter are downloaded and executed via webmail. Thus 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 2014, AVG Internet Security 2014, AVIRA Internet Security 14.0, Baidu Internet Security 2014 (English version), Bitdefender Internet Security 2014, BullGuard Internet Security 14.0, Emsisoft Anti-Malware 8.1, eScan Internet Security 14.0, ESET Smart Security 7.0, F-Secure Internet Security 2014, Fortinet FortiClient 5.0, Kaspersky Internet Security 2014, Kingsoft Internet Security 2013.SP6, Lavasoft Ad-Aware Free Antivirus+ 11.1, McAfee Internet Security 2014, Microsoft Security Essentials 4.5, Panda Cloud Free Antivirus 2.3, Qihoo 360 Internet Security 4.9, Sophos Endpoint Security and Control 10.3, Tencent QQ PC Manager 8.10, ThreatTrack Vipre Internet Security 2014 and Trend Micro Titanium Internet Security 2014.

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

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 APRIL 2014 (1030 test cases). This year, we are including the results of the false-positives test in the monthly factsheets; these are also shown in the graph below.



Microsoft's out-of-box protection: 88.4% (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 may sometimes be 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

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

AV-Comparatives (May 2014)