Factsheet October 2017

Real-World Protection Test

Whole Product Dynamic

Real-World Protection Test

Language: English
October 2017

Last Revision: 10th November 2017

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 2017. The detailed overall result reports (covering five 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 five-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. Currently, we are running this test under Microsoft Windows 10 RS2 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 an non-up-to-date system 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.

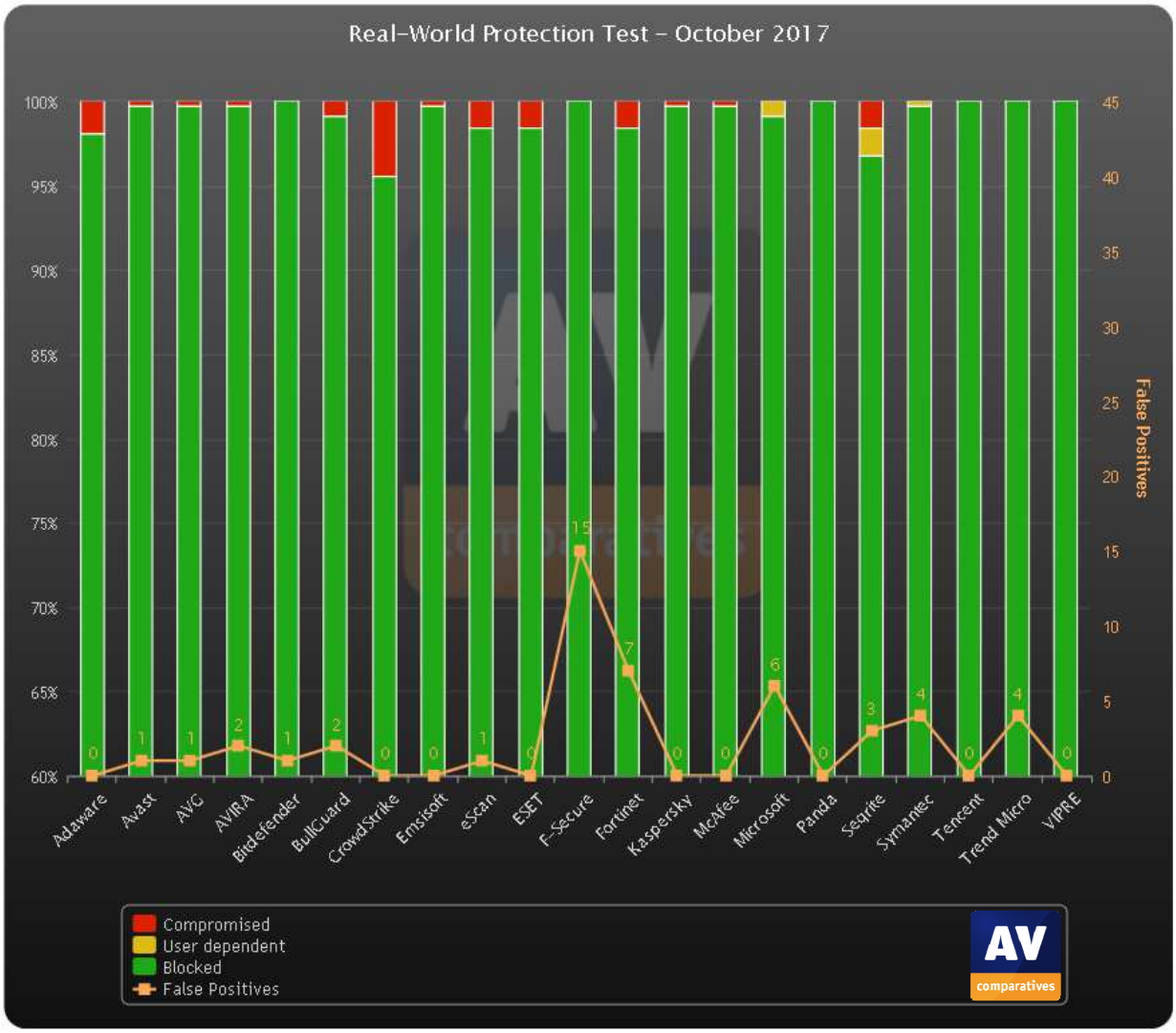
The results are based on the test set of **316** live test cases (malicious URLs found in the field), consisting of working exploits (i.e. drive-by downloads) and URLs pointing directly to malware. Thus exactly the same infection vectors are used as a typical user would experience in everyday life. The 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: Adaware Pro Security 12.2, Avast Free Antivirus 17.7, AVG Free Antivirus 17.7, AVIRA Antivirus Pro 15.0, Bitdefender Internet Security 22.0, BullGuard Internet Security 18.0, CrowdStrike Falcon Prevent 3.7, Emsisoft Anti-Malware 2017.9, eScan Corporate 360 14.0, ESET Internet Security 11.0, F-Secure Safe 17.0, Fortinet FortiClient 5.6, Kaspersky Internet Security 18.0, McAfee Internet Security 20.4, Microsoft Windows Defender 4.11, Panda Free Antivirus 18.3, Seqrite Endpoint Security 17.0, Symantec Norton Security 22.11, Tencent PC Manager 12.3, Trend Micro Internet Security 12.0 and VIPRE Internet Security Pro 10.1.

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

Graph of protection

Every month (from February to June and from July 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 2017 (316 test cases). The results of the false-positives test are also shown in the monthly factsheets/graph below.



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 (November 2017)