Anti-Virus Comparative

Comparative Test of Business Security Products

Language: English
October 2016
Last revision: 4th November 2016

http://www.av-comparatives.org
http://www.mrg-effitas.com

Content

Introduction

For this assessment, MRG Effitas and AV-Comparatives combined their strengths to conduct a joint test. The Malware Protection Test was performed by AV-Comparatives, and the Exploit Test was performed by MRG Effitas.

General

Malicious software poses an ever-increasing threat, not only due to the number of malware programs increasing, but also due to the nature of the threats. Infection vectors are changing from simple file-based methods to distribution via the Internet. Malware is increasingly focussing on users, e.g. by deceiving them into visiting infected web pages, installing rogue/malicious software, cyber espionage, ransomware or opening emails with malicious attachments. The scope of protection offered by antivirus programs like signatures and heuristics is extended by the inclusion of e.g. URL-blockers, content filtering, reputation systems, cloud based methodologies and user-friendly behaviour-blockers. If these features are perfectly coordinated with the signature-based and heuristic detection, the protection provided against threats increases. However, we would recommend that all parts of a product should be as effective as possible. It should be borne in mind that not all malware enters computer systems via the Internet, and that e.g. a URL blocker is ineffective against malware introduced to a PC via a USB flash drive or over the local area network.

We congratulate the four vendors who participated in this test for having their business products publicly tested by an independent lab. We invited a number of other vendors to participate in this test, but they declined, mostly as they already have their consumer products thoroughly tested by us, and these results are likely to be similar to those for their corresponding business products.

Tested Products

The following products[1] have been reviewed/tested with default settings under Windows 10 64-bit:

Vendor	Product	Version
AVG	CloudCare	2016
Bitdefender	GravityZone Advanced Business Security Cloud	6.2.9
ESET	Endpoint Security	6.4
Kaspersky Lab	Endpoint Security Cloud	1.0

AV comparatives Approved Business Product 2016

Overview

In this test, the protection offered by the products has been evaluated. The tests were performed from September till October 2016.

The following tests were performed:

RTTL: 500 most prevalent malicious samples according to the AMTSO Real-Time Threat List (RTTL) were **executed** on the system.

AVC: 500 most recent and prevalent malicious samples from our own database were **executed** on the system.

WPDT: 50 malicious websites were tested by using our **Real-World Testing** Framework, which simulates the activities of a typical computer user (whether at home or in the office) surfing the Internet.

FPs: a false alarm test in which 1000 clean files have been **executed** on the system has also been performed. The false positive test measures the ability of products to distinguish clean from malicious files.

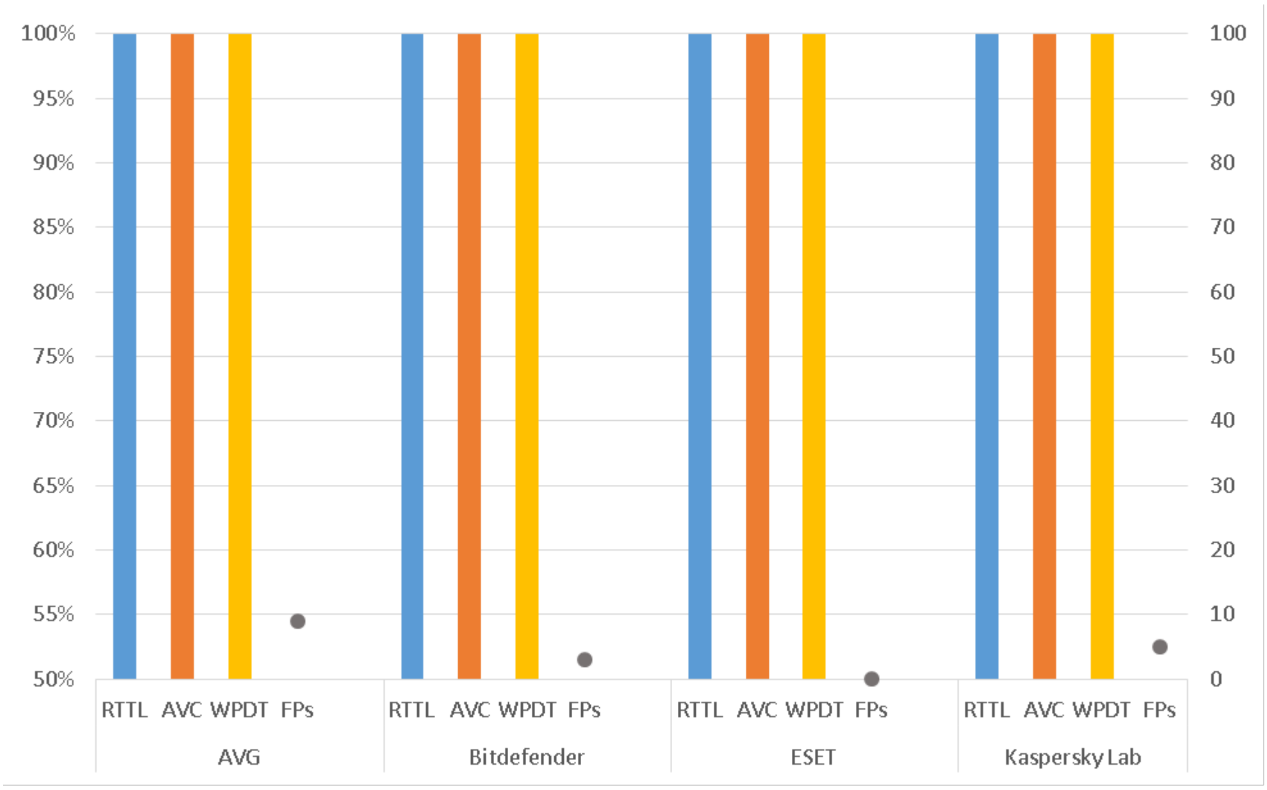
Exploit Test: 21 exploits have been used in the Exploit test.

[1] All four above products are Approved Business Security Products. See details here: https://www.av-comparatives.org/wp-content/uploads/2016/10/avc_cor_2016_en.pdf

Results

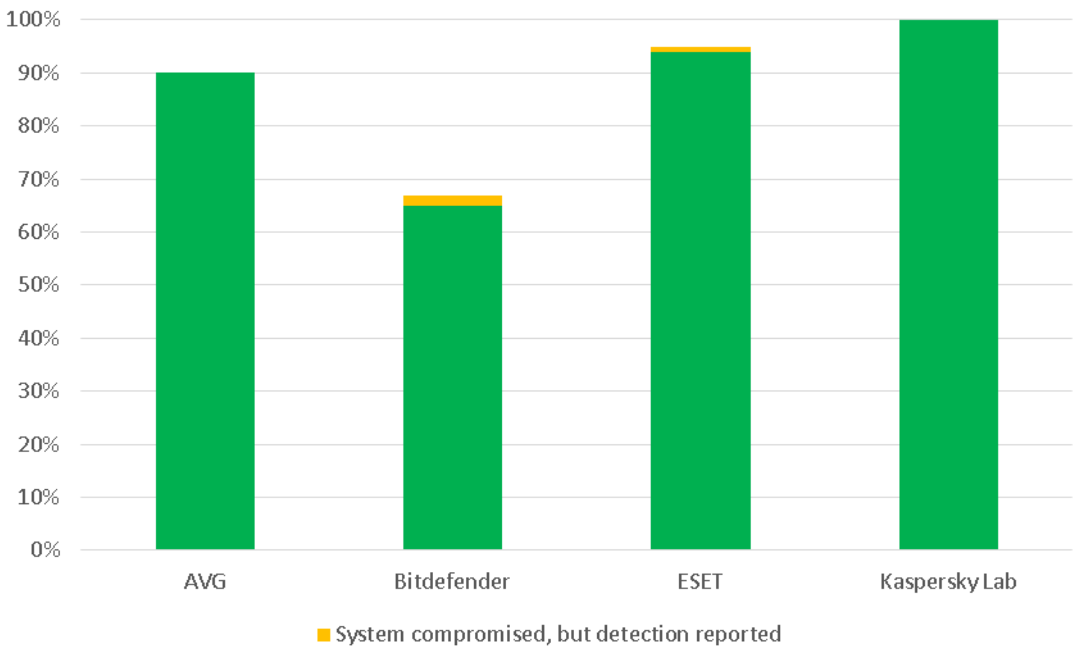
Malware Protection Test

The following chart shows the results of the malware protection test.



	RTTL	AVC	WPDT	FPs
AVG	100%	100%	100%	9
Bitdefender	100%	100%	100%	3
ESET	100%	100%	100%	0
Kaspersky Lab	100%	100%	100%	5

Exploit Protection Test



	Protected	Detected
AVG	90%	90%
Bitdefender	65%	67%
ESET	94%	95%
Kaspersky Lab	100%	100%

Scoring / Calculation of Results

Scoring Of The Exploit Protection/Detection Results

We defined the following stages, where the exploit can be prevented by the endpoint protection system:

1. Blocking the URL (infected URL, exploit kit URL, redirection URL, malware URL) by the URL database (local or cloud). For example, a typical result is the browser displaying a "site has been blocked" message by the endpoint protection. The sooner the threat is detected in the exploit chain, the easier it is to remove the malicious files from the system, the less information can be gathered from the system by the attackers, and there is less risk of an attack targeting the particular security solution on an endpoint.

2. Analysing and blocking the page containing a malicious HTML code, JavaScripts (redirects, iframes, obfuscated JavaScripts, etc.), or Flash files.

3. Blocking the exploit before the shellcode is executed.

4. Blocking the downloaded payload by analyzing the malware before it is started. For example, the malware payload download (either the clear-text binary or the encrypted/encoded binary) can be seen in the proxy traffic, but no malware process starts.

5. The malware execution is blocked (no process create, load library).

6. There was a successful start by the dropped malware.

7. There was a successful start by the dropped malware, but after some time, all dropped malware was terminated and deleted ("malware starts, but blocked later").

The "protection" scoring of the results was calculated as the followings:

- If no malicious untrusted code was able to run on the endpoint, 5 points were given to the products. This can be achieved via blocking the exploit in step 1, 2 or 3.
- If malicious untrusted code run on the system (exploit shellcode, downloader code), but the final malware was not able start, 4 points were given to the product. This can be achieved via blocking the exploit in step 4 or 5.
- If both the exploit shellcode (or downloader code) and the final malware was able to run, 0 point was given to the product.
- If at by any stage of the infection, a medium or high severity alert has been generated (even if the infection was not prevented), 1 point was given to the product.

The "detection" scoring of the results was calculated as the followings:

- If at by any stage of the infection, a medium or high severity alert has been generated (even if the infection was not prevented), 1 point was given to the product.

We used this scoring for the following reasons:

- The scope of the test was exploit prevention and not the detection of malware running on the system.
- It is not possible to determine what kind of commands have been executed or what information exfiltrated by the malware. Data exfiltration cannot be undone or remediated.
- It cannot be determined if the malware exited because the endpoint protection system blocked it, or if malware quit because it detected monitor processes, virtualization, or quit because it did not find its target environment.
- Checking for malware remediation can be too time-consuming and remediation scoring very difficult in an enterprise environment. For example, in recent years we experienced several alerts that the endpoint protection system blocked a URL/page/exploit/malware, but still the malware was able to execute and run on the system. On other occasions, the malware code was deleted from the disk by the endpoint protection system, but the malware process was still running, or some parts of the malware were detected and killed, while others were not.
- In a complex enterprise environment multiple network and endpoint products protect the endpoints. If one network product alerts that malicious binary has been downloaded to the endpoint, administrators have to cross-check the alerts with the endpoint protection alerts, or do a full forensics investigation to be sure that no malware was running on the endpoint. This process can be time and resource consuming, which is why it is better to block the exploit before the shellcode starts.
- Usually the exploit shellcode is only a simple stage to download and execute a new piece of malware, but in targeted attacks, the exploit shellcode can be more complex.

We believe that such zero-tolerance scoring helps enterprises to choose the best products, using simple metrics. Manually verifying the successful remediation of the malware in an enterprise environment is a very resource-intensive process and costs a lot of money. In our view, malware needs to be blocked before it has a chance to run, and no exploit shellcode should be able to run.

Test Procedure / Methodology

Exploit Test Setup

Testing Cycle for Each Test Case

1) One default installation of Windows 10 64-bit on a virtual machine (VirtualBox) endpoint was created. The default HTTP/HTTPS proxy was configured to point to a proxy running on a different machine. SSL/TLS traffic was not intercepted on the proxy.

2) The security of the OS was weakened by the following actions:
   a) Microsoft Defender was disabled
   b) Internet Explorer SmartScreen was disabled
   c) Vulnerable software was installed, see “Software Installed” for details.
   d) Windows Update was disabled

3) From this point, different snapshots were created from the virtual machine, several with different endpoint protection products and one with none. This procedure ensured that the base system was exactly the same in all test systems.

   The following endpoint security suites, with the following configuration, were defined for this test:

   a) No additional protection (this snapshot was used to infect the OS and to verify the exploit replay)
   b) Product 1 installed
   c) Product 2 installed
   d) …

The endpoint systems were installed with default configuration, potentially unwanted software removal was enabled, and if it was an option during install, cloud/community participation was enabled.

4) The exploit sources can be divided into two categories. In-the-wild threats and Metasploit. VBscript based downloaders and Office macro documents were also in scope, as these threats are usually not included in other test scenarios.

5) The virtual machine was reverted to a clean state and traffic was replayed by the proxy server. The replay meant that the browser was used as before, but instead of the original webservers, the proxy server answered the requests based on the recorded traffic. When the “replayed exploit” was able to infect the OS, the exploit traffic was marked as a source for the tests. This method guarantees that exactly the same traffic will be seen by the endpoint protection systems, even if the original exploit kit goes down during the tests. This exploit replay is NOT to be confused with tcpreplay type replay.

6) After new exploit traffic was approved, the endpoint protection systems were tested. Before the exploit site was tested, it was verified that the endpoint protection had been updated to the latest version with the latest signatures and that every cloud connection was working. If there was a need to restart the system, it was restarted. In the proxy setup, unmatched requests were allowed to pass through and SSL/TLS was not decrypted to ensure AV connectivity. VPN was used during the test on

the host machine. When user interaction was needed from the endpoint protection (e.g. site visit not recommended, etc.), the block/deny action was chosen. When user interaction was needed from Windows, we chose the run/allow options. No other processes were running on the system, except the Process Monitor/Process Explorer from SysInternals and Wireshark (both installed to non-default directories).

7) After navigating to the exploit site, the system was monitored to check for new processes, loaded DLLs or C&C traffic.

8) The process went back to step 5, until all exploit site test cases were reached.

The following hardware was dedicated to the virtual machine:

- 4 GB RAM memory
- 2 processors dedicated from AMD FX 8370E CPU
- 65 GB free space
- 1 network interface
- SSD drive

The VirtualBox host and guest system for the exploit test has been hardened in a way that common virtualization and sandbox detection techniques cannot detect the system as an analysis system.

Analysis Of The Exploit Kits Used In The Exploit Test

Unfortunately, the time of the test and OS configuration was not in favor for the exploit test. At the time of the tests, two exploit kits dominated the Internet. Sundown and RIG. Unfortunately, RIG used old (mostly Flash) exploits, which was unable to exploit the test configuration at all. That is why it was important to test with Metasploit and with some not super-fresh, but not too-old exploit kits as well (Neutrino).

We also used two sample, which is not an exploit itself, but rather a non-PE downloader, like an Office macro and a WSF downloader. We added these into the mix because these “egsotic” file types are often excluded from Real World tests, but meanwhile, prevalent in-the-wild.

A total of 21 test cases have been tested.

- 8 Sundown EK
- 5 Neutrino EK
- 4 Metasploit
- 1 Powershell Empire
- 1 Metasploit Macro
- 1 Locky malspam WSF
- 1 unknown EK

These exploit kits were targeting Adobe Flash, Internet Explorer, Microsoft Office (macro), Silverlight, Firefox, Java.

Software Installed

For the exploit test part, the following vulnerable software was installed:

Vendor	Product	Version		Vendor	Product	Version
Adobe	Flash Player ActiveX - builtin	21.0.0.182		Microsoft	SilverLight	5.1.10411.0
AutoIT	AutoIT	3.3.12.0		Mozilla	Firefox	31.0
Microsoft	Internet Explorer	11.162.10586		Oracle	Java	1.7.0.17
Microsoft	Office	2016				

Scoring of the Malware Protection Results

The scoring of the malware protection is straightforward, whenever the system got compromised by the malware, 0 point were given to the product, and whenever the malware was blocked or remediated, 1 point was given. If a pop-up was shifting the decision to the user, 0.5 point were given.

False positive test

The same scoring principle as described above has been applied for the false alarms test. In this test, 1000 non-malicious applications have been used.

About the test-labs

AV-Comparatives

AV-Comparatives is a vendor-independent organization offering systematic testing that checks whether security software such as PC/Mac-based antivirus products and mobile security solutions lives up to its promises. Using one of the largest sample collections worldwide, AV-Comparatives create real-world environments for accurate security tool testing offering freely accessible results to individuals, media and scientific institutions. Certification by AV-Comparatives provides an official seal of approval for software performance which is globally recognized. Currently, the Real-World Protection Test is the most comprehensive and complex test available when it comes to evaluating real-life protection capabilities of antivirus software. For this purpose, AV-Comparatives runs one of the world largest IT security testing frameworks in a data centre located in Innsbruck.

Members of AV-Comparatives give frequently talks at the major IT security conferences like Virus Bulletin, AVAR, EICAR, IEEE Malware Conference, WATeR, AMTSO, BSides, Ninjacon.

The methodology of AV-Comparatives' Real-World Protection Test has received the following awards and certifications, including:

- **Constantinus Award** – given by the Austrian government
- **Cluster Award** – given by the Standortagentur Tirol – Tyrolean government
- **eAward** – given by report.at (Magazine for Computer Science) and the Office of the Federal Chancellor
- **Innovationspreis IT** – "Best Of" – given by Initiative Mittelstand Germany

AV-Comparatives' Management System is ISO 9001:2008 certified. The certification has been received from TÜV Austria for the management system with scope "Independent Tests of Anti-Virus Software".

AV-Comparatives is the first certified EICAR Trusted IT-Security Lab.

The data centre where AV-Comparatives runs the test equipment is ISO 27001:2013 certified.

TÜV AUSTRIA
ZERTIFIZIERT
EN ISO 9001
ZERTIFIKAT NR. 20 100 141369414
TÜV AUSTRIA CERT GMBH

eicar
trusted
IT-security

MRG Effitas

MRG Effitas is a UK based, independent IT security research organisation which focuses on providing cutting edge efficacy assessment and assurance services, supply of malware samples to vendors and the latest news concerning new threats and other information in the field of IT security.

MRG Effitas' origin began when the "Malware Research Group" was formed in 2009 by Sveta Miladinov, an independent security researcher and consultant. In June 2009, Chris Pickard, joined, bringing expertise in process and methodology design, gained in the business process outsourcing market.

The Malware Research Group rapidly gained a reputation as being the leading efficacy assessor in the browser and online banking space and due to increasing demand for its services, was restructured in 2011 and became "MRG Effitas" with the parent company "Effitas".

Today, MRG Effitas has a team of analysts, researchers and associates across EMEA, USA and China, ensuring a truly global presence.

Since its inception, MRG Effitas has focused on providing ground-breaking testing processes, realistically modelling real world environments in order to generate the most accurate efficacy assessments possible.

MRG Effitas is recognised by several leading security vendors as being the leading testing and assessment organisation in the online banking, browser security and cloud security spaces and has become the partner of choice.

Members of MRG Effitas give frequently talks at the major IT security conferences like Botconf, DEF CON, WATeR (AMTSO), Hacktivity, Hacker Halted etc.

Our professionals hold the following certifications: CISSP, OSCP, OSCE, GPEN, SLAE, SPSE, CPTS, CHFI, MCP, OSWP.

Copyright and Disclaimer

AV-Comparatives / MRG Effitas and its testers cannot be held liable for any damage or loss which might occur as a 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 liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives / MRG Effitas. 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.

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

AV-Comparatives / MRG Effitas (November 2016)