MalwareTips AV Test – March 2017 – AVG Internet Security

March 2017	Total Number of Samples	Static Test	Dynamic Test	Bait Files Encrypted	Total Detection	Second Opinion System Status	System's Final Status
1.3.2017.	1	1	N/A	No	1	All Clean	Clean
1.3.2017.	24	11	6/13	No	17	IL	Protected
2.3.2017.	15	9	4/6	No	13	IL	Protected
3.3.2017.	23	12	4/11	No	16	IL	Protected
4.3.2017.	7	6	1/1	No	7	All Clean	Clean
6.3.2017.	20	9	9/11	No	18	IL	Not Clean
8.3.2017.	27	17	5/10	No	22	IL	Protected
9.3.2017.	16	9	6/7	No	15	IL & MSM	Not Clean
10.3.2017.	20	7	7/13	No	14	IL	Protected
11.3.2017.	1	0	1/1	No	1	All Clean	Clean
11.3.2017.	3	2	1/1	No	3	All Clean	Clean
12.3.2017.	1	1	N/A	No	1	All Clean	Clean
13.3.2017.	17	8	7/9	No	15	IL	Protected
14.3.2017.	1	1	N/A	No	1	All Clean	Clean
14.3.2017.	1	1	N/A	No	1	All Clean	Clean
15.3.2017.	20	10	10/10	No	20	All Clean	Clean
16.3.2017.	2	2	N/A	No	2	All Clean	Clean
17.3.2017.	12	2	6/10	No	8	AL & MSM	Infected
17.3.2017.	1	1	N/A	No	1	All Clean	Clean
19.3.2017.	1	0	1/1	No	1	All Clean	Clean
20.3.2017.	1	0	1/1	No	1	All Clean	Clean
20.3.2017.	17	9	7/8	No	16	All Clean	Protected
23.3.2017.	18	11	5/7	No	16	All Clean	Protected
24.3.2017.	30	12	10/18	No	22	AL	Infected
27.3.2017.	20	14	5/6	No	19	All Clean	Clean
31.3.2017.	31	19	5/11	No	24	AL	Infected
26 Tests	330	174	101	100%	275		

Total Number of Samples – Number of potential malicious samples used for testing purposes.
Static Test – A type of test used to determine security product's ability to detect malicious file without file's execution.
Dynamic Test – A type of test used to determine security product's ability to detect malicious file upon its execution.
Bait Files – A collection of files of common file types (documents, images, music, etc.) used upon a ransomware attack test. Ransomware usually tries to encrypt these files in order to ask you for a ransom.
Total Detection = Static Detection + Dynamic Detection
Second Opinion System Status – A collection of tools our Malware Testers use to check the system for malware, malware traces, leftovers, malicious processes, malicious system modifications, malicious network connections, etc. IL – Inactive leftovers, AL – Active leftovers, MSM – Malicious System Modification, MNM – Malicious Network Modification
System's Final Status :
Clean means that a security product was able to detect all the samples by static or dynamic detection mechanisms.
Protected means that some samples were missed by security product's detection mechanisms, but any malicious activity was successfully blocked, with a confirmation that Second Opinion Scanners didn't show any sign of malicious presence, malicious activity or malicious system modification.
Not Clean means that some samples were missed by security product's detection mechanisms. No malicious file is running in system's memory, there is no obvious malicious activity or malicious system modification detected but Second Opinion Scanners show the malicious leftovers are present on the test system.
Infected means that system is compromised by at least one malware. Present signs of active malware infection, malicious network connections, malicious system modification, bait files successfully encrypted, broken system's stability and usability, BSODs, etc.

MalwareTips AV Tester reserves the right to cooperate with other malware researchers in order to make the final and objective judgment whether the tested system is Clean, Protected, Not Clean or Infected, collecting and analyzing all the criteria needed. Subjective System's Final Status can be given in borderline situations. Please note that not all the samples tested are indeed malicious, and some malicious ones are VirtualMachine-Aware.

Virtual Environment : Shadow Defender v1.4.0.653, Windows 10 Home v1607 - build 14393.969
Tested Security Product : AVG Internet Security v17.3.3010 (build 17.3.3442.0), Potentially Unwanted Programs detection enabled
Tests conducted by MalwareTips AV Tester Der.Reisende (https://malwaretips.com/members/der-reisende.32430/)

During our test, conducted from 1.03.2017. to 31.03.2017. AVG Internet Security, detected 275 out of 330 samples with the detection rate of 83,33%. AVG Internet Security was able to detect 174 samples out of 330 with our Static Test (detection without execution), and additional 101 samples on Dynamic Test (upon sample execution). No bait files were encrypted during the whole testing period. Out of 156 samples missed by the static scan, AVG Security accomplished to detect 101 of them by its behavioral mechanisms with dynamic detection ratio of 64,74%. Out of 26 tests, AVG Internet Security failed to protect the system 5 times.

<div align="center">

Static Detection Rate : 52,72%
Dynamic Detection Rate : 64,74%
Total Detection Rate : 83,33%

</div>

All tests were conducted in protected virtual environment. Due to the small number of samples used in these tests, you should take results with a grain of salt. This test shows how the tested product behaves with certain malware samples, under unique circumstances, in a given period of time. Product's malware detection rate is not an equivalent of protection. This should not be mixed up. MalwareTips encourage you to compare these results with others and take informed decisions on what security products to use.