MalwareTips AV Test – March 2017 – Windows Defender + Immunet Free

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.	24	18	0/6	No	18	All Clean	Protected
2.3.2017.	15	12	2/3	No	14	AL	Not Clean
3.3.2017.	23	18	1/5	No	19	All Clean	Protected
4.3.2017.	7	6	1/1	No	7	AL	Not Clean
6.3.2017.	20	18	1/2	No	19	All Clean	Protected
8.3.2017.	27	21	4/6	No	25	AL	Not Clean
9.3.2017.	16	13	1/3	No	14	AL	Infected
10.3.2017.	20	16	0/4	No	16	All Clean	Protected
11.3.2017.	3	3	N/A	No	3	All Clean	Clean
13.3.2017.	17	15	1/2	No	16	All Clean	Protected
15.3.2017.	20	18	2/2	No	20	All Clean	Clean
16.3.2017.	2	2	N/A	No	2	All Clean	Clean
17.3.2017.	12	9	1/3	No	10	AL	Infected
20.3.2017.	17	13	2/4	No	15	All Clean	Protected
23.3.2017.	18	16	1/2	No	17	All Clean	Protected
24.3.2017.	30	16	2/14	Yes	18	AL	Infected
27.3.2017.	20	19	0/1	No	19	All Clean	Protected
29.3.2017.	15	12	1/3	No	13	All Clean	Protected
18 Tests	**306**	**245**	**20**	**94,44%**	**265**		

MalwareTips
Your Security Advisor

MalwareTips AV Test – March 2017 – Windows Defender + Immunet Free

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 : Virtual Box 5.1.8, Windows 10 x64 (v1607 build 14393.693)
Tested Security Product : Windows Defender, Potentially Unwanted Programs detection enabled, + Immunet Free
Tests conducted by MalwareTips AV Tester Av Gurus (https://malwaretips.com/members/av-gurus.28210/)

During our test, conducted from 1.03.2017. to 31.03.2017. Windows Defender in combination with Immunet Free, detected 265 out of 306 samples with the detection rate of 86,60%. Windows Defender with Immunet Free was able to detect 245 samples out of 306 with our Static Test (detection without execution), and additional 20 samples on Dynamic Test (upon sample execution). Bait files were encrypted once during the whole testing period. Out of 61 samples missed by the static scan, Windows Defender with Immunet Free accomplished to detect 20 of them by its behavioral mechanisms with dynamic detection ratio of 32,78%. Out of 18 tests, Windows Defender with Immunet Free failed to protect the system 6 times.

Static Detection Rate : 80,06%
Dynamic Detection Rate : 32,78%
Total Detection Rate : 86,60%

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.

MalwareTips
Your Security Advisor