Test of McAfee Endpoint Security for Linux

A test commissioned by McAfee and performed by AV-TEST GmbH. Date of the report: December 11th 2019

Executive Summary

In August 2019, AV-TEST performed a review of the McAfee Endpoint Security for Linux to determine the static detection capabilities of Linux and Windows PE malware. A further requirement was to check the performance influence and whether the scanner provides malware detection without too many false positives.

In order to conduct the test, several thousand malicious files from July 06th to August 06th had been selected from AV-TEST analysis systems and third-party sources. Only those files that have been reported as being "prevalent malware" by at least two independent parties were used in the Windows test set.

In total 21,895 Linux malware files, and 3,698 Windows PE files were used for the malware detection test. For the false positive test two different sets were used. The first set contained 129,737 files from Linux Ubuntu installations. The second set contains 402,026 files from popular Windows programs from major download sites as well from Microsoft Windows and Office installations. Additionally, also a dynamic false positive test was conducted in which widespread Linux software was downloaded from their original source and then installed to check for false positives during typical user behavior.

Test Results

The test has been performed between August 8th and 20th. The Linux and Windows malware detection results are outlined in the table below.

Linux Malware	Reference	Detected Files	99.90%
Total Detection Rate	**21,895**	**21,873**	**99.90%**
* Elf	12,248	12,230	99.85%
* Scripts	298	297	99.66%
* Gzip	9324	9321	99.97%
* Rar	3	3	100%
* Zip	13	13	100%
* Tar	9	9	100%
Windows Malware			
Total Detection Rate	3,698	3,698	100%

The overall detection rate for Linux malware is 99.90%. In the Windows malware test all samples have been detected.

As a counterpart a false positive test was conducted. There were no detection in the static nor the dynamic test. Details are presented in the tables below.

Static False Positive Test	Reference	Detected Files
* … from Linux installations (critical)	129,737	0
* … from popular Windows programs from major download sites (less critical)	402,026	0
Dynamic False Positive Test	**Reference**	**Detected Files**
Blocked Programs / Installations (negative)	46	0
Warning messages (negative)	46	0
Detailed Results: Installation / Usage and Update		
* Android Studio 3.4.2.0	2	+ / +
* Angry IP Scanner 3.6.0	2	+ / +
* AsciidocFX 1.7.0	2	+ / +
* Balena Etcher 1.5.53	2	+ / +
* Blender 2.80	2	+ / +
* cudatext 1.85.0	2	+ / +
* Detect It Easy 2.04	2	+ / +
* Eclipse 2019-06	2	+ / +
* EPUB-Checker 1.9.3	2	+ / +
* Final Crypt 5.3.1	2	+ / +
* Gaia Sky 2.2.0	2	+ / +
* Gimp 2.10	2	+ / +
* Java jdk 12.0.2	2	+ / +
* Opera 62.0.3331.116	2	+ / +
* Pixeluvo 1.6.0-2	2	+ / +
* Putty 0.7.0	2	+ / +
* Skype 8.51.0.72	2	+ / +
* Teamviewer 14.4.2669	2	+ / +
* TorBrowser 8.5.4	2	+ / +
* Thunderbird 60.8.0	2	+ / +
* VideoLan 3.0.7	2	+ / +
* Virtual Box 6.0.10	2	+ / +
* Wine 4.0-1	2	+ / +

A performance test, including an on-demand scan as well as two copy tests didn't show any serious impact on the systems performance.

Performance Test	Reference (in seconds)	Measured Time (in seconds)	Impact
Copy files from local to local	95.78	97,88	2.14%
Copy files from server to local	159.82	164,37	2.76%
Scanning 127906 performance files (in seconds)		1417.96	