FireEye Detection Test

A test commissioned by FireEye and performed by AV-TEST GmbH. Date of the report: February 22nd 2019

Executive Summary

In January 2019, AV-TEST performed a review of a FireEye Command Line scanner for Windows to determine the static detection capabilities of Windows PE malware. A further requirement was to check whether the scanner provides malware detection without too many false positives.

In order to conduct the test, several thousand malicious files from January 01st to January 17th had been selected from AV-TEST 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 test set.

In total 15407 malware files, including 1907 potentially unwanted applications, were used for the malware detection test.

For false positive test set consisted of two different sets. The first set contained 397608 files from Windows and Office installations. The second set contains 408158 files from popular programs from major download sites.

Test Results

The test has been performed on January 21st, the test results are outlined in the table below.

Sum total (prevalent malware)	15407	15327	99,48%
Win32 Malware			
* Backdoors	405	405	100,00%
* Bots	1629	1629	100,00%
* Viruses	205	205	100,00%
* Worms	195	195	100,00%
Trojan Horses			
* Downloader	277	268	96,75%
* Dropper	678	677	99,85%
* Generic	9973	9930	99,57%
* Password-Stealer (PWS)	130	129	99,23%
Other Malware			
* Potentially Unwanted Applications (PUA)	1907	1881	98,64%
* Rogue Applications (e.g. Fake AV)	8	8	100,00%

The overall detection rate for malware is 99,48% and PUA has been detected with 98,64%.

On top of that test the false positive test was conducted with the following results.

False positives (negative)			
* … from Windows and Office installations (critical) (Win7, Win8, Office 2013 Pro)	397608	1	0,00%
* … from popular programs from major download sites (less critical)	408158	156	0,04%

One file from Windows installations was detected which could cause critical false positives and system instabilities. Furthermore 156 files from popular programs were flagged, including popular and widely used applications such as Firefox and Google Chrome. Overall the false positive rate was still acceptable though.

The detailed list of hashes/files that were used for the test and that were detected is available on request.