Independent Tests of
Anti-Virus Software

AV
comparatives

Single Product Test
Bitdefender ML engine

Offline File Detection Test for VT integration

TEST PERIOD: SEPTEMBER 2019

COMMISSIONED BY: BITDEFENDER

LANGUAGE: ENGLISH
LAST REVISION: 12TH SEPTEMBER 2019

WWW.AV-COMPARATIVES.ORG

Tested product

Bitdefender is having the test performed in order to get its machine learning (ML) engine integrated into the VirusTotal (VT) search service. According to a VirusTotal policy, any new engine to be integrated into VirusTotal requires an independent test, including an explicit check that the new solution/engine adds value to the ecosystem and does not rely on VT results (directly or indirectly). The test has to be done with the same candidate (same solution/engine) to join VirusTotal.

The ML-only SDK has been submitted for this test by Bitdefender. The ML-only engine was tested regarding its on-demand file detection capabilities the same way as it will be submitted to VirusTotal, and offline, without using any other engine or cloud services (no other engines were used).

Offline File Detection Test

An offline file detection test using 1,000 malware samples and 1,000 clean samples has been conducted. This test evaluates how effective and accurate the ML engine of Bitdefender reports malicious and clean files.

The used command line was as follows:

bdc.exe -log -r -i –deepscan -detection-clue="~=|WEAREINBUSINESS|=~" -use-system-certs %*

Test Results

Bitdefender ML-only engine
malware detection rate   **97.6%**

False Alarm rate   **21 (2.1%)**

As the test results confirm - despite being offline and relying only on the ML engine – the submitted ML engine of Bitdefender detected the majority of the malicious samples used in this test, showing that it adds value to the ecosystem. Unfortunately, in case of clean files, the ML-engine of Bitdefender wrongly alerted on 2.1% of the 1000 tested innocent files, which corresponds to a very high false alarm rate.

Copyright and Disclaimer