Kaspersky Endpoint Security for Business scored 100% detection rate in AV-Test fileless threats protection test

Kaspersky Endpoint Security for Business showed a 100% detection rate and the highest prevention rate (94.12%) of 14 endpoint security vendors in a recent assessment by AV-TEST. The products were judged on the ability to detect fileless threats and to protect and remediate malicious actions.

Fileless threats are used in many forms of malicious activity – from advanced targeted attacks to widespread malware campaigns or even generic malware, such as Trojan-clickers and adware. Kaspersky researchers are constantly revealing these threats in various attacks, such as the PowerGhost cryptominer, attacks on banks with DarkVishnya, Turla's APTs and the Platinum APT. Detection of fileless malware is more complicated than other malware because its malicious code does not store itself on a hard drive. It can exist in memory, registry, OS scheduler tasks or Windows system storages, such as WMI objects.

In its study, AV-TEST examined products for different categories of fileless attacks, including malware execution from WMI storage or by Task Scheduler, running a PowerShell script after the execution of exploits or macros. On top of these, the test also monitored for false positives. Of all the solutions tested, Kaspersky Endpoint Security for Business was the only one to detect all 33 attacks, while the average detection rate of all the products was 67.75%. As for protection and remediation, Kaspersky's product prevented 48 out of 51 malicious actions, compared to an average protection level of 59.10%. The false positive test revealed no false detection or blocks by the Kaspersky product.

According to AV-TEST, it ran this test “to discover how marketing promises of efficient fileless threat protection, claims about unbelievable advantages of some protective tools, and different ad slogans correlate with reality. This test is aimed to show what fileless malware can do and which security products are capable of detecting, blocking and remediating fileless attacks — irrespective of what is claimed by security vendors themselves”.

“Fileless threats are a growing trend in malware landscape which makes efficient protection a challenge for all endpoint protection products. This test reveals big differences in the abilities of assessed security solutions to detect fileless infection techniques. Kaspersky proved to be the most efficient in detection of and prevention against fileless attacks,” says Maik Morgenstern, Chief Technology Officer, AV-TEST.

“We appreciate AV-TEST showing the real results of cybersecurity products against current serious threats, such as fileless malware. Kaspersky researchers have been analyzing fileless threats for a long time as they are widely used in different attack stages. Whenever possible cybercriminals try to reduce their footprint and use malware which is less well-detected, making fileless a growing option. Thanks to our intelligence we have created the necessary protection technologies, such as our advanced behavior-based detection. With these technologies, our business customers will always be protected from fileless and other threats,” comments Timur Biyachuev, Vice President, Threat Research, Kaspersky.

The full report “Advanced Endpoint Protection: Fileless Threats Protection Test” commissioned by Kaspersky and performed by AV-TEST GmbH can be found here.
https://www.av-test.org/fileadmin/pdf/reports/AV-TEST_Kaspersky_Fileless_Malware_Test_Report_2019-09_EN.pdf

No product results were excluded from the report to keep the security picture complete.

For more information about Kaspersky Endpoint Security for Business please visit this page.
https://www.kaspersky.com/enterprise-security/endpoint-product