Invincea Endpoint Protection Test

A test commissioned by Invincea and performed by AV-TEST GmbH. Date of the report: May 2nd, 2016

Executive Summary

In April 2016, AV-TEST performed a review of the Invincea Endpoint protection solution to determine the malware detection and blocking capabilities. Invincea commissioned AV-TEST to run this independent test.

In order to ensure a fair review, the sponsor has not supplied any samples or had any influence or any prior knowledge regarding the samples being tested. The following test scenarios are standard tests that AV-TEST does on a regular basis for endpoint antimalware solutions:

1. **Protection:** Measuring the effectiveness of the product in protecting the system. One part is the protection against real-world attacks, such as malicious websites or e-mail attachments. The other part is the detection of widespread and prevalent malicious Windows binaries.
2. **Usability/False Positives:** False detections of legitimate software during a scan or while installing and using popular programs.
3. **Performance:** The performance impact of the security solution while performing typical tasks on a computer on two different hardware platforms.

Breaking out the data by test shows that Invincea provided a very good protection level and minimal performance impact.

	Real-World Testing	Detection of prevalent Malware
Total Test Cases	64	12,281
Detected Samples	64	12,210
Detection Rate	100%	99.42%

Figure 1: Summary of the test results for Malware blocking

	False Positives (Microsoft files)	False Positives (Popular Programs)	During Installation and Usage (Popular Programs)
Total Test Cases	397,612	100565	82
Detected Samples	0	112	1
False Positive Rate	0%	0.11%	1.22%

Figure 2: Summary of the test results for False Positives

	Old hardware	New hardware
Download files	0,32%	0,68%
Load websites	11,42%	5,37%
Install applications	4,82%	9,37%
Run applications opening specific documents	4,31%	6,29%
Copy files	6,04%	1,80%

Figure 3: Summary of the test results for Performance Testing

Overview

With the increasing volume of malware, targeted attacks and advanced persistent threats spreading through the Internet these days, the danger of getting infected is higher than ever before. In the year 2000, AV-TEST received more than 170,000 new unique samples, and in 2015, the number of new samples grew to over 140,000,000. The growth of these numbers is displayed in Figure 4.

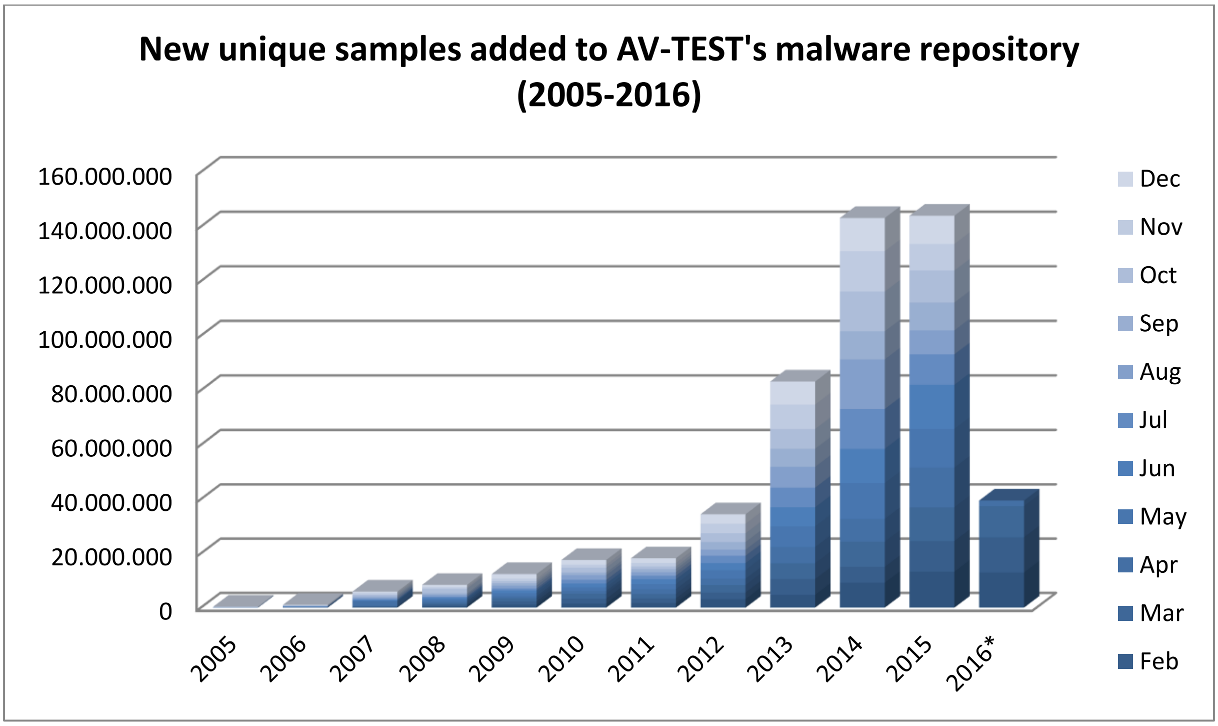

Figure 4: New malware samples per year

To protect the enterprise network against the enormous number of threats a well working endpoint protection is required. Old approaches such as simple static signatures are not enough anymore to protect against mass attacks as well as targeted attacks. Products need to deliver protection with different layers: static signatures, heuristics, dynamic detection, URL blocking, reputation and possibly more.

A clever combination of those layers makes it hard for the attacking site to infiltrate the enterprise network.

Product Tested

The product Invincea Enterprise in Version 6.0.0.22576 was tested.

Methodology and Scoring

Platform

The test has been performed on several PCs with identical hardware, running Windows 7 Ultimate, SP1 (64-Bit). The hardware platform for the tests was as follows:

- Older standard business PC: Intel Xeon X3360 @ 2,83GHz, 4 GB RAM, 500 GB HDD
- Recent High-End PC (for Performance testing only): Intel i7 3770 @ 3,40GHz, 16 GB RAM, Samsung 512 GB SSD

Testing methodology

Invincea provided help in setting up the product and configuring it. The test itself has been performed by AV-TEST engineers according to the methodologies described at https://www.av-test.org/en/test-procedures/test-modules/

Test Results

The following table shows the individual results of Invincea vs. the average results from the public tests that AV-TEST performed in Nov/Dec 2015 (11 products)[1] and Jan/Feb 2016 (12 products)[2] for enterprise protection products. Please note that the test sets and samples were different for all three tests. Also the performance test was changed in the 2016, so there are no values from Nov/Dec 2015.

	Invincea	Nov/Dec 2015	Jan/Feb 2016
Protection			
Real-World Attacks	100%	97.9%	98.1%
Prevalent Malware	99.4%	99.9%	99.8%
Usability/False Positives			
Critical files from Windows/Office	0	0	0
Less Critical files from popular programs	112	6	2
False Warnings during the execution and Usage of Programs	0	0	0
False Blockages during the execution and Usage of Programs	1	0	0
Performance			
Total Impact Old Hardware	5,38%	-	16.16%
Total Impact New Hardware	4,70%	-	18.93%

Figure 5: Test Results compared to Nov/Dec 2015 and Jan/Feb 2016 average results

Protection Results

In this test the product had to protect against 64 malicious websites. Invincea managed to block all the attacks and no infection occurred. Comparing this to previous published AV-TEST results from Nov/Dec 2015 and Jan/Feb 2016 shows that 100% protection is not the standard yet. The average was 97.9% in Nov/Dec and 98.1% in Jan/Feb 2016. So 100% detection and blocking can be considered very good.

The second part of the protection test involved 12,281 widespread and prevalent malicious files that had to be detected either by a scan or during execution. Invincea managed to detect 99.42% of the files. This is only slightly below the average of the Nov/Dec 2015 and Jan/Feb 2016 test, but still a very good result.

False Positive Results

The static false positive testing has been carried out against 397,612 critical files from Windows and office installations. No false positives occurred here. A second test set consisted of 100,565 files from popular programs downloaded from major download sites. Invincea detected 112 files as malicious or unwanted. This is the only part of the testing where Invincea showed a weakness. However, in a

[1] https://www.av-test.org/en/antivirus/business-windows-client/windows-10/december-2015/
[2] https://www.av-test.org/en/antivirus/business-windows-client/windows-7/february-2016/

business environment the risk of false positives is much smaller, as the average user is usually not allowed to install additional software.

A further test involved the installation and usage of 41 well known products such as 7-Zip, Adobe Reader, Java JDK or Google Chrome. During this test we check for warning messages or wrong blockings of certain action. Invincea blocked the installation of one product: HD Clone 6.0.5

As mentioned before, in a business environment these kinds of false positives are probably not a big problem. Should they occur, the system administrator can easily whitelist those cases for proper usage.

Performance Results

The performance tests are run on older and newer hardware to cover the different hardware platforms that are in use in different companies. In both cases the performance impact of Invincea was minimal and actually one of the best values we have experienced in our tests so far. There were no notable problems anywhere and the impact was a lot less than the average impact we measured in the public Jan/Feb 2016 testing of other products.

Summarized Score

When publishing results, AV-TEST translates the detection rates etc. into a score from 0 to 6, where 6 is the best possible result. If this is done with the Invincea results the following scores would be achieved:

- Protection: 5.5
- Usability/False Positives: 4
- Performance: 6

This allows a rough comparison with the Nov/Dec 2015 and Jan/Feb 2016 results, see tables below. Please note that different test sets have been used and the tests ran on different dates. Also the performance test has been updated for 2016. So the results are not directly comparable, but give a first indication how products would compare.

November and December 2015	Protection	Usability	Performance	Total
Bitdefender	6	5.5	6	17.5
Cylance	5.5	4	4	13.5
F-Secure	6	5.5	4.5	16
G Data	5.5	4.5	5.5	15.5
Kaspersky	6	6	6	18
Intel Security	5.5	5	6	16.5
Microsoft	4.5	4.5	6	15
Seqrite	4.5	3	5.5	13
Sophos	6	5	5.5	16.5
Symantec	6	5.5	5.5	17
Trend Micro	6	5.5	6	17.5
Invincea (April private test)	5.5	4	6	15.5

Figure 6: Test Results compared to Nov/Dec 2015

January and February 2016	Protection	Usability	Performance	Total
AVG	6	5	6	17
Bitdefender	6	5.5	6	17.5
F-Secure	6	6	5	17
G Data	5.5	5	6	16.5
Kaspersky (Endpoint)	6	5.5	6	17.5
Kaspersky (Small Office)	6	6	6	18
Intel Security	5.5	5	6	16.5
Microsoft	3	5	6	14
Seqrite	4	3.5	5.5	13
Sophos	5	4	6	15
Symantec	6	5.5	6	17.5
Trend Micro	6	4.5	6	16.5
Invincea (April private test)	5.5	4	6	15.5

Figure 7: Test Results compared to Jan/Feb 2016

Summary

The results illustrate that Invincea is able to provide the same level of protection as other products that are regularly included in AV-TEST public comparative tests. The performance impact was also minimal and one of the best values we ever measured. Only the false positive testing revealed a few weaknesses. This is something that can be improved in feature. However even now those false positives shouldn’t be a big problem in business environments as they occurred primarily on consumer software and could easily by whitelisted by a system administrator.