Comparative Remediation Testing Report

A test commissioned by Enigma Software Group and performed by AV-Test GmbH
Date of the report: October 17th, 2017, last update November 27th, 2017

Executive Summary

In August and September 2017, AV-Test performed a comparison test on the remediation capabilities of SpyHunter by the Enigma Software Group. The test was run on a clean Windows 7 (SP1, 64-bit) system and the same disk image was used on several identical PCs.

The malware test corpus for the remediation test consisted of 20 samples and was divided into two parts. Test Part 1: First, the image was infected with one of the malware samples. The next step was to try to install the security product, scan the PC and remove any threats that were found. Test Part 2: First, the AV software was disabled so that the system could become infected. The AV software was then enabled again and a reboot was performed in order to ensure that all components of the AV software were working correctly. The next step involved trying to remediate the system and performing an additional system scan.

Test part 1: The product that achieved the best score was Bitdefender with a total of 98.33%. SpyHunter also achieved a very good score of 95% and cleaned all active components of the malware, only leaving three inactive components on the system. The third-placed product from Trend Micro also performed well, achieving a score of 92.50%. Emsisoft and Malwarebytes followed with scores between 87 and 88%, while IObit lagged a long way behind with a score of just 1.67%.

Test part 2: This part of the test showed the same order of results as observed in part 1. Bitdefender achieved a very good score of 98.33% followed by SpyHunter, which also performed well and achieved a score of 96.50%. Both products were able to clean all active parts of the malware and left only a created task (Bitdefender) or files in the temp folder (SpyHunter) on the system. Trend Micro came in at third place with a good score of 91.67%, while Emsisoft Anti-Malware and Malwarebytes Premium achieved an acceptable score of 88.33%. With a score of just 1.67%, IObit again lagged a long way behind.

Overview

With the increasing number of threats that are being released and spreading through the Internet in the present day, the danger of systems becoming infected is also increasing. A few years back, new viruses were released every few days but it is now the case that several thousand new threats are occurring every hour.

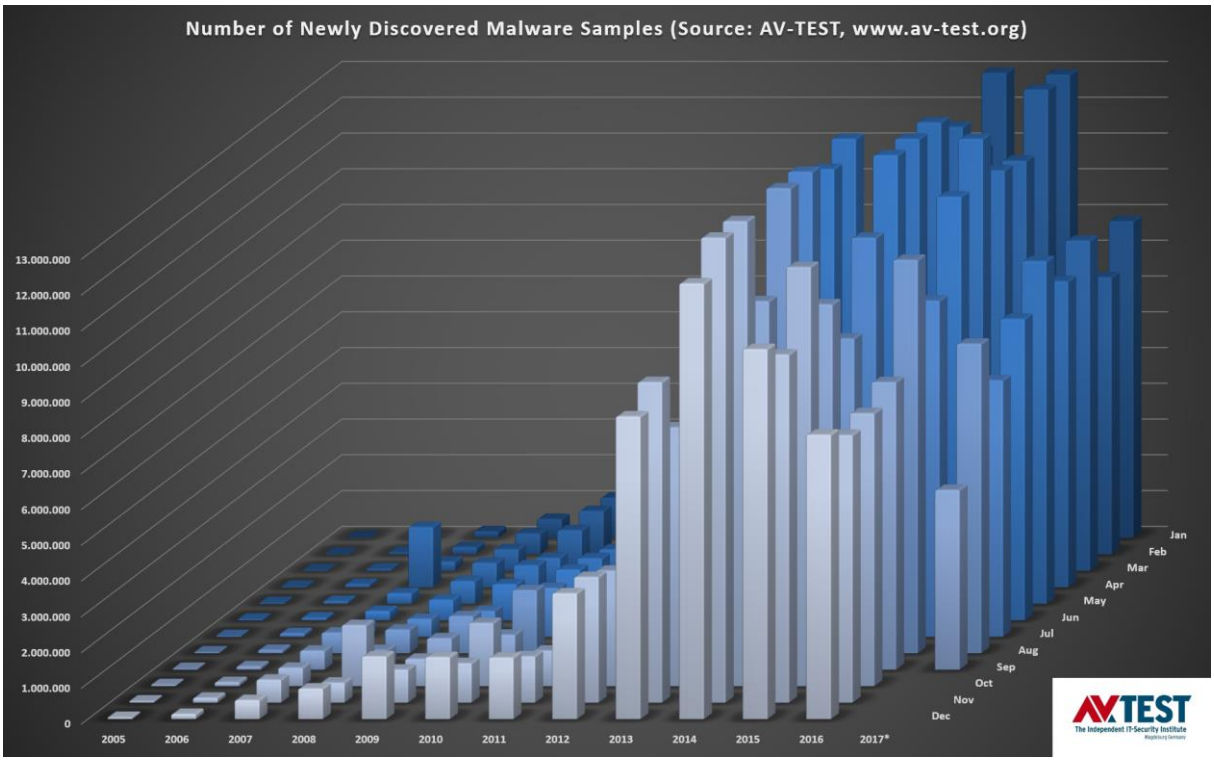

Figure 1: New samples added per year

In the year 2000, AV-Test received more than 170,000 new samples, and in 2013, the number of new samples grew to over 80,000,000. The numbers have continued to grow in the year 2017, as can be seen in Figure 1. AV-TEST currently has more than 670 million malware samples in its database.

The volume of new samples that have to be processed by anti-malware vendors in order to protect their customers can create problems. It is not always possible to successfully protect a PC in time. A PC may get infected even if up-to-date anti-malware software is installed because signatures are only provided every few hours, which sometimes may be too late. Infections lead to financial loss, either because sensitive data is stolen or because the PC can no longer be used for productive work until the malware has been completely removed from the system.

Remediation techniques have therefore become more important in order to get an infected PC up and running again. When using such techniques, it is imperative that the cleaning process is reliable in two ways:

1. The malware and all of its components have to be removed and any malicious system changes have to be reverted.

2. No clean applications or the system itself is allowed to be harmed by the cleaning process.

Products Tested

The test was performed in August and September. AV-TEST used the latest releases of the following software available at the time of the test:

- Bitdefender Internet Security
- SpyHunter by Enigma Software Group
- Emsisoft Anti-Malware
- IObit Malware Fighter
- Malwarebytes Premium
- Trend Micro Internet Security

Methodology and Scoring

Platform

All tests were performed on identical PCs equipped with the following hardware:

- Intel Xeon Quad-Core X3360 CPU
- 4 GB Ram
- 500 GB HDD (Western Digital)
- Intel Pro/1000 PL (Gigabit Ethernet) NIC

The operating system was Windows 7 (SP1, 64-bit) and only contained the hotfixes that formed part of this version and all patches that were available on August 4, 2017.

Testing Methodology

The remediation test was performed in ten steps, following the methodology described below:

1. **Clean system for each sample**. The test systems were restored to a clean state before being exposed to each malware sample.
2. **Physical machines**. The test systems used were actual physical machines. No virtual machines were used.
3. **Internet access**. The machines had access to the Internet at all times in order to use in-the-cloud queries if necessary.
4. **Product configuration**. All products and their accompanying remediation tools or bootable recovery tools were run with their default, out-of-the-box configuration.
5. **Infection of test machines**. A native machine was infected with one threat and then rebooted. It was necessary to make sure that the threat was fully running.
6. **Sample families and payloads**. The tested samples did not come from the same family or have the same payloads.
7. **Remediation while using all available product capabilities**.
    a. Try to install the security product using the default settings. Make sure to follow the complete product instructions for removal.
    b. If a. does not work, try using a ***stand-alone fix tool/rescue tool*** solution (if available).

c. If b. does not work, launch the stand-alone ***boot solution*** (if available) and use it to remediate.

8. **Validate removal**. The PC was manually inspected in order to validate proper removal and artifact presence.
9. **Score removal performance**. The effectiveness of the tool and the security solution as a whole were evaluated using the agreed scoring system.
10. **Overly aggressive remediation**. The test also measured the aggressiveness of a product during remediation. Some products, for example, will completely remove the hosts file or remove an entire directory when it is not necessary to do so for successful remediation. This type of behavior should count against the product.

Efficacy rating

For each sample tested, points were awarded according to the following system:

a. Malware completely removed (3)
b. Malware detected and removed, only inactive traces remained (2)
c. Something detected and partly removed, but malware traces were still active (1)
d. Malware not detected, nothing remediated (0)

The scoring should not take into consideration which of the available techniques were needed to remove the malware. All techniques, however, should be applied. When a product cleans out the entries in the hosts file that relate to that very product and leave the machine uninfected and the product functional and updateable, it should be given full credit for remediation even if entries for other security vendors remain in the hosts file.

Samples

The set contained 20 malicious files that were able to infect Windows 7 (SP1, 64-bit).

Test Results

Bitdefender performed best in this test and achieved 118 out of a total of 120 possible points. SpyHunter came in at second place with a good result of 115 points, closely followed by Trend Micro Internet Security, which also achieved a good score of 111 points. The products in fourth and fifth place are Malwarebytes Premium with 106 points and Emsisoft Anti-Malware with 105 points. IObit Malware Fighter only managed to score two points out of the total of 120 points available.

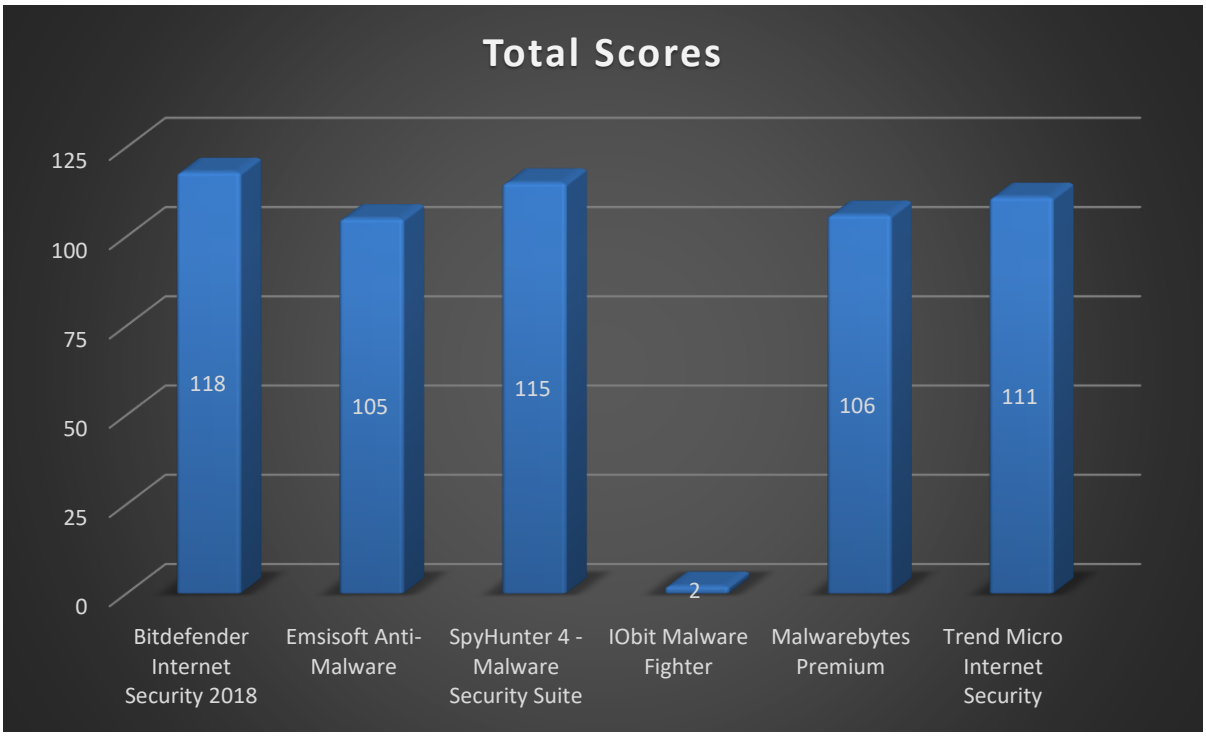

Figure 2: Total remediation scores – parts 1.1 + 1.2

The results of parts 1 and 2 of the test are nearly identical, as can be seen in Figures 3 and 4. The maximum number of points achievable in parts 1 and 2 of the test was 60.

Bitdefender achieved a nearly perfect score of 59 points in both parts of the test and only left one created task file on the system in each part. SpyHunter also achieved a good score of 57 points in part 1 of the test and a very good score of 58 points in part 2. In both parts of the test, SpyHunter left inactive components in the system's temp folder, as well as two inactive executables in part one.

The third-placed product is Trend Micro Internet Security with 56 points in part 1 of the test and 55 in part 2. Trend Micro was unable to clean one sample in both parts of the test. Malwarebytes achieved a good score of 53 points in both parts of the test and also cleaned all of the active components of the malware. Emsisoft followed closed behind with only one point less after achieving 52 points in part 1 and 53 in part 2 of the test.

The product with the worst result was IObit, which only achieved one point in each part of the test. IObit was unable to clean 19 of the 20 samples tested.

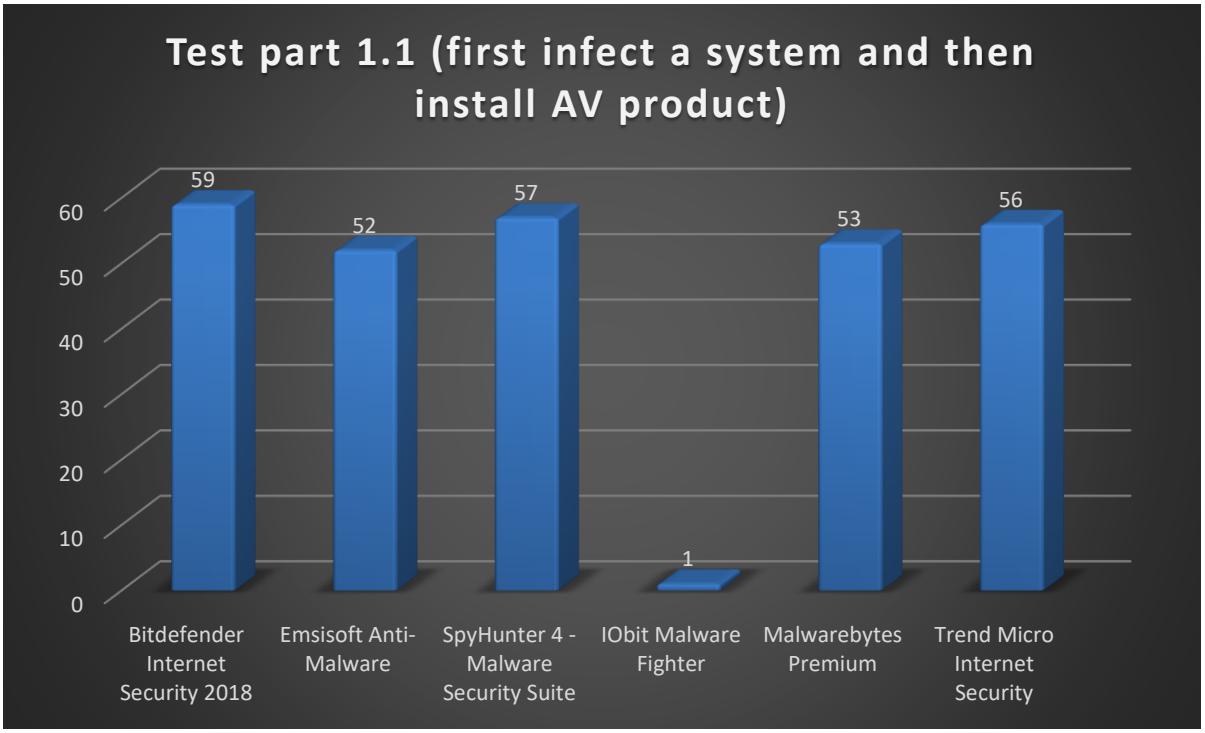

Figure 3: Remediation scores – test part 1.1

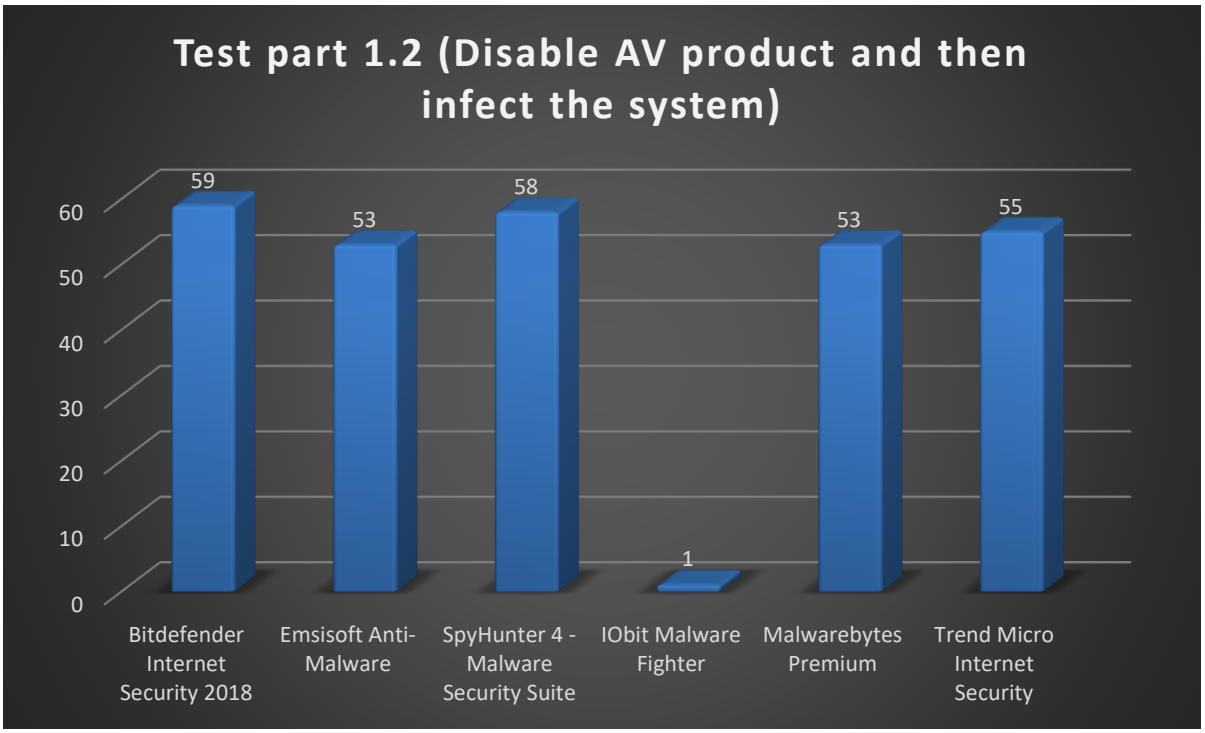

Figure 4: Remediation scores – test part 1.2

Appendix

Version information of the software tested

Developer, distributor	Product name	Program version	Engine/signature version
Bitdefender	Internet Security	22.0.8.118	7.72906
Emsisoft	Anti-Malware	2017.7.0.7838	4.0.1.883/20170824
Enigma Software Group	SpyHunter 4	4.28.5.4848	2017.08.23v01
IObit	Malware Fighter	5.2.0.3992	1679
Malwarebytes	Malwarebytes Premium	3.2.2.2018	n/a
Trend Micro	Internet Security	11.1.1045	9.900.1004/13.611.95

List of malware samples used in the remediation test

(SHA256)
* 0x0295885f04a0c58eed9b64ff54acc493ace4ab1265e8ce16a7e4143d1a9c3e75
* 0x17bf5bdea2138d265fa42a0afd8569dbc57870e6c43f9afca5fdef4adf753c61
* 0x220c3ca396726cd13de60ba1207ff28555771e16944fa3d525490c83dbaefcfe
* 0x2f478c2377e85b68fee3ca05a1d90a968e063669fc7dbd94e96219fbede57cb2
* 0x3ff811769f05694868edb4bd217cf292064d9aac9cfa96dcbc371b1e8427e399
* 0x4ad3552847f32638536401ed3785d5c3281f2d96ce0f2aad7ea25b2108576aee
* 0x5b7f3a5714895e8154e8a82d930d76b5d6beed589341ad01c7ff93af6088ab96
* 0x6ca192242ef08a32e287f4fd9119db92c8ad0c19f4cc3860e86711c6fee13c1d
* 0x7c70d922054d201ee2e04e9cff4b67bf82c99705b8401c1dcb308e1206bdc4b0
* 0x8520ab735a4902da6cbb7fd99d7c67580d5b9c98a36552896512f8da4931192c
* 0x8dc371b12dd48be1ae647a045684a243d89a85010f3cb8b8fa53cf315cb7e2c6
* 0x9872814915ee58abd8bab6e6eb40a1dd14049d9ac62f4f8ca76e7b7b1b4c7d79
* 0xa18e329dd10e8b2da5980836bdee6924513efe3c808896757939b96a989d18b1
* 0xb4b60bfa28c2be1f912ca27b7016476b26029cbc5d5dff298fce8bad9039f13f
* 0xc6e87ce6fb9076c87024cd27bcea510de925b3cf1dd65be1d52ae8b06ba902a4
* 0xdae8ceba81dbcbccaefb297b15eb86a61e95ae40a1654f96e8c53d765bd18cd2
* 0xdd519253f01d706573215f115528c59c606107a235f6052533226d0444731688
* 0xe08d42bdd0aff3c5d52a196b3981f8e6fccbc70819da90c2d29ac58c456ab818
* 0xf4083e48161ed3313b27a40712c930de229cc75eb969d91b78689462a76f6fc4
* 0xf61bd77c459db0bb703759869d3c5f140c6b093c092e87806bec5eeac9763bc7