Remediation Testing Report

A test commissioned by Enigma Software Group and performed by AV-TEST GmbH
Date of the report: September 03th, 2018, last update September 04th, 2018

Executive Summary

In August 2018, AV-TEST performed a test on the remediation capabilities of SpyHunter by the Enigma Software Group. The test was run on a clean Windows 10 (RS3, 64-bit) system and the same disk image was used on several identical PCs.

The malware test corpus for the remediation test consisted of 12 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.

SpyHunter achieved a perfect result with 100% in both parts of the test. The Enigma software cleaned all active components as well all artifacts of the malware from the system.

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.

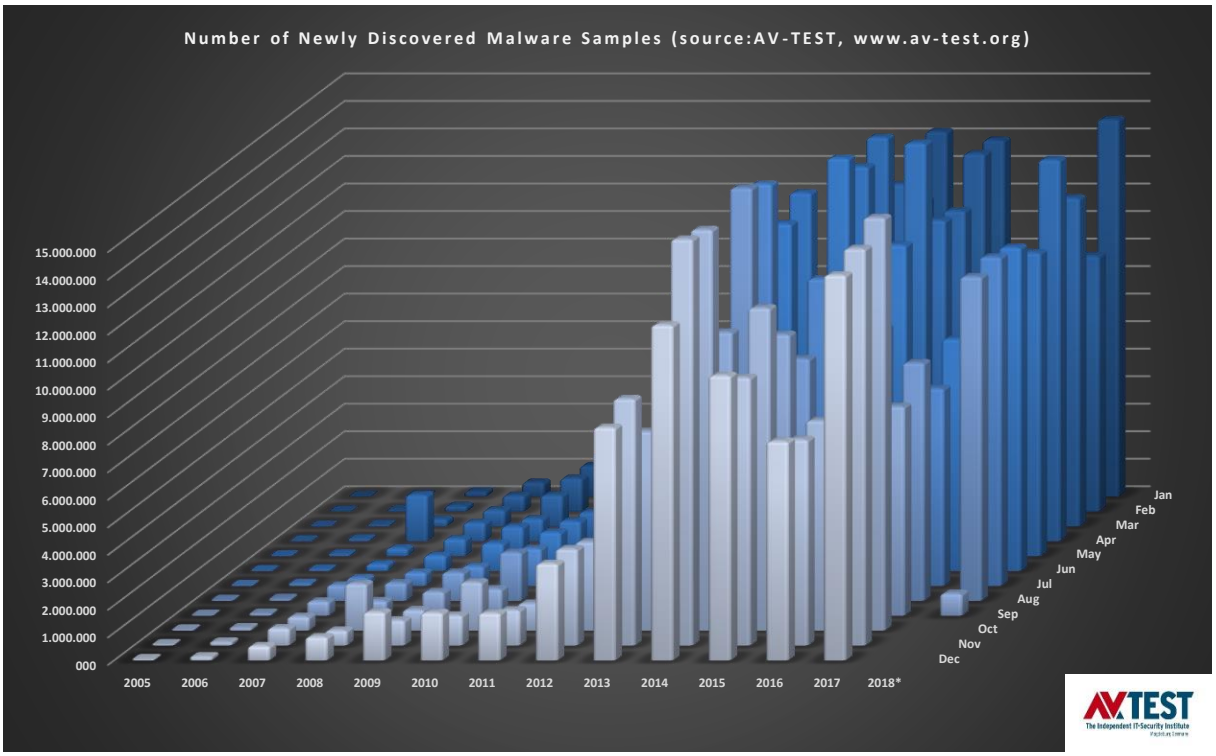


Figure 1: New samples added per year

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 continued to grow in the following years, and the development of their growth can be seen in Figure 1. AV-TEST currently has more than 800 million malware samples in its database, and in the first half of 2018, the AV-TEST detection systems registered about 10 million new samples per month.

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

Product Tested

The test was performed in August 2018. AV-TEST used the latest release of the following software available at the time of the test of:

- SpyHunter by Enigma Software Group

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 test was conducted in August 2018. AV-TEST used the latest version of the following software, which was available at the time of testing.

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 12 malicious files that were able to infect Windows 10 (RS3, 64-bit).

Test Results

Enigma Software Group scored perfectly with100% in the first and second part of the test. The results of both test parts can be seen in Figure 2.

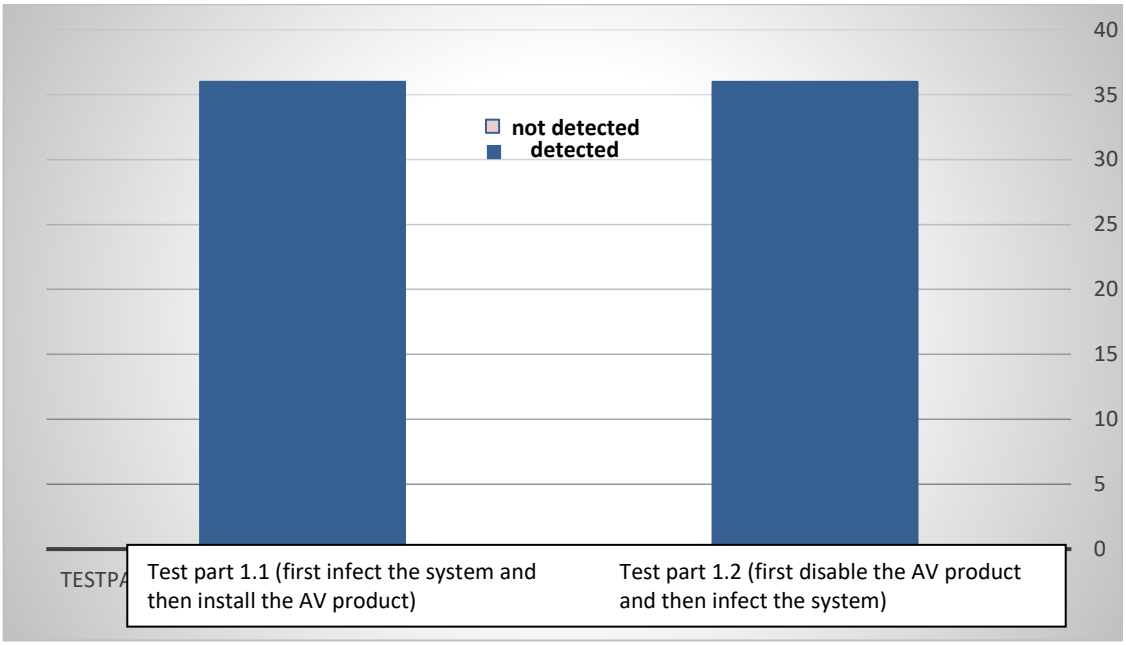
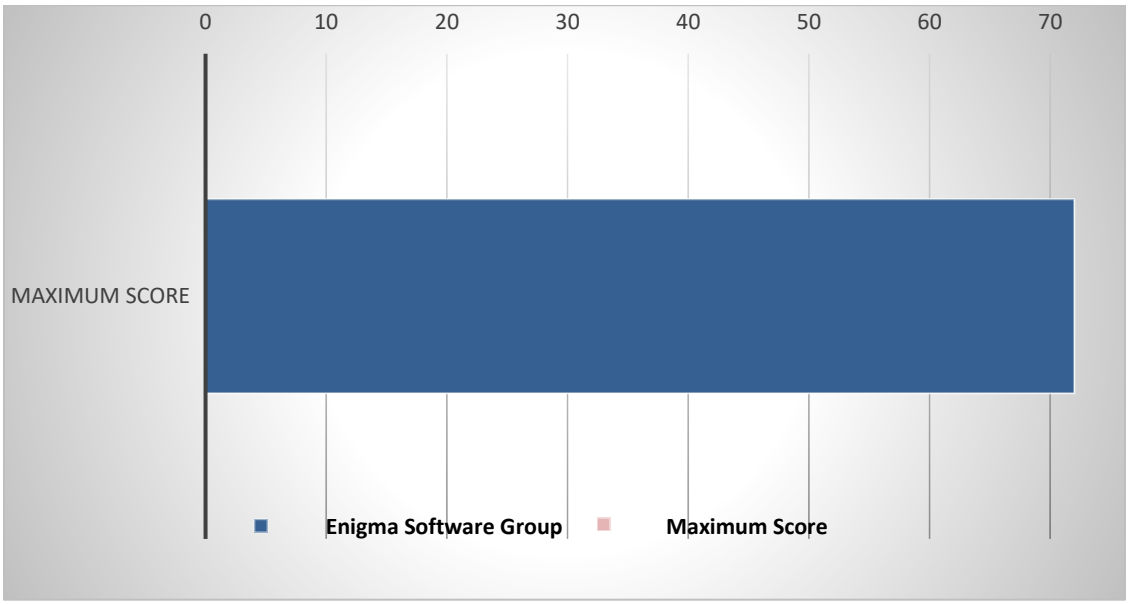


Figure 2: Remediation score – test parts 1.1 +1.2

In terms of cleaning efficiency, SpyHunter was able to completely clean the system in 12 of the 12 tested samples. Also all artifacts and registry entries were also cleaned perfectly.

The maximum score available was 72. As can be seen in Figure 3, Enigma Software Group achieved the excellent overall score of 72.



Appendix

Version information of the tested software

Developer, distributor	Product name	Program version
Enigma Software Group	SpyHunter 5	5.0.30.51

List of malware samples used in the remediation test

(SHA256)
0x0bf737607d46bfa4434a8d62b2376b9fdd4b013bb1614bd5f089fa332feef0b2
0x179cb0ba8030ee09e2e7d5be3a9d0f1b20663a5e1f49e8d1d876b3f76e088476
0x3c5fc8acd9a0ef88795d2592fee6a20be800a3874a40f672700bf23707ca9f82
0x4ff747afb05bc711742f3617d92735a8435eb16c8954dbfe1e558cb7b5de7c3d
0x5400e496f79ad8d09b6be069ca680af2e359f81625993e15fa52a09b1444f78b
0x6287b31e3681973ecfc969ce082cc195badd8f571ce057695a021c9227ee63d4
0x6abef4b7e1d91fc80c7f83cfebffa1ac129333c4acb8e7779bd646a1e66129c3
0x7e8a7fd6bb805f8bd42d30c17490b9bd0a9602485efcb708abfca3e1d5b16c01
0xa058357700d6bbec06232492c40a88487f57e343f7a7c6180582b4d83714f1bd
0xc3519c9fc77812b3ad088174729fc3f712de69505659f73e4d277af6b4ba31ab
0xe67ddfdfdca394eb8a4ebf7fe64c7dc7459df1b3b050e680ce94ab51a2e54c0c
0xf4e496f3a1d094eddf13a93e92e22dbc6a224aa8e8e8664fdf7fdbb4b456485c