# Remediation Testing Report

A test commissioned by Enigma Software Group and performed by AV-TEST GmbH
Date of the report: August 20th, 2018, last update August 28th, 2018

## Executive Summary

In July 2018, AV-TEST performed a test of Enigma Software Group SpyHunter remediation capabilities. The test has been run on a clean Windows 10 (RS3, 64-bit). 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 trying to install the security product, scanning the PC and removing any threats that have been found. Test Part 2: In the second part the AV was disabled to infect the system. Then the AV was enabled again and to ensure that all components of the AV are enabled correctly a reboot was performed. The next step was trying to remediate the system and performing a system scan additionally.

SpyHunter scored very good in both test parts and managed to clean 10 out of 12 samples completely. All active parts of the malware were cleaned by SpyHunter.

## Overview

With the increasing number of threats released and spread through the Internet these days, the danger of getting infected increases as well. A few years back new viruses were released every few days. Nowadays, there are several thousand new threats per hour.

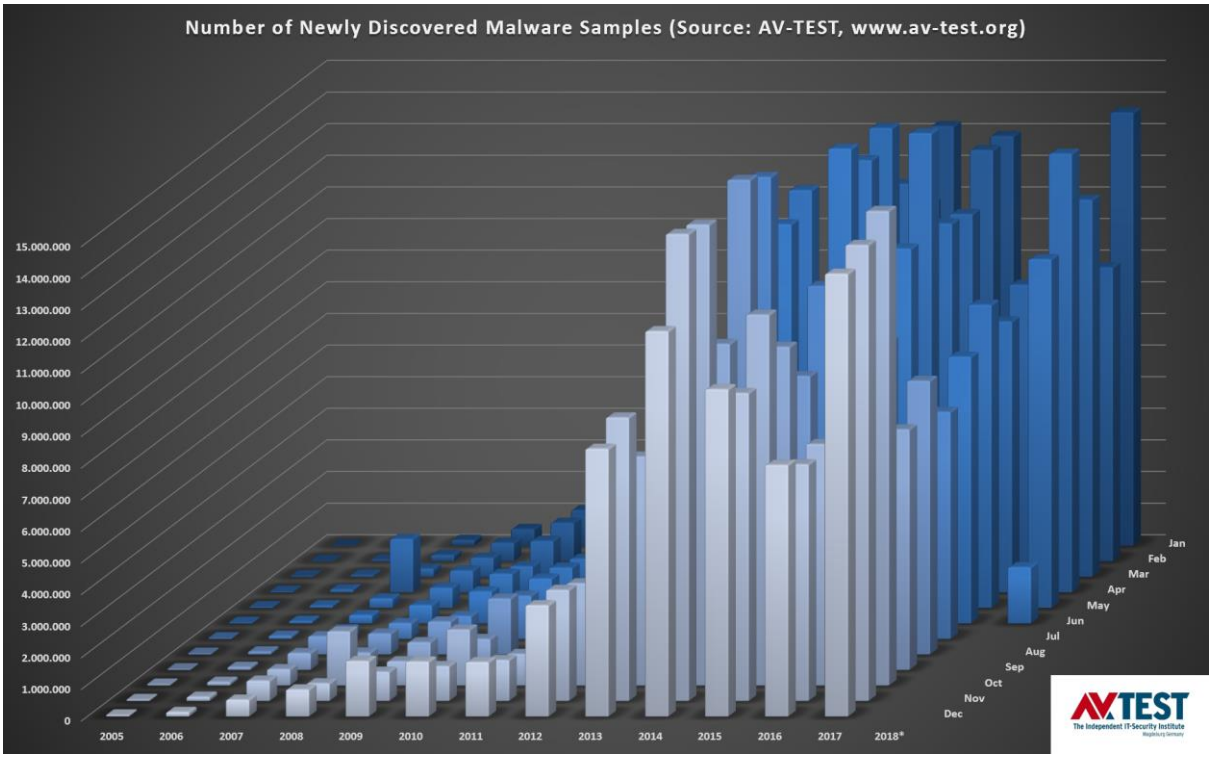


**Figure 1: New samples added per year**

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 new samples. The numbers continued to grow in the year 2016. The growth of these numbers is displayed in Figure 1. AV-TEST currently has over 800 million malware samples in its database and in the first 6-month of 2018 the AV-TEST detection systems have seen 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. It is possible that a PC can get infected, even if up-to-date anti-malware software is installed because signatures are provided only every few hours, which sometimes may be too late. Infections create financial loss, either because sensitive data is stolen or because the PC cannot be used for productive work anymore until the malware has completely removed from the system.

Therefore remediation techniques become more important to get an infected PC up and running again. In that process 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 must be harmed by the cleaning process.

## Products Tested

The testing occurred in July. AV-TEST used the latest releases available at the time of the test of:

- Enigma Software Group SpyHunter

## Methodology and Scoring

### Platform

All tests have been 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 10 (RS3, 64-bit) with only those hotfixes that were part of this version as well as all patches that were available on June 4th 2018.

### Testing methodology

**The remediation test has been performed accordingly to the methodology explained below.**

1. **Clean system for each sample**. The test systems should be restored to a clean state before being exposed to each malware sample.
2. **Physical Machines**. The test systems used should be actual physical machines. No Virtual Machines should be 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. **Infect test machine**. Infect native machine with one threat, reboot and make sure that threat is fully running.
6. **Sample Families and Payloads**. No two samples should be from the same family or have the same payloads.

7. **Remediate using all available product capabilities**.
    a. Try to install security product in default settings. Follow complete product instructions for removal.
    b. If a. doesn't work, try ***standalone fixtool/rescue tool*** solution (if available).
    c. If b. doesn't work, boot standalone ***boot solution*** (if available) and use it to remediate.
8. **Validate removal**. Manually inspect PC to validate proper removal and artifact presence.
9. **Score removal performance**. Score the effectiveness of the tool and the security solution as a whole using the agreed upon scoring system.
10. **Overly Aggressive Remediation**. The test should also measure how aggressive a product is at remediating. For example some products 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 are applied accordingly to the following schedule:

a. Malware completely removed (3)
b. Detected and removed, only inactive traces remain (2)
c. Something detected and partly removed, but malware traces are still active (1)
d. 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 should however, be applied. When a product cleans out the entries in the host's 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 host's file.

### Samples

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

## Test Results

Enigma Software Group achieved in the first and second test part a very good score of 97,2%. Both can be seen in Figure 2.

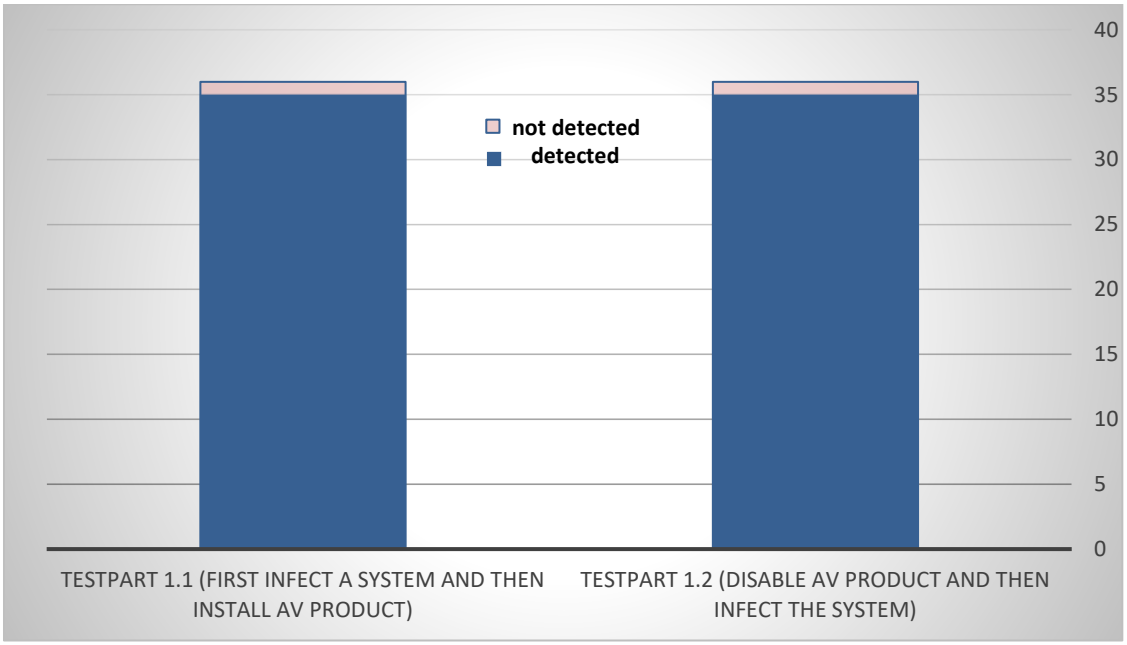


Figure 2: Remediation Score – Part 1.1 +1.2

In terms of cleaning efficiency, SpyHunter was able to completely clean the system in 10 out of 12 tested samples.

And only for one sample in both test parts, SpyHunter could not clean the registry entries of the malware, resulting in a minimal point deduction.

The maximum score that could be reached was 72. The overall score of Enigma Software Group was 70 as shown in Figure 3.

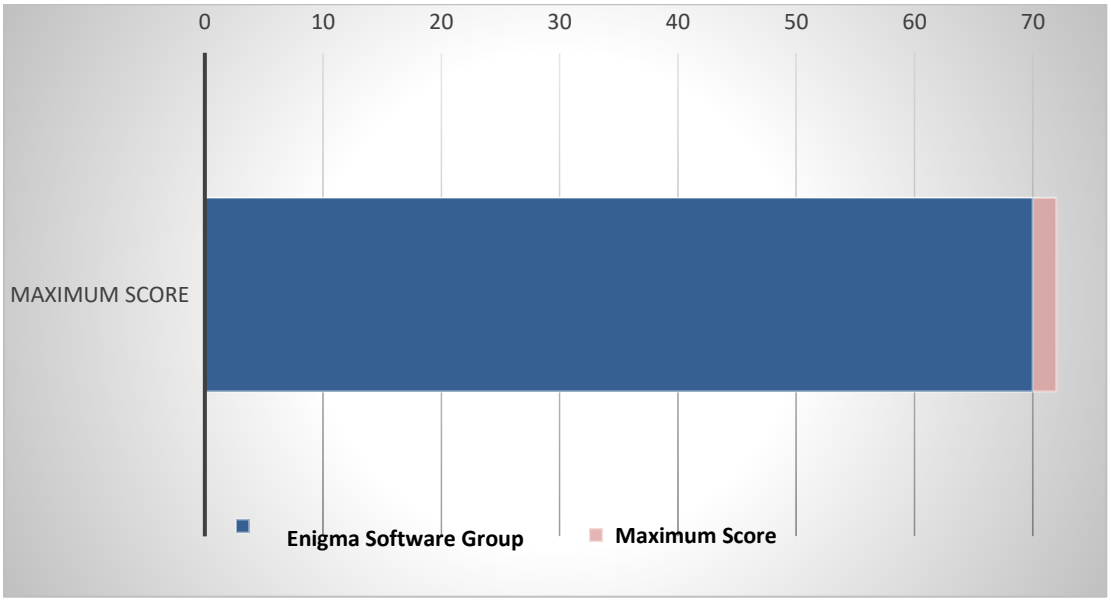


Figure 2: Remediation Score – Maximum Score

# Appendix

## Version information of the tested software

| Developer, Distributor | Product name | Program version |
|---|---|---|
| **Enigma Software Group** | SpyHunter 5 | 5.0.30.51 |

## List of used malware samples (Remediation Test)

| (SHA256) |
|---|
| 0x10864dff8bcea96f842f6642bca59199b677e28e6e174c3e4d7b65391b0698b0 |
| 0x2942841f850c59c1f7bedd1922aca54c886bad1eb51b90b32af7d6b6b6e5cab4 |
| 0x5ba58146b785d5e72993430d95960486cbf9bf9429e5e3bf4fa2fe2e88f4e250 |
| 0x69bb101c4c53fe2a87ed2200dd46b7d82d92c86943e47a31ce7922455b92d345 |
| 0x70179938e6c056df16b1403615cc553a10a90297601446f95d6ad004ca1e29eb |
| 0x86958f2f177eed14d6164d48a18cb15c12516bdb59f1125471d966f3e212b989 |
| 0x980f254b3954b3d7ded9772cad328d6872491fbd645ac3dae3d277620cfb88b7 |
| 0xac186a20bbec078f08788cc8a4a746de0139a061a6d2588787d217f019c2eb90 |
| 0xb3548b485e919e043b935b071ad54f37e1c996046fcfbefae51d76a437ee6a93 |
| 0xd8a3f066a3b961b4c8623e0d30e3e867fd7a1c9187aa396de8457df70b602efe |
| 0xe275e10bea80834252aea1b5dba9a817b278b5c4a6d0594b01b1605de0b66f79 |
| 0xf92dd910c0c00e5924a27bbffcdb303e5f724b3caf540e844c3f82a291cc7a30 |