Executive Summary

In January 2017, AV-Test performed a test of Enigma Software Group SpyHunter remediation capabilities. The test has been run on a clean Windows 7 (SP1, 64-bit). 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 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 perfectly in both test parts and managed to clean 20 out of 20 samples completely in part 1 and part2.

SpyHunter cleaned all active parts as well all dropped files of the malware on the system.
Overview

With the increasing number of threats that is being released and spreading through the Internet these days, the danger of getting infected is increasing as well. A few years back there were new viruses released every few days. This has grown to several thousand new threats per hour.

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 continue to grow in the year 2016. The growth of these numbers is displayed in Figure 1. AV-TEST currently has over 600 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. 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 January. 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 7 (SP1, 64-bit) with only those hotfixes that were part of this version as well as all patches that were available on January 3rd 2017

Testing methodology
The remediation test has been performed according 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, apply points according to the following schedule:

a. Malware completely removed (3)
b. Detected and removed, only inactive traces remains (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 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

Enigma Software Group achieved in the first and second test part a perfect score of 100%. Both can be seen in Figure 2.

Figure 2: Remediation Score – Part 1.1 +1.2

The maximum score that could be reached was 120. The overall score of Enigma Software Group was 120 as can be seen in Figure 3. Regarding the cleaning efficiency in the Test Part 1.2 the system was completely cleaned by Spyhunter.

And also on the test part 1.1 Spyhunter scored perfectly and cleaned the infected system completely.
Appendix

Version information of the tested software

<table>
<thead>
<tr>
<th>Developer, Distributor</th>
<th>Product name</th>
<th>Program version</th>
<th>Engine/ signature version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enigma Software Group</td>
<td>SpyHunter 4</td>
<td>4.24.3.4750</td>
<td>2017.01.17v01</td>
</tr>
</tbody>
</table>

List of used malware samples (Remediation Test)

```
(SHA256)
0x0248ae5f55dd424770217a568e6d6e621b08f010faecc3bd889e815bdba562b7
0xe9b94aa0d8f1fe0c8f75faad8fe213cc982678925e883199d4e73316830e27
0x379d26795c02cd0285fc33210b598228a82f3f9926bac3566e8e1044c30f496
0x3963f7595ab1c34f6e7ae23424bb2631d24908c3c25bb5b70f3bfa8403f63e7a8
0x496baddd81a03f9a74f3fc312225b876dc6aaf61e224e2328f3b3f3853
0xe5212dc2bb56db362abdb2ed33bcb871151c11a1a7b6f1c16d5a843ae7bc4
0x455bf64160044d9a769ab277f85ba954e2a2e182c6da4d0672790cf1d48309
0x534ceec806ee84ae7f5fdd2e3f1c837cb1e263f52e03a733666a199f45456afcf2
0x5847e0b5f7279000e7335a0b0925b413718810cf5591d8ea253ae55893a197
0x6b17b1dc8eb3b0ae6412bd2d7fe73832e9b4cb2a59d9d13e46427401c4145
0x73e7b43fed5fe22d58ba0c36080eb70f00640ea9e615d8e5ce1785d76df2a76
0x814dfc756520e8bc86f8f54a352d17bb7636333a206c27bc0710320fabd279
0x90c1e0eb0e8b37300e2177b465b9289daa9102df2a6b56e63f3504958f7a71bc8
0x93133393d7088136994f0f613083fc393e17ee99c10bc2d2e0a8038816b1c289
0x3b3c5f67fb188ba39277b33d0a89b2f079a72a3583ad663df5d806c49546
0x132ee2f13c42925717274da35c41461ab9d947533163da315474ca40b8161f6
0xd861451df5ee19419a829b2db0d622ce9e1edc6e9f16a52f57ee0744771ae76
0x2ce09e14d11d6217853b7ef22bf31e0c58f9d2048782e2e28e6f9e1eba782
0xfed13e753e4b879610a02dbd77212a6bdf637e6c288a48672276bb96d24d2
0x937b95df816eed946a50284f4фе9185baf3cc6c6bc66047331cfb35a2654a
```

Copyright © 2017 by AV-Test GmbH, Klewitzstr. 7, 39112 Magdeburg, Germany
Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web http://www.av-test.org