Remediation Testing Report

A test commissioned by Enigma Software Group and performed by AV-Test GmbH
Date of the report: May 19th, 2016, last update May 24th, 2016

Executive Summary

In April and May 2016, 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 managed to clean 19 out of 20 samples completely in part 1 which is a very good result. For part two 16 out of 20 samples were cleaned. This is still a good result.

SpyHunter cleaned the active parts of the malware on the system. The most leftovers are dropped executable files of the malware into the “C:\Users\vtc\AppData\Roaming\” folder on the system. Only for one test case SpyHunter could not clean the active components of the malware and the system is still infected.

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.

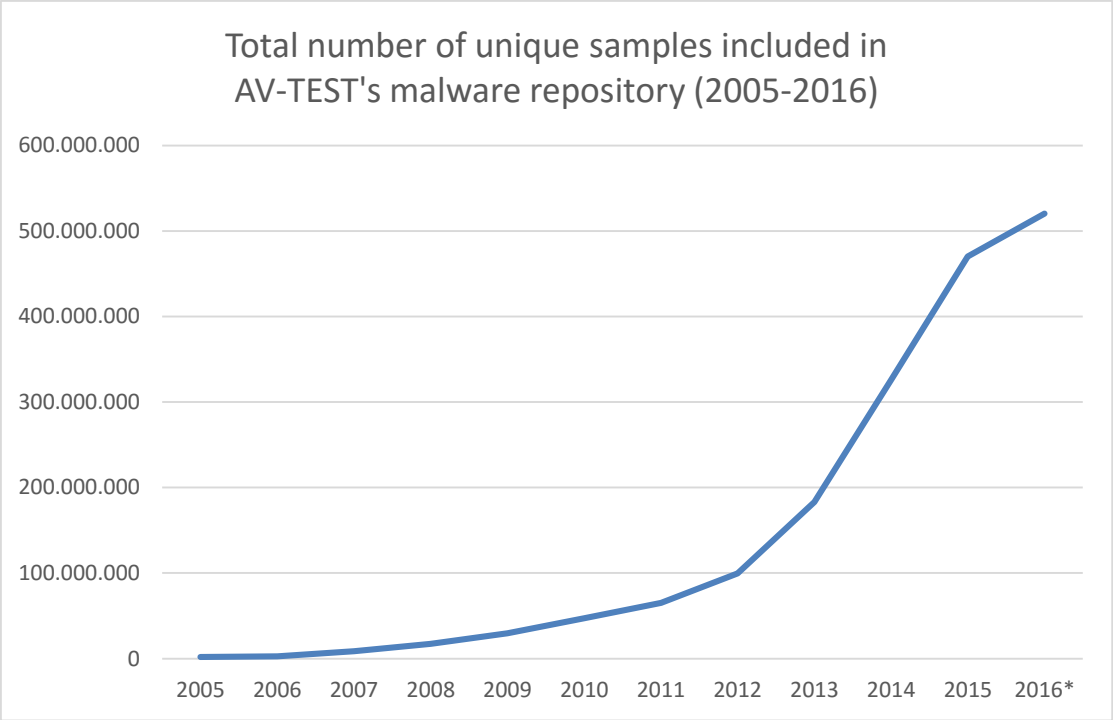


Figure 1: New samples added per year

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 continue to grow in the year 2016. The growth of these numbers is displayed in Figure 1. AV-TEST currently has over 500 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 April and May 2016. 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 March 1st 2016

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 a very good score in the first test part with only one partial miss. The score in the second test part was 55 of 60. Both can be seen in Figure 2.

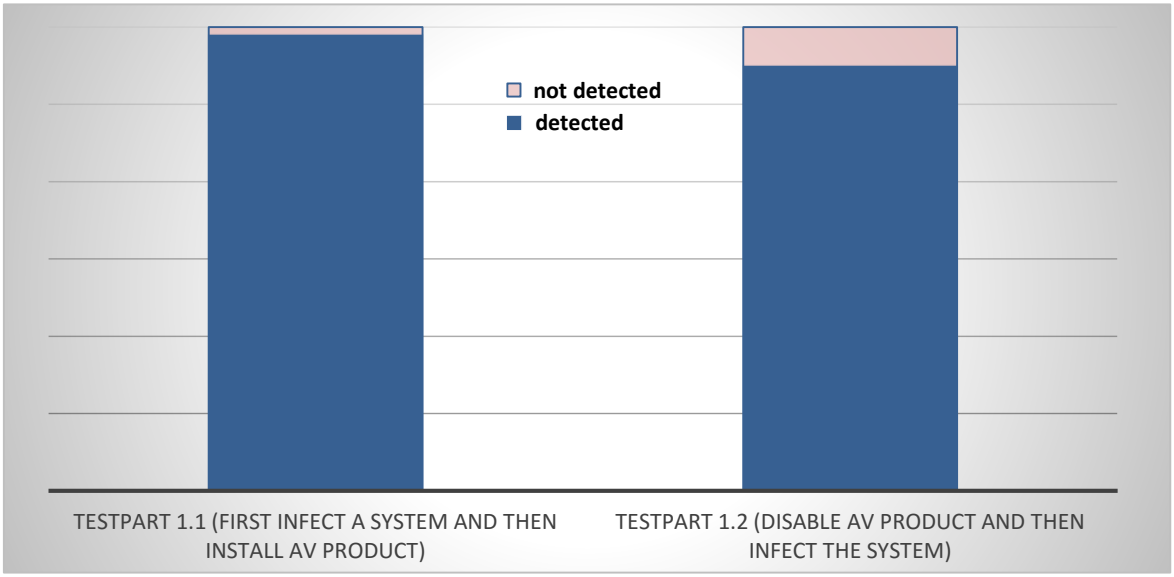
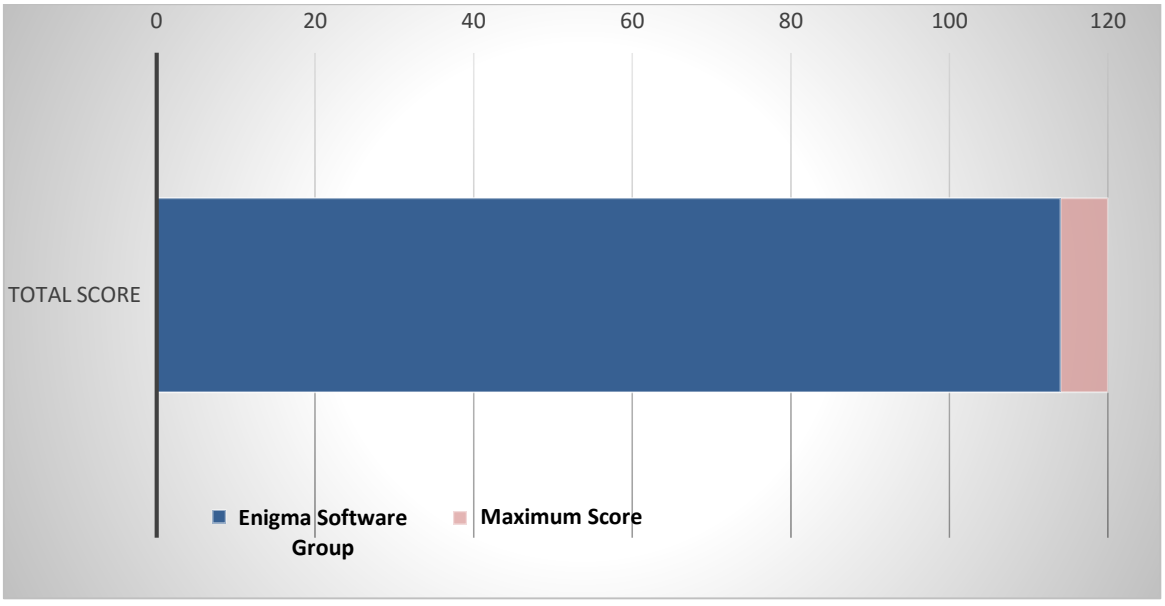


Figure 2: Remediation Score – Part 1.1 +1.2

The maximum score that could be reached was 120. The overall score of Enigma Software Group was 114 as can be seen in Figure 3. Regarding the cleaning efficiency in the Test Part 1.2 several cases were not completely cleaned. SpyHunter cleaned the active parts of the malware on the system. The most leftovers are dropped executable files of the malware into the "C:\Users\vtc\AppData\Roaming\" folder on the system. Only for one test case SpyHunter could not clean the active components of the malware and the system is still infected.

On the other hand the result of part 1.1 is very good with only one miss.



Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Enigma Software Group	SpyHunter	4.22.4.4657	2016.04.26v1

List of used malware samples (Remediation Test)

(SHA256)
0x026bb4f1db988785351ab7d3889c3b322b69398042ae7d52e8e4740e9618eec1
0x02c6d5aeb2ab78f781d72ba60d6f7ff7f5928d47a26ca8dcc4a5c1398850e62a
0x1e3a054ed8051c06a78dc37922c2297a5c3da51a84beb99bc2a487381851ede4
0x1eaef8613ab91e13484646dcb61f5721858066850124a7de5ffce2767bad2ff0
0x2164f112693ab13ef45f159a0444ea64b94942518e829aa55b7d277722b87179
0x2656834a0380bc4c830daef09cfafd038fd5e7727303b09170a8fe37c35a1e34
0x32f0a426e80fb26d098a22bf624d3fb21342372a2135337e9f06ffc4af442846
0x3436da965e7fdbde9a9836acc712ff437d5e7c49a821366451308e11555924f1
0x406ada699acb288bfa2755a9ebe807aa86b90f475b332799f925d85b0d195c61
0x443660d22f3c4bfdb2c2ff4d3e25dafd01f7002bcde53ad7bac8b777e700123a
0x56e24a3dc8b07ea6e08e3d4e4ba96e1e9101aca932523c34350fafbcff02ac85
0x5c596c8afd4656946f0a9741f2be4bb088dda26f1ddcf41eb8c427fbb6d1c3ec
0x60eeb661ad33aa50d9ce1355f9e70afde317411f81e7d0890f38ae28ea79b1b4
0x659896ed065fd59fb843022022a7796ec76620000c7c29a009c7f399898845cb
0x70b64248b23182827c8f52be598a4a10bf0784dc1d97e8721a528ec9cec3acc9
0x76c9c0758ea91e38f8cf47fcc01d597a213eed5f2001ff5f8f7763df236e6baf
0x882ac415de83252554349e3221c7bb5028da1db36b55f196f3cf0a9861ef4597
0x95a1d1207cc0a75eaaeef1a985b8c8bbe15a314c43f2b4d593033cf426bb9212
0x9a679f8745896abd8fbe1586eabc3690858f6d966f4a9c5eb52b6f3b64cd35dd
0xa3efd281adaf729075ee466793fe2a2a6972b746d15e9578355957fc7e7daee2