Real World and Vulnerability Protection, Performance and Remediation Report

A test commissioned by Symantec Corporation and performed by AV-Test GmbH
Date of the report: September 17th, 2014, last update: September 18th, 2014

Executive Summary

In August and September 2014, AV-Test performed a comparative review of 7 home user security products to determine their real-world/vulnerability protection and remediation capabilities. In addition to the core product, dedicated removal tools as well as bootable rescue media (which are being offered by some of the vendors) were added to the test. Further to that the impact of the security products on the system performance has been evaluated with five typical user scenarios. All tests have been run on a clean Windows 8.1 (64-bit) image was used on several identical PCs. The only exception was the exploit test that ran on Windows 7 (32-bit).

The malware test corpus for the remediation consisted of 25 samples. This image was then 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. If one of these steps could not be carried out successfully, additional freely available removal tools or rescue media were used, if available, from the respective vendor.

The malware test corpus for the real-world test consisted of 30 samples, including direct downloads and drive-by-downloads. On the disk image image, the security software was installed and then the infected website or e-mail was accessed. Any detection by the security software was noted. Additionally the resulting state of the system was compared with the original state before the test in order to determine whether the attack was successfully blocked or not.

The malware test corpus for the vulnerability protection test consisted of 25 samples which were created out of different exploits, payloads and obfuscation. On the disk image, the security software was installed and then Metasploit was used to apply the exploit. Any detection by the security software was noted.

The performance test consisted of 5 different real user scenarios, such as visiting websites, installing software and copying files. To perform the single test runs a clean Windows 8.1 (64-bit) image was used on several identical PCs. The tests have been repeated several times to calculate an average result.

G Data showed the best results in terms of malware protection and removal but added some overhead in the performance test. Norton showed perfect malware protection results and nearly perfect removal results with no performance overhead.

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.

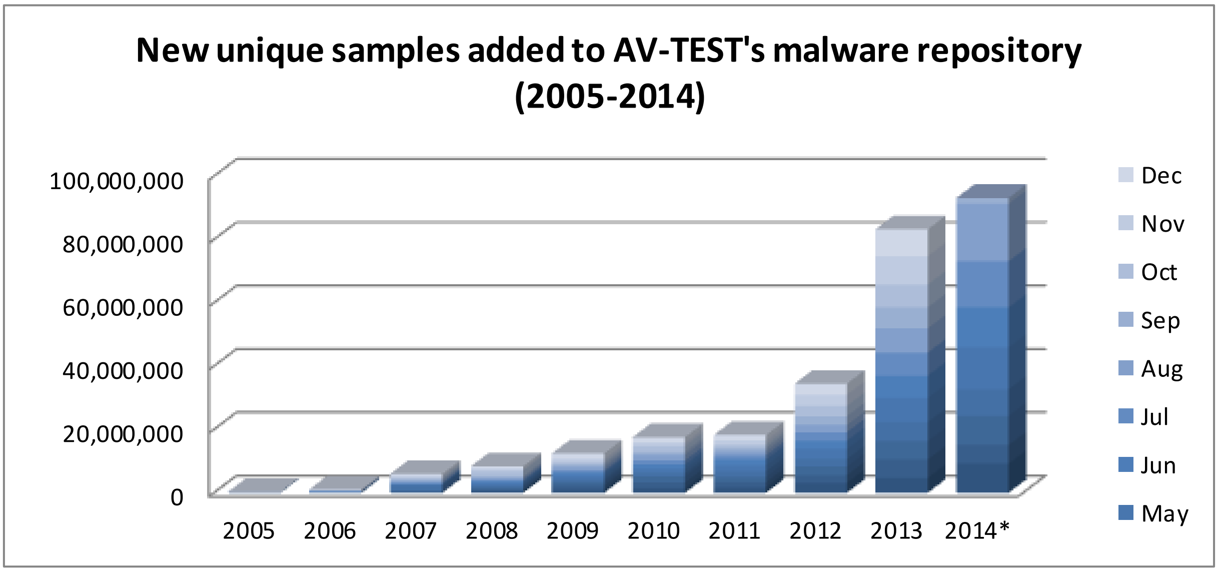

Figure 1: New samples added per year

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 2014. The growth of these numbers is displayed in Figure 1. AV-TEST currently has over 270 million malware samples in its database and two third of it where added in the year 2013 or 2014.

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

Fulfilling these two requirements is not easy. In order to be able to handle the high volume of different malware samples and different behavior it would be necessary to apply more generic cleaning techniques, because there is simply no time to deploy a dedicated cleaning routine for every single malware sample. As soon as generic techniques are used, the risk of false positives (and therefore the risk of harming the system and clean software) increases. On the other hand, malware uses a lot of techniques to avoid successful detection (e.g. rootkit techniques are used to hide files, registry entries and processes) or removal (e.g. the anti-malware software is blocked from starting up). In order to cope with these problems, some vendors provide specific removal tools and rescue media, that don't face the problems of the regular anti-malware software.

Since not all attacks can be stopped in time as we have learned the time until protection is available is crucial too. The first few users might be affected by a threat and require later remediation. But lots of others can be protected if there are automated analysis and classification systems in place at the backend of the anti-virus vendor. They allow to automatically detect new threats and deliver protection very fast.

Furthermore generic detection techniques to cover the most often used infection vectors are required. Exploits are a common way to infiltrate systems by abusing vulnerabilities in the operating system or third party software. Having exploit detection is a good way to generically stop a big number of attacks.

With all this effort to protect the user it is clear that the software will have some impact on the system performance. Nearly all actions an user performs have to be checked for malicious intent. Visiting websites, downloading files, opening e-mail attachments or installing software all pose the risk of malware.

All these aspects have been considered in this test and the corresponding details will be presented on the next few pages.

Products Tested

The testing occurred in August and September 2014. AV-Test used the latest releases available at the time of the test of the following thirteen products:

- Bitdefender Internet Security 2015
- ESET Smart Security 7
- G Data InternetSecurity 2015
- Kaspersky Internet Security 2015
- McAfee Internet Security 2015
- Symantec Norton Security BETA 2015
- Trend Micro Titanium Internet Security 2014

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 8.1 (64-bit) with only those hotfixes that were part of this version as well as all patches that were available on August 1st 2014. The exploit test has been performed on a plain Windows 7 (32-bit) without security patches.

Additionally, the following applications have been installed to provide a "vulnerable" system for the URLs that use exploits to infect the system.

Developer	Product	Version
Adobe	Adobe Reader	9.2.0
Sun	Java	1.6.0_19-b04

Testing methodology

Remediation Test

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.
11. **False Positive Testing**. The test should also run clean programs and applications to make sure that products do not mistakenly remove such legitimate software.

In addition to the above, the following items had to be considered:

Fixtools: No threat-specific fixtools should be used for any product's remediation. Only generic remediation standalone/fixtools and bootable tools should be used.

Licensed vs. Unlicensed Bootable or Remediation tool: Only licensed bootable or other generic remediation tools offered by vendors as part of their security product or pointed to by their infection UI workflow should be included in the test. No unlicensed tools should be used in the t est.

Microsoft's Malicious Malware Removal Tool: This is part of the windows update and as such a part of the Windows OS. This tool should not be used as a second layer of protection for any participating vendor's products.

Real-World Test

The real-world 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. **Product Cloud/Internet Connection**. The Internet should be available to all tested products that use the cloud as part of their protection strategy.
4. **Product Configuration**. All products were run with their default, out-of-the-box configuration.
5. **Sample variety**. In order to simulate the real world infection techniques, malware samples should be weighted heavily (~80 per cent) towards web-based threats (of these, half should be manual downloads like Fake AV and half should be downloads that leverage some type of exploited vulnerability i.e. a drive-by download). A small set of the samples (5 – 10%) may include threats attached to emails.
6. **Unique Domains per sample**. No two URLs used as samples for this test should be from the same domain (e.g. xyz.com)
7. **Sample introduction vector**. Each sample should be introduced to the system in as realistic a method as possible. This will include sending samples that are collected as email attachments in the real world as attachments to email messages. Web-based threats are downloaded to the target systems from an external web server in a repeatable way.
8. **Real World Web-based Sample User Flow**. Web-based threats are usually accessed by unsuspecting users by following a chain of URLs. For instance, a Google search on some high trend words may give URLs in the results that when clicked could redirect to another link and so on until the user arrives at the final URL which hosts the malicious sample file. This test should simulate such real world user URL flows before the final malicious file download happens. This ensures that the test exercises the layers of protection that products provide during this real world user URL flow.
9. **Sample Cloud/Internet Accessibility**. If the malware uses the cloud/Internet connection to reach other sites in order to download other files and infect the system, care should be taken to make sure that the cloud access is available to the malware sample in a **safe** way such that the testing network is not under the threat of getting infected.

10. **Allow time for sample to run**. Each sample should be allowed to run on the target system for 10 minutes to exhibit autonomous malicious behavior. This may include initiating connections to systems on the internet, or installing itself to survive a reboot (as may be the case with certain key-logging Trojans that only activate fully when the victim is performing a certain task).
11. **Measuring the effect**. A consistent and systematic method of measure the impact of malicious threats and the ability of the products to detect them shall be implemented. The following should be observed for each tested sample:
    a. **Successful Blocking of each threat**. The method of notification or alert should be noted, including any request for user intervention. If user intervention is required, the prompted default behavior should always be chosen. Any additional downloads should be noted. The product should be able to block the malware from causing any infection on the system. This could mean that the malware executes on the system before it tries to do any malicious action, it is taken out by the product.
    b. **Successful Neutralization of each threat**. The notification/alert should be noted. If user intervention is required, the prompted default behavior should always be chosen. Successful neutralization should also include any additional downloads. Additionally, indicate whether all aspects of the threat were completely removed or just all active aspects of the threat.
    c. **Threat compromises the machine**. Information on what threat aspects were found on the system and were missed by the product should be provided.

Vulnerability Protection Test

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. **Product Cloud/Internet Connection**. The Internet should be available to all tested products that use the cloud as part of their protection strategy.
4. **Product Configuration**. All products were run with their default, out-of-the-box configuration.
5. **Sample introduction vector**. Samples have been created with Metasploit and were accessed with Internet Explorer.
6. **Scoring**. If the exploit or payload was successfully blocked this was noted as block, if the payload could be execute that was noted as miss.

Performance Test

1. **Clean system for each test run**. The test systems should be restored before starting the performance testing runs.
2. **Physical Machines**. The test systems used should be actual physical machines. No Virtual Machines should be used.
3. **Product Cloud/Internet Connection**. The Internet should be available to all tested products that use the cloud as part of their protection strategy.

4. **Product Configuration**. All products were run with their default, out-of-the-box configuration.
5. **Test cases.** The following five scenarios have been tested:
   a. Downloading files
   b. Visiting websites
   c. Installing software
   d. Using software
   e. Copying files
6. **Repeated tests.** All tests have been repeated several times to calculate an average value for each of the five scenarios.
7. **Scoring**. Depending on the percentage added to the reference value, a score ranging from 1 (minimal impact) to 5 (high impact) has been given for each of the five test categories.

Efficacy Rating

Remediation Test

For each sample tested, apply points according to the following schedule:

a. Malware completely removed (5)
b. Malware removed, some unimportant traces left (4)
c. Malware removed, but annoying or potentially dangerous problems remaining (2)
d. Malware not removed (0)
e. Product is overly aggressive (e.g. takes out the entire hosts file, entire directory containing threat file etc.) (-2)
f. Product's remediation renders the machine unbootable or unusable (-5)

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.

Real-World Test

For each sample tested, apply points according to the following schedule:

a. Malware is Blocked from causing any infection on the system by the product (+2)
b. Malware infects the system but is Neutralized by the product such that the malware remnants cannot execute any more (+1)
c. Malware infects the system and the product is unable to stop it (-2)

The scoring should not depend on which of the available protection technologies were needed to block/neutralize the malware. All technologies and the alerts seen should be noted as part of the report however.

Vulnerability Protection Test

For each sample tested, apply points according to the following schedule:

a. Exploit/Payload is blocked by the product (+1)
b. Exploit/Payload is not blocked by the product (0)

The scoring should not depend on which of the available protection technologies were needed to block/neutralize the malware. All technologies and the alerts seen should be noted as part of the report however.

Performance Test

Scores from 1 to 5 are given for each of the five categories according to this scheme:

- Score 1: Less than 20% impact
- Score 2: Less than 40% impact
- Score 3: Less than 60% impact
- Score 4: Less than 90% impact
- Score 5: More than 90% impact

Samples

Remediation Test

The set contained 25 malicious files that were able to infect Windows 8.1 (64-bit).

Real-World Test

The malware set contains 30 web based threats from distinct URLs that have been discovered by AV-TEST at the day of the test.

Vulnerability Protection Test

25 different combinations of exploits, payloads and obfuscation have been used.

Test Results

Vulnerability Protection Test

The results of the exploit test show more differences than the two previous tests. There were only two products that were able to block all 25 exploit attacks, G Data and Norton. Details can be seen in Figure 2.

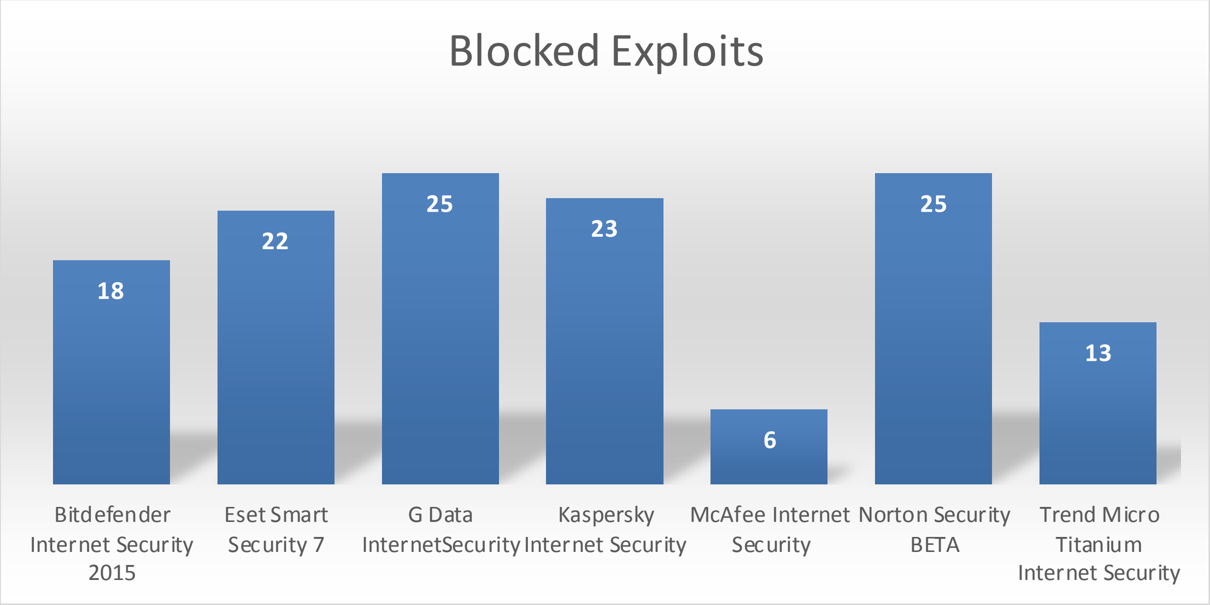

Figure 2: Blocked Exploits

The average score was 19 out of 25 and the median 22. Four products were equal or better than the average. The results vary a lot between the different products. Some didn't detect certain exploits at all others just failed at certain combinations of exploits and payloads.

In total this indicates that generic exploit detection techniques are not yet common in all products.

Real-World Test

All products but one achieved the maximum score of 60.

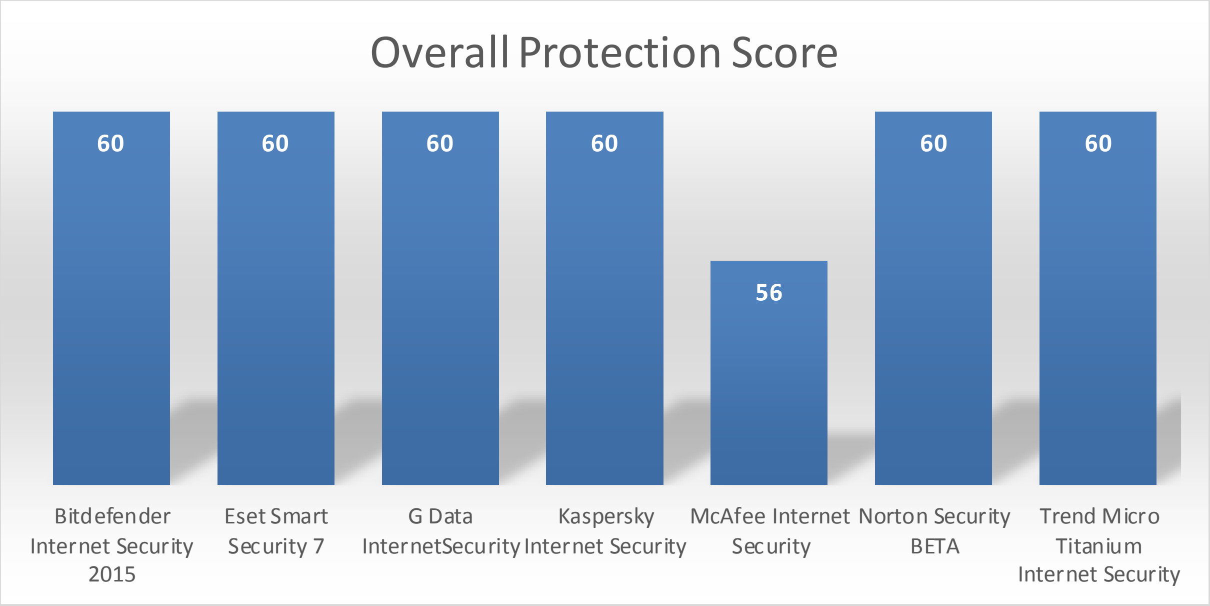

Figure 3: Overall Score

In Figure 3 the overall result is given. All products but McAfee scored the maximum of 60 points. McAfee only missed one threat.

Performance

Performance testing showed more differences among the products. Bitdefender, Kaspersky and Norton had nearly no noticeable impact on the system performance and therefore receive the best score of 5 points each.

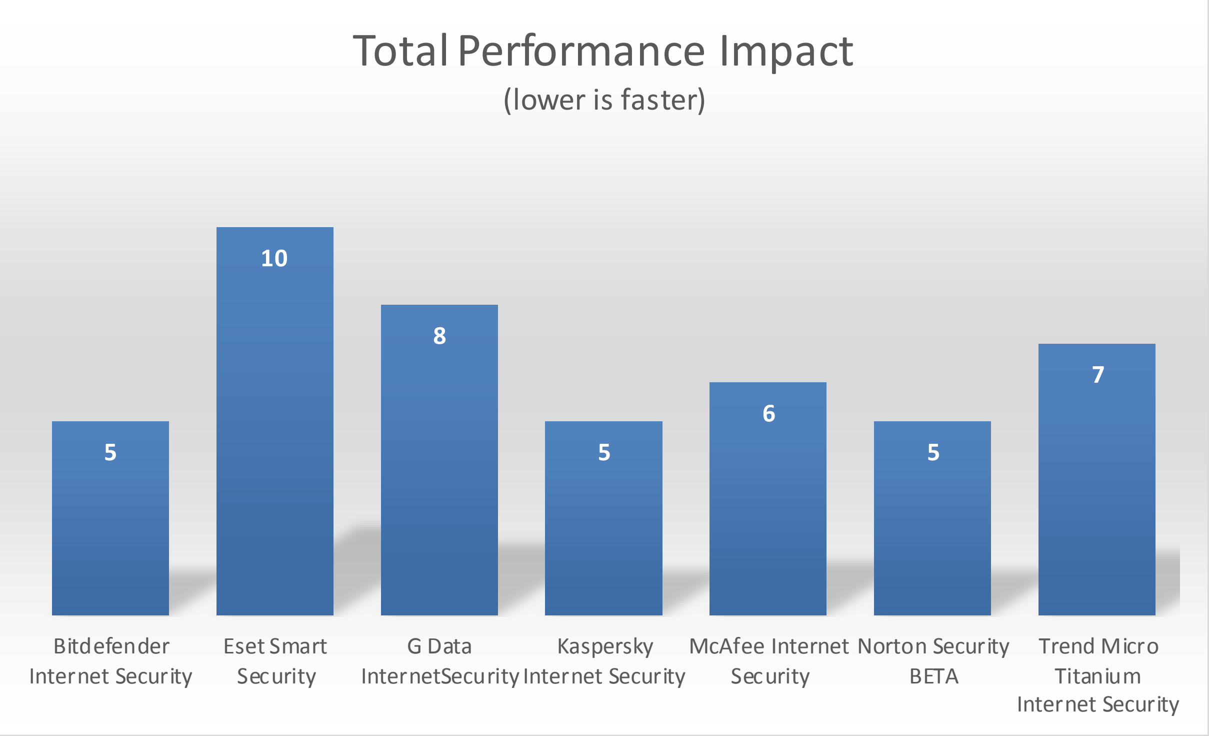

Figure 4: Performance Impact

McAfee and Trend Micro are showing a slight overhead when running applications (both programs) and when loading websites (Trend Micro) resulting in a score of 6 for McAfee resp. 7 for Trend Micro. G Data and ESET are further behind with impact scores of 8 (G Data) and 10 (ESET). However the system impact of all tested products is rather low and better than the industry average.

Remediation Test

G Data and Trend Micro achieved the best overall removal score for, as can be seen in Figure 5. It should be kept in mind that the numbers shown here are the result of the combined effort of the core product and additional removal tools and rescue media, if available.

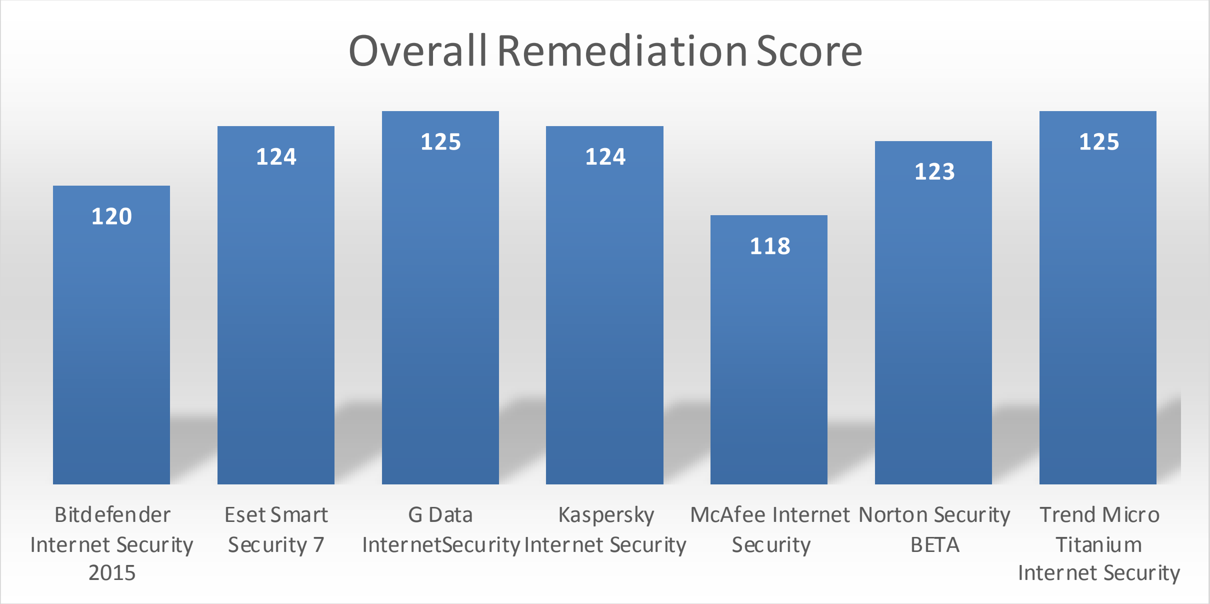

Figure 5: Overall Remediation Score

The maximum score that could be reached was 125. The best score was 125, achieved by G Data and Trend Micro closely followed by Eset and Kaspersky with 124 as well as Norton with 123. The worst score was 118. The average score was 123 and the median score 124. This means that five products were better than or equal to the average and two products were worse than the average.

Summary

From the different tests there is no clear number one product. G Data was the only product with a perfect score for remediation, real-world protection and exploit protection but adds more overhead in the performance testing. Kaspersky on the other hand had a nearly perfect score for remediation, a perfect score for real-world protection and a perfect performance testing score but missed two exploit test cases. The Norton product missed two points in the remediation test but scored perfect in all other tests.

This shows that it is difficult for a product to do well in all aspects. There is always some trade somewhere. Perfect protection may affect the performance. On the other hand good dedicated remediation results don't necessarily mean that generic exploit protection works well too.

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Bitdefender	Bitdefender Internet Security 2015	18.13.0.1012	7.56147
ESET	ESET Smart Security 7	7.0.317.4	1433/10181
G Data	G Data Internet Security 2015	25.0.1.4	Engine A (AVA_24.3425) (31.07.2014), Engine B (GD_25.3675) (2014-07-31)
Kaspersky Lab	Kaspersky Internet Security 2015	15.0.0.463(a)	16.5.3.8
McAfee	McAfee Internet Security 2015	16.8.819	1966.0
Symantec	Norton Security BETA 2015	22.0.0.79	20141.1.0.298
Trend Micro	Trend Micro Titanium Internet Security 2014	7.0.1255	9.750.1005/ 10.953.95

Table of removal tools

Developer, Distributor	Removal Tool	Comment
Bitdefender	-	
ESET	-	
G Data	-	
Kaspersky	Virus Removal Tool 11.0.0.1245	
McAfee	Stinger 12.1.0.1025	
Symantec	Norton Power Eraser 4.3.0.13	
Trend Micro	SysClean 3.00-1018	

List of used malware samples (Remediation Test)

Other malware (SHA256)
0x046d8a840041b2ae575466a96d2f849c0679873dd5d659c73c40fa52a3cae775
0x11425ad218cb6415d60c8487f68478b157fb1f79ac3f9eac4e3b67faf539ab7f
0x126febc828e3e3f337ab1b98ff289be61c30692c3b89235b1c0eaf68b3c49b39
0x283cbb80c68c8d5775d9b2f85229527817962f82c797955b7e3b4c528fab04de
0x2abc1f93ee402306a04faf89159e25cd8fa908f39c46fb83272fc043dc8d8d1e
0x377408f40b5d0313e74c0ffebae4fa4486620ffdfa0be9189c4a13780721cff9
0x3c66607d8eb340d04bef8f3a95a9703fd1ac7f3efbe5541cae683dfd5cf19813
0x4263bca641295aae4142976805a6c8d661cb327cfdffdc33cf18ed03ab88ac40
0x48da4330f5e20de1b9f5072704f215b65c896190d533b66b465536da2bd53936
0x52a1b4bfaf9f0453c27d715be6a6f035b4f276c010722d6626a6ecc76357ede5
0x57af04fe6bd6d51d77e2cd9aaac981857e2bf6d0bc43b7c00667ef7631281d0a
0x691366e40e7ff010c57ca4acadc1d8f7a00f33300e626c40fe95cef79bca4a59

0x6d8705a29ce00a62c129f4773831803b33541d18cbce46caa207c92085db9139
0x78a982285b2fd5187bbeb3eb3a50b885e60cc84a359a5ed096ec37c910f021e1
0x8912cf3859cead0288e6a24575900bd35f17b471df9b778c359723435da96cde
0x983f075ce3ec06b2531d74b9c8e57bcc7be4414597c86ba8bb3c6bbfbd07ada6
0xa8207d0e463ddbfe7a0ed664f6c9d8aca08b994e059372d0436a0d9f095aecb3
0xac1a02954970af65ad044ef5a97960a4ff039cbe119fcb1209159bbc9bae37cf
0xb21309b161acca8bb15a0954837c44992371251 2faf02d2db3ae4855a787f361
0xc18c7585a4b21d2a407b69448fa43d2305a70055217b8d83088568bac0f81b07
0xc6a7a188dc0e63a8bf72b2dee5e4059cc5eb009b29ec9606f8928c8167d2dc8f
0xd8f6c3da5b8705e314bad6e0228906f8f458ee0c0fb5a4ead4c8e8ac2bdd3eda
0xe599b80805876f646c2186122287b9d5d2fe1e832603445956f518f00e382e46
0xf8f4ab037bda3ccc8b2bc1f7172b3700e51a431799c135eed05425fc14e02f7c
0xfff34fb6068b8c7165c7a8bc9ff695f8295c745db54e911cd1a309163ad213a1

List of used malware samples (Real-World Test)

Direct Downloads and Drive-By-Downloads	
http://www.filehole.net/files/69bee82f39b09f048781ada457992125.exe	http://neiindia.com/News/bass/DOC_0011163873872gst7e63.exe
http://uploads.tmweb.ru/WIRvFjygif.exe	http://martinavogliosina.altervista.org/NuovaCartella/Patatina____.scr
http://jojik-international.com/images/wav.exe	http://www.weebly.com/uploads/3/7/4/3/37439271/ouija_game_spanish.exe
http://download1.ihyip.pw/64.exe	http://142.4.117.206/v3.exe
http://efax.download.efaxsecureemail.iiisbkdsjiubskjbakaa.secureconnect3398kdjsbkab.39822221.secure.lloyds-download.com/Fax_001_28072014_612.scr	http://paintercity.com/wp-content/03_06_2013.jpg.exe
http://dc281.gulfup.com/cT7nnv.exe?gu=f_DN5wQ4UUVHnnOTow56iw&e=1406985656&n=66696c656e616d652a3d5554462d3827275370656564446f776e6c6f61642e657865	http://cbmm.ru/styles/css.exe
http://entrepreneuressacademy.com/blog/wp-content/plugins/wp-get-post-image/27-07-homer_original.exe	http://37.187.241.22/server.exe
http://acessoriamaster.com.br/modulos/acesoriacheque001.exe	http://filesreferat.info/sex/dl/?q=video
http://daraltasneem.com/images/pdf.exe	http://77.237.123.141/wp-content/themes/f679rqp75g.exe
http://dc262.gulfup.com/4qOSE3.exe?gu=BxWMZs-6Hi2QCMiNbuZH1w&e=1407053990&n=66696c656e616d652a3d5554462d38272744 6f776e6c6f61642e657865	http://iridiumservers.net/FreeMinecraftCodes.exe
http://download1.regexxx.pw/64.exe	http://partysupplydepot.ca/photos/1%2eexe
http://pagamentosbrasil.com/KLS/upda.exe	http://www.pictrace.com/b/TdYYgy/ratter.exe
http://commerceavenues.com/images/Lus2.exe	http://zacc.af/12-08-14.jpg.exe
http://5.135.47.59/bin.exe	http://178.33.69.16/Glueckskeks.exe
http://www.findfreelancer.net/wp-content/plugins/30_07_2014.jpg.exe	http://trip-pk.org/TripPK.exe

List of used exploits

Exploit	Payload
(exploit/windows/browser/ie_cgenericelement_uaf)	generic/shell_reverse_tcp
(exploit/windows/browser/ie_cgenericelement_uaf)	windows/download_exec

(exploit/windows/browser/ie_cgenericelement_uaf)	windows/exec
(exploit/windows/browser/ie_cgenericelement_uaf)	windows/shell/reverse_tcp
(exploit/windows/browser/ms11_003_ie_css_import)	generic/shell_reverse_tcp
(exploit/windows/browser/ms11_003_ie_css_import)	windows/download_exec
(exploit/windows/browser/ms11_003_ie_css_import)	windows/exec
(exploit/windows/browser/ms11_003_ie_css_import)	windows/shell/reverse_tcp
(exploit/windows/browser/ms13_037_svg_dashstyle)	generic/shell_reverse_tcp
(exploit/windows/browser/ms13_037_svg_dashstyle)	windows/download_exec
(exploit/windows/browser/ms13_037_svg_dashstyle)	windows/exec
(exploit/windows/browser/ms13_037_svg_dashstyle)	windows/shell/reverse_tcp
(exploit/windows/browser/java_cmm)	generic/shell_reverse_tcp
(exploit/windows/browser/java_cmm)	windows/download_exec
(exploit/windows/browser/java_basicservice_impl)	generic/shell_reverse_tcp
(exploit/windows/browser/java_basicservice_impl)	windows/download_exec
(exploit/windows/browser/java_basicservice_impl)	windows/exec
(exploit/windows/browser/java_basicservice_impl)	windows/shell/reverse_tcp
(exploit/windows/browser/java_docbase_bof)	generic/shell_reverse_tcp
(exploit/windows/browser/java_docbase_bof)	windows/exec
(exploit/windows/browser/java_docbase_bof)	windows/shell/reverse_tcp
(exploit/windows/browser/adobe_cooltype_sing)	generic/shell_reverse_tcp
(exploit/windows/browser/adobe_cooltype_sing)	windows/download_exec
(exploit/windows/browser/adobe_cooltype_sing)	windows/exec
(exploit/windows/browser/adobe_cooltype_sing)	windows/shell/reverse_tcp

Phone +49 (0) 391 60754-60, Fax +49 (0) 391 60754-69, Web http://www.av-test.org