Windows 8 Malware Protection Test Report

A test commissioned by Kaspersky Lab and performed by AV-Test GmbH

Date of the report: January 11th, 2013, last update: January 11th, 2013

Executive Summary

In December 2012, AV-Test performed a comparative review of Kaspersky Internet Security and the built-in Windows 8 security components to determine their capabilities to protect against malware. Four individual tests have been performed. The first was a real-world protection test of malicious URLs and E-Mails with 42 samples, the second was a static detection test of 111487 malicious files, the third test was another static detection test of 2500 prevalent files and the final test was a static false positive test with 345900 samples. To perform the test runs, a clean Windows 8 image was used on several identical PCs. On this image, the security software was installed resp. for the plain Windows 8 image all security related components were left in default state and then the individual tests have been carried out. In case of the dynamic test, the URLs have been accessed and the downloaded samples have been executed and 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. In case of the static detection test, the products had to scan two sets of files in default settings. Detections have been noted to determine the detection result.

Kaspersky provided near perfect results, blocking all 42 URL and E-Mail attacks, while Microsoft failed to block 5 attacks. There were also dramatic differences in the static detection of malware. Kaspersky detected 99% of the tested samples, Microsoft only managed to detect 90%. Regarding static detection of prevalent malware and false positives there were no problems for either product. Both of them detected all 2500 prevalent malware samples and neither created a false positive detection in the set of clean files. The results indicate that Windows Defender and other security features in Windows 8 do offer a baseline protection. However, this is not enough to reliably protect against the magnitude of attacks seen to Windows systems these days. A commercial solution, such as the tested Kaspersky Internet Security provides a far better protection.

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.

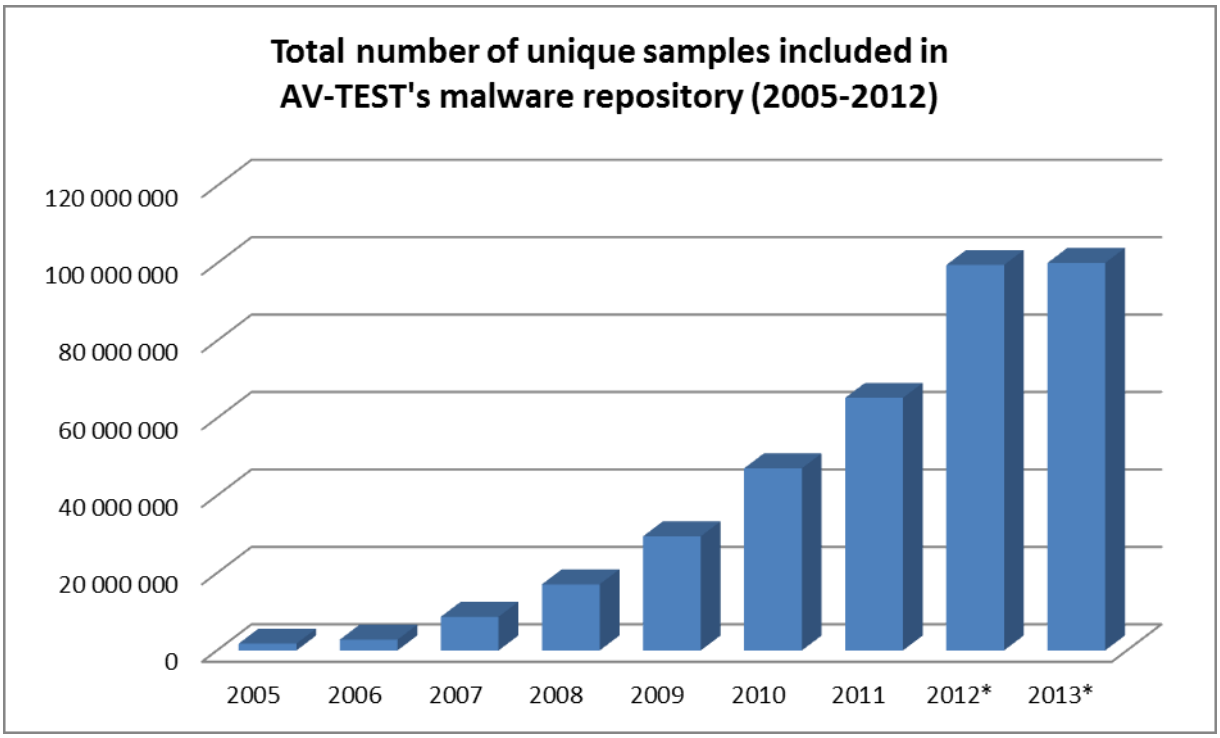

Figure 1: New samples added per year

In early 2013 the AV-TEST collection of malware exceeded 100.000.000 unique samples and the growth rates are getting worse and worse. In the year 2000, AV-Test received more than 170,000 new samples, and in 2010 and 2011, the number of new samples grew to nearly 20,000,000 new samples each. The numbers continue to grow in the year 2012 and 2013.

Microsoft reacted to these threats and each version of Windows released in the last years was more secure than its predecessor. Windows 8 now even included a built-in malware scanner (Windows Defender) and URL blocking components (SmartScreen filter). This report will assess whether these features are enough to protect the users from today's threats.

Products Tested

The testing occurred in December 2012. AV-Test used the latest releases available at the time of the test of the following products:

- Microsoft Windows 8 Pro with built-in Windows Defender 4
- Kaspersky Internet Security 2013

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 Pro with only those patches that were available on December 1st 2012.

Testing methodology

General

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 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.
6. **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).

The procedures below are carried out on all tested programs and all test cases at the same time in order to ensure that all protection programs have the exact same test conditions. If a test case is no longer working or its behavior varies in different protection programs (which can be clearly determined using the Sunshine analyses), the test case is deleted. This ensures that all products were tested in the exact same test scenarios. All test cases are solely obtained from internal AV-TEST sources and are always fully analysed by AV-TEST. We never resort to using test cases or analyses provided by manufacturers or other external sources.

Real-World Test

1. The products are installed, updated and started up using standard/default settings. The protection program has complete Internet access at all times.
2. AV-TEST uses the analysis program Sunshine, which it developed itself, to produce a map of the non-infected system.

3. It then attempts to access the URL or receive the E-Mail
4. If access is blocked, this is documented
5. If access is not blocked, the malicious sample is downloaded from the URL resp. the malicious attachment is stored to disk
6. If this is blocked, this is documented
7. If this is not blocked, the malicious file will be executed.
8. If execution of the sample is blocked with static or dynamic detection mechanisms by the program, this is documented.
9. If execution is not blocked, an on-demand scan (Full computer scan) will be carried out. Any detections will be noted and any removal actions will be allowed.
10. Given that the detection of malicious components or actions is not always synonymous to successful blockage, Sunshine constantly monitors all actions on the computer in order to determine whether the attack was completely or partially blocked or not blocked at all.
11. A result for the test case is then determined based on the documented detection according to the protection program and the actions on the system recorded by Sunshine.

Static Scanning Test

1. The test ran in the timeframe from December 3rd to December 10th, 2012
2. A first scan over the whole collection has been carried out and all non-detected files have been identified
3. Finally a rescan of all non-detected samples has been performed on December 10th, 2012
4. The combined result of these scans has then been noted

The malware set for the real-world test contains 42 samples (39 URLs, 3 E-Mails). These samples have been collected during December 11th and December 18th 2012. The malware set for the static scanning test contains 2500 prevalent samples and 111487 further samples. These files have been collected during November 1st and November 30th 2012.

Test Results

The results of the first test (Figure 2) show that Kaspersky was able to protect against all 42 Real-World threats used in the test, while Microsoft failed to block 5 out of them, which would result in an infection of the system.

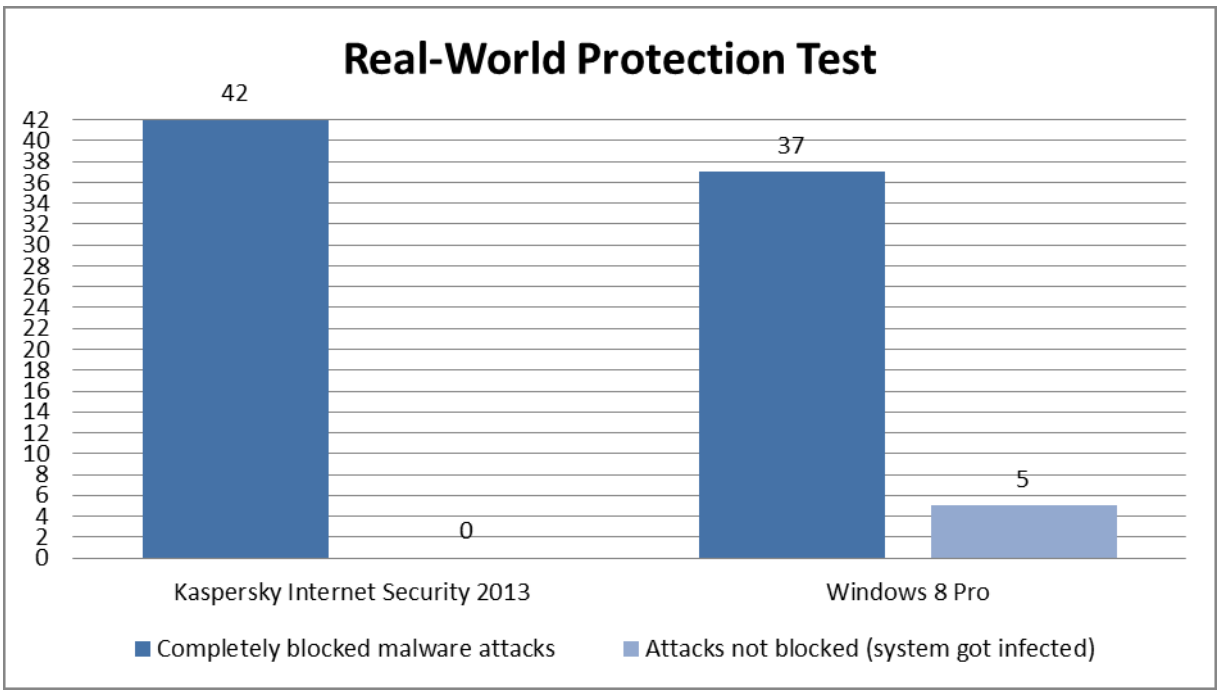

Figure 2: Real-World Protection

As most of the infections these days take place via malicious websites or malicious e-mail attachments it is especially important to provide a solid protection level in this area.

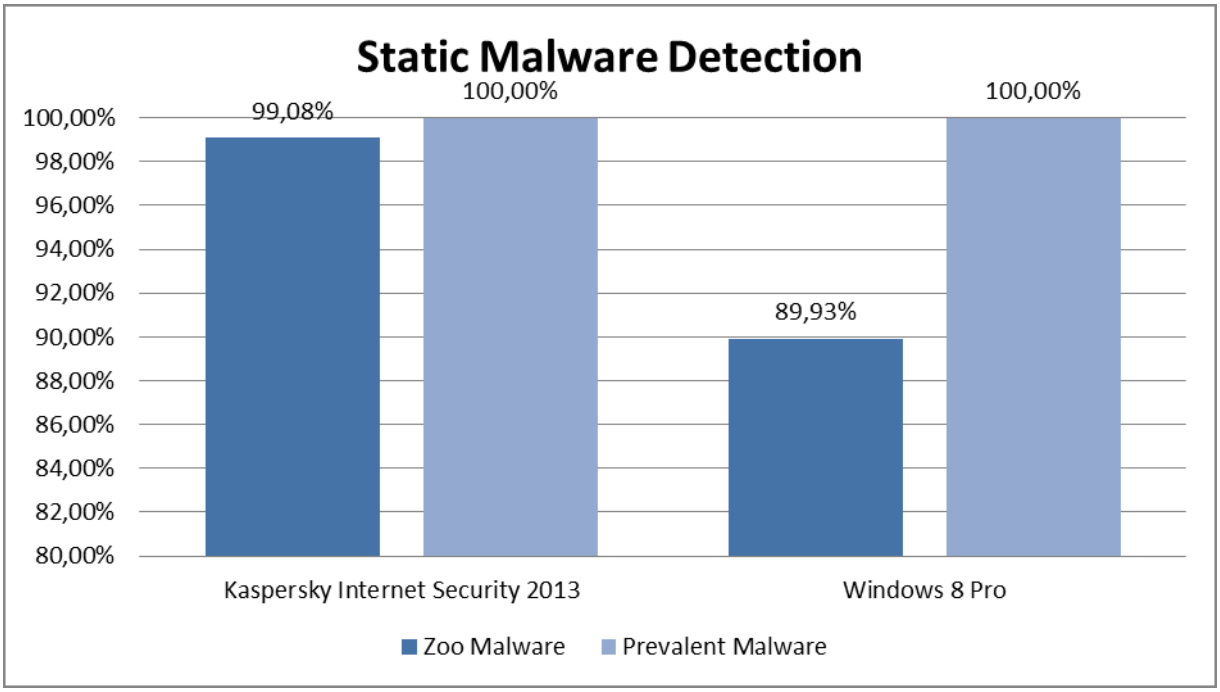

Figure 3: Static Malware Detection

The next test shows the capability of statically detecting malware. Two different testsets have been used to determine the results of the two products. There was one set of highly prevalent malware that should be detected by all products and as can be seen in Figure 3 both tested products did detect all samples of this set. The other testset however showed differences between both products. This set contains malware that may not be as widespread but still is a risk to the user. Microsoft detects less 90% of the 111487 samples (11228 missed samples) while Kaspersky stops over 99% of the samples (1031 missed samples).

While static detection is only one feature of a set of protection features in modern security software it still is a very important one and many products mainly rely on this technique to detect malware. As such these results indicate that the built-in Windows Defender in Windows 8 is not good enough to reliably protect the user.

The final test was a test for false positives. 345900 files collected from clean applications have been scanned with both products to see whether any of these files have been wrongly flagged as malware. Neither product did this and not a single false positive occurred. This shows that even a product with a very good detection and protection rate (Kaspersky) can go without any false positives.

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Kaspersky Lab	Kaspersky Internet Security 2013	13.0.1.4190 (c)	16.5.2.1
Microsoft	Windows 8 Pro with Windows Defender	4.0.9200.16384 (Windows Defender Version)	1.1.9002.0/ 1.141.952.0 (Windows Defender Version)

List of used URLs, Mails and Samples

URLs	
http://www.fauziyahospital.com/mego/OMG.exe	http://www.stellardayproducts.com/expensekeeper/OperaPMupdate/OperaPMupdate.exe
http://204.15.124.183/bX2XdF.exe	http://ge.tt/api/1/files/9dMi6OQ/0/blob
http://shaiyaner.de/downloads/svchost.exe	http://s3-sa-east-1.amazonaws.com/vonoloa/Contrato_61277.pdf.exe
http://restterem.ru/media/admin26.exe	http://37.59.66.1/Server.exe
http://troykaakademi.net/media/firsale.exe	http://nause.com/LjRjU.exe
http://citrus.doolr.com/appr1.exe	http://ds.searchstar.co.kr/filepop/bacon.exe
http://kamalbose.com/uY3VZr.exe	http://hack3d.3dom.fr/shouky/rcv.exe
http://ballyhooindia.com/brlaikza/9qf.exe	http://beyondcreative.com.au/flashupdate.exe
http://cateringumbria.eu/ox1.exe	http://206.253.165.71/phpmyadmin/5566.exe
http://1337.kz/vsocks-1.3.0.0.exe	http://chat.ru/~dhoffmanfan/syscfg.exe
http://tkprinter.com/Expl0it/forjd/warp.exe	http://demo.ovh.net/download/c356f845248362888ed36ead5a5280ae/c99199151.exe
http://89.248.166.21/prx.exe	http://videoiindir.weebly.com/uploads/1/2/7/6/12763800/video2.exe
http://74.63.196.69/bee/panel/panel/uploads/bzeusnet.exe	http://tanvirassociates.pk/ENTEL/formulario.exe
http://211.147.15.3/dls/qqtodta.exe	http://baniganm.net/uploads/files/baniganm-a8a31351d0.exe
http://weebly.com/uploads/1/2/1/1/12113165/dvxplayer.scr	http://dyneema.co.uk/components/com_ag_google_analytics2/dir/Core777.exe
http://update.qmxsoft.com/1.3.exe	http://empuriaonline24.com/iJZWa.exe
http://www.yerlipornoizle.org/porno-video.exe	http://file.findlock.co.kr/ndn/r.exe
http://mytightride.info/missing.exe	http://u.websuprt.co.kr/NewSidebar/Angel/AngelSupporter.exe
http://solarpanelinstallers.org.uk/media/firsale.exe	http://carroceriasfejoben.com/components/com_ag_google_analytics2/dir/p.exe
http://www.genckizlarr.com/videolar/super_sikis_videosu.exe	
Mails	
Subject: “aussage”	Subject: “Incoming Wire Notification”
Subject: “uberweisung”	
Static Detection	
List of the samples not given because of size, but it is available on request.	