Real World Testing Report

A test commissioned by Symantec Corporation and performed by AV-Test GmbH

Date of the report: July 30th, 2012, last update: July 30th, 2012

Executive Summary

In July 2012, AV-Test performed a comparative review of Norton Internet Security and Windows 8 with its built in security functions to determine their real-world protection capabilities. The test was designed to challenge the products against 0-day attacks from the internet, which includes the most common infection vectors these days. The samples were primarily accessed via direct links to malicious executable files, due to the low likelihood of working exploits on the Windows 8 platform.

The malware test corpus consisted of 50 samples, including direct downloads and drive-by-downloads. The false positive corpus consisted of 26 known clean applications. To perform the single test runs, a clean Windows 8 image was used on several identical PCs. On this image, the security software was installed respectively the pre-installed Windows Defender was used and then the infected website 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. For the false positive part, 26 known clean applications were installed and any false detections from the security products were noted.

The best result in the described test has been achieved by the Symantec product. Furthermore, no false positives occurred for this product.

Overview

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

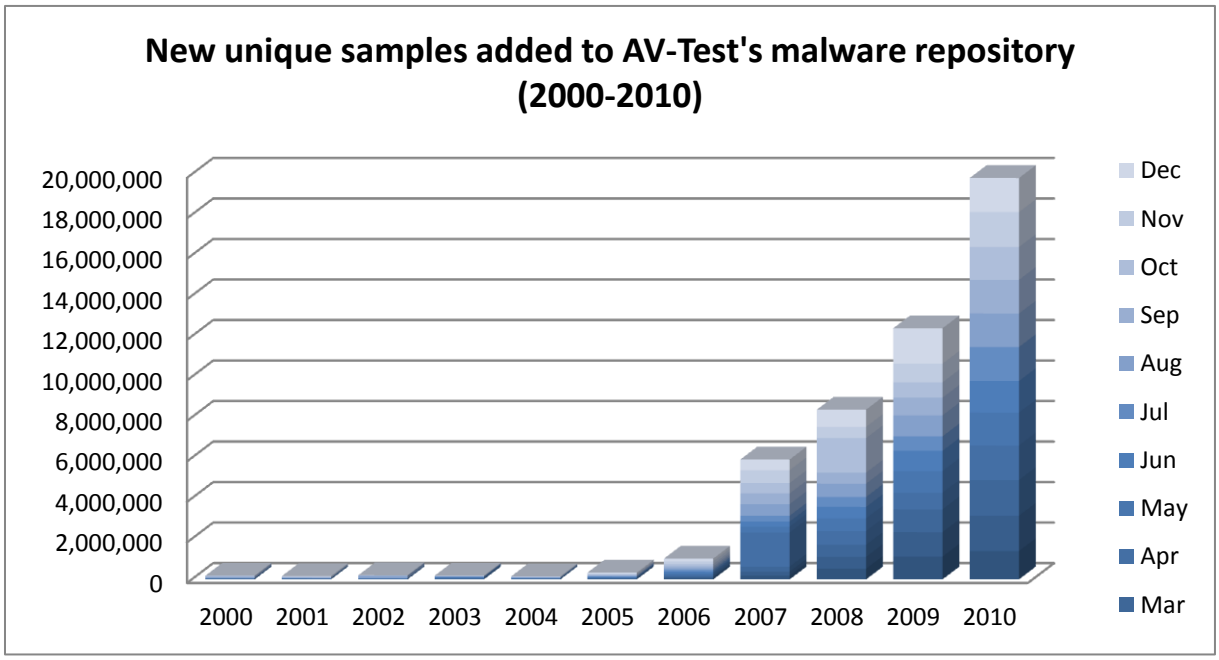

Figure 1: New samples added per year

In the year 2000, AV-Test received more than 170,000 new samples. In 2010 the number of new samples has grown to over 19,000,000 and the numbers continue to grow in the year 2012. The growth of these numbers is displayed in Figure 1.

The volume of new samples that have to be processed by anti-malware vendors in order to protect their customers is creating problems. It is not always possible to deploy a signature for a certain binary in time. Heuristics and generic detections do add some additional protection, but that alone is not enough. These static detection mechanisms are therefore accompanied by dynamic detection mechanisms which don't rely on a specific signature to detect malware. Instead the behavior of programs is observed and if they are suspicious or malicious they will be reported and blocked. However, due to the massive amount of malware samples and behavior, neither static nor dynamic detection technologies are enough to secure a system. Therefore, yet another detection layer has been introduced that tries to prevent attacks at an earlier stage. This includes URL blocking and exploit detection. As soon as a URL is visited that is known to spread malware, access can be denied. Also, if a website contains malicious code, such as exploits, the access can be denied or the exploit can be stopped. If these mechanisms don't successfully detect the malware, the static and dynamic detection mechanisms are still in place to stop the malware.

This test considers all of the protection mechanisms that are included in today's security software and challenges them against real-world threats in order to determine the real protection capabilities of the products. The results of test and the corresponding details will be presented on the next few pages.

Products Tested

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

- Microsoft Windows Defender 4.0
- Symantec Norton 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 (Release Preview Build 8400) with all patches that were available on July 1st 2012.

The URLs have been accessed with Firefox 13.0.1.

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	Flash Player 10 ActiveX	10.0.12.36
Adobe	Flash Player 10 Plugin	10.0.12.36
Adobe	Acrobat Reader	V8 or v9
ICQ	ICQ6	6.00.0000
Sun	Java SE Runtime Environment 6 Update 1	1.6.0.10
Mozilla	Firefox (2.0.0.4)	2.0.0.4 (en-US)
Apple	QuickTime	7.3.0.70
Real Networks	RealPlayer	10.5
WinZip Computing LP	WinZip	10.0(6667)
Yahoo! Inc	Messenger	8.1.0.413

Testing methodology

The test was 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.

Efficacy Rating

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.

Samples

The malware set contains 50 direct downloads and drive-by-downloads. No mails with malicious attachments have been included in this test. In addition to this, 26 known clean programs were used for the false positive testing. The details to the samples used can be found in the appendix.

Test Results

Symantec achieved the best score with blocking every attack that was used in this test.

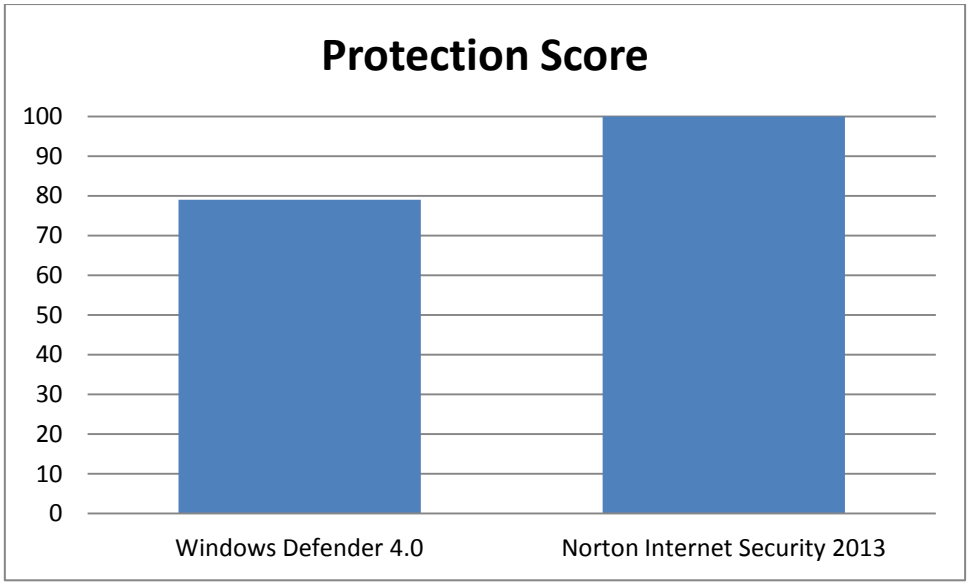

Figure 2: Protection Score

In Figure 2 the overall result is given. Out of 100 possible points Norton achieved 100. Windows Defender managed to block 44 threats out of 50 completely and blocked some components of another threat. 5 threats were not blocked, resulting in a score of 79.

It has to be noted, that the generic SmartScreen messages have not been counted as detection as they are not clearly telling that a malicious file has been found. Instead they only tell that an unrecognized app has been found and delegate the decision to the user, see screenshot below.

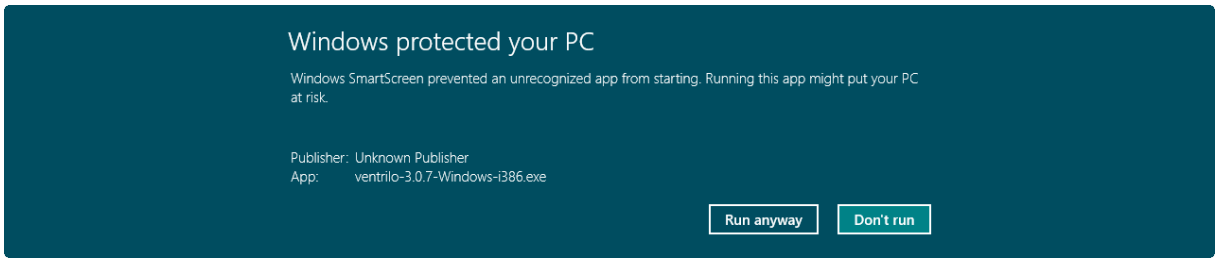

Figure 3: SmartScreen Detection

Besides the detection and blocking of malware, it is important to have a well balanced product so that no clean applications will be blocked or detected as malware. Therefore, 26 widely known applications were used to determine whether any product would report them as being suspicious or malicious. Neither Norton nor Windows Defender had any problems here. There were no false warnings or blockings.

The results show that Windows 8 offers a fair baseline protection with the included Windows Defender. The SmartScreen filter adds another layer of security for web based threats but require the user to make the decision, which most users probably can't do. Norton instead takes all the decisions on its own and does not rely on the user, successfully blocking all attacks with zero false positives.

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Microsoft	Microsoft Windows Defender	4.0.8400.0	1.1.8502.0/ 1.129.1589.0
Symantec	Norton Internet Security 2013	20.0.0.132	n/a

List of used malware samples

Direct Downloads	
http://www.xhamstersesli.com/wp-content/themes/rt_affinity_wp/js/rokbox/themes/dark/dark.exe	http://tube214-host.mrbonus.com/download-id92503/flash_player_installer.exe
http://directlink.tv/f/e43bb2_img65nakedtightteen.exe	http://188.132.163.17/nn.exe
http://fotograftrapp.se/UPDATE.exe	http://www.entmedikal.net/Scripts/Scripts.exe
http://rap-mag.fr/S8FRKQM7K2.exe	http://liptee.ru/zs/bot.exe
http://212.124.118.16/strung.exe	http://ddoser.pro/dsak.exe
http://vinday.org/soft/antivirus.exe	http://www.bahrainprimeminister.net/images/wafat%20hekem%20albahrain/wafat%20hekem%20albahrain.exe
http://mgdrp.eu/m/o.exe	http://volam2-auto-ver1.googlecode.com/files/VoLam2-Autover9.exe
http://auto-vip-volam2.googlecode.com/files/autofullvolam2.exe	http://14-1-2011.com/inst_e.exe
http://www.mesuu.com/smssc.exe	http://vdh-parts.nl/q2k.exe
http://www.fenessaw.com/pdf/Neslihn_demirz_STupPhoto.exe	http://vin4game.110mb.com/HackGame.com
http://www.chatkolik.org/tmirc.exe	http://medianet.yartel.ru/dou/dou3//images/banners/Intimacao.com
http://mer30.org/generic/k25.exe	http://c-d-b-d.googlecode.com/files/ngu.exe
http://www.iznikmavicini.com/_vti_cnf/3.exe	http://69.162.82.26/version2/webber/1/bot.exe
http://massmail.isandt.com/xt9ptH87/BUPQ4u.exe	http://overhill.comicgenesis.com/yJ1sth2P/5YRcxZ.exe
http://atsd.com.au/DM6jo1NE/Bss.exe	http://78.38.244.12/dl/rat.exe
http://pwndu.no-ip.org/xbl%20code%20generator.exe	http://coolfiles.toget.com.tw/off_line/wbsbetav.exe
http://www.amciks.com/Giris.exe	http://ifacebooklogin.com/download/pluginVideo309.exe
http://cheats-tankionline.com/texture.exe	http://guessit.in/ORANT/ORAINST/ORAINST.exe
http://s3.amazonaws.com/cncncn/zyklon.exe	http://bvnscope.info/jjegbs/icvbxn.exe
http://salonywpolsce.pl/m03.exe	http://boundlessblue.com.au/12.exe
http://winsecuritysys.com/exe/32.exe	http://volamtruyenky12.110mb.com/ChipFeeAutoProvl2710.com
http://xxlx.altervista.org/drona.exe	http://8975674.org/download/adobe.exe
http://bidikmisi.polibatam.ac.id/wp-includes/images/OpenSSL/Copyright/Postales_Amor.exe	http://therfordium.ru/mz/l/x.exe
http://tubesworldjxw.co.cc/hot/xxx-HD-movie.avi.exe	http://ventrilo4download.com/ventrilo-3.0.7-Windows-i386.exe
http://91.229.20.105/srv1.1.exe	http://ipchanger-download.pl/Bynacam.exe

List of used clean samples

Program name	
7-Zip 9.20	IrfanView 4.33
Adobe FlashPlayer 11.3.300.262	iTunes 10.6.1.7
Adobe Reader 10.1.3	Java 7u4
Ashampoo Burning Studio 6.8 Free	Libre Office 3.5.4
CCleaner 3.20	Notepad++ 6.1.4

Daemon Tools Lite 4.45.4	Picasa 3.9
DVD Shrink 3.2.0.15	Recuva 1.42.544
DVR Studio HD 2.23	Skype 5.8.0.158
Firefox 13.0.1	Teamviewer v7.0.12979
Gimp 2.8.0	Thunderbird 13.0.1
Google Chrome 19.0.1084.52 m	VLC Media Player 2.0.1
Google Earth 6.2.2.6613	Winamp 5.63
ImgBurn 2.5.7.0	Winzip 16.5

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