

Real World Testing Report

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

Date of the report: January 27th, 2011, last update: February 10th, 2011

Executive Summary

In January 2011, AV-Test performed a comparative review of 6 corporate endpoint security products 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 accessed via direct links to malicious executable files, by drive-by-download websites that utilize exploits and by opening mail attachments.

The malware test corpus consisted of 52 samples, including direct downloads and drive-by-downloads. The false positive corpus consisted of 50 known clean applications. To perform the single test runs, a clean Windows XP image was used on several identical PCs. On this 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. For the false positive part, 50 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.

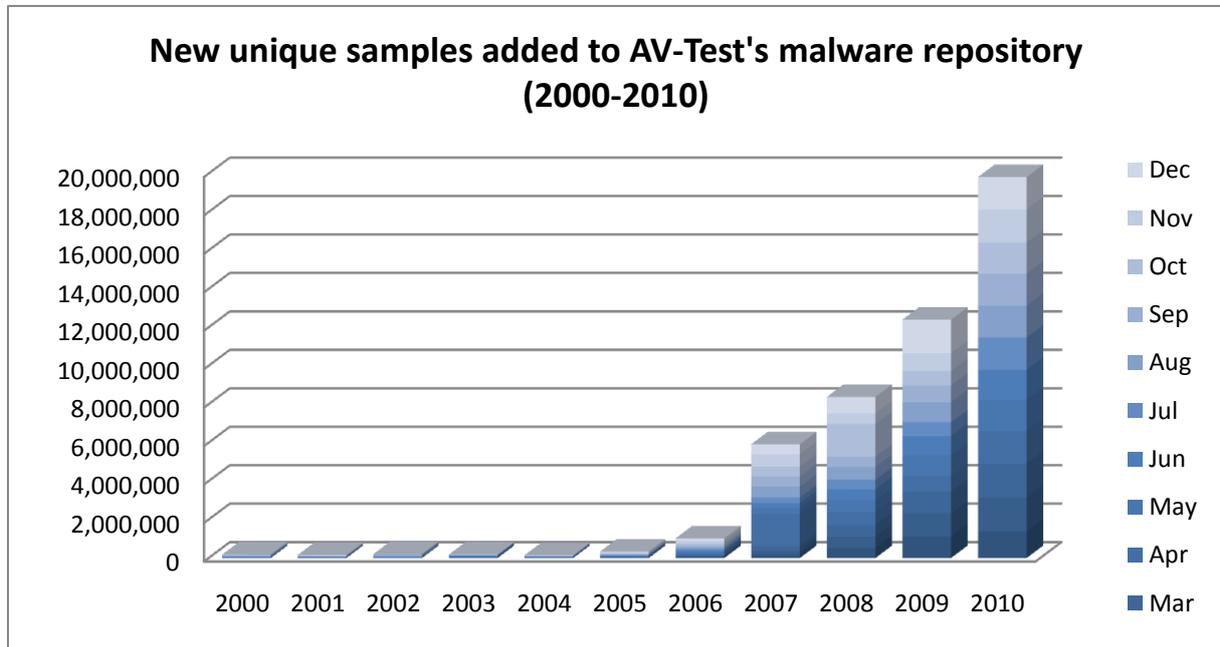


Figure 1: New samples added per year

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 2011. 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 between December 2010 and January 2011. AV-Test used the latest releases available at the time of the test of the following six products:

- Kaspersky Anti-Virus 6.0 for Windows Workstations
- McAfee VirusScan Enterprise 8.7.0i
- Microsoft Forefront Client Security 2.0
- Sophos Endpoint Security and Control 9.5.4
- Symantec Endpoint Protection 12.1 (Pre-Beta Release)
- Trend Micro OfficeScan 10.5

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 XP Service Pack 3 with only those hotfixes that were part of SP3. 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 52 samples which are split into 38 direct downloads and 14 drive-by-downloads. In addition to this, 50 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 Endpoint Protection 12.1 achieved the best overall score. This is the combined result of the three individual test sets that the products were tested against. The individual results of the direct exe downloads, the drive-by-downloads and the malicious mail attachments will be discussed below.

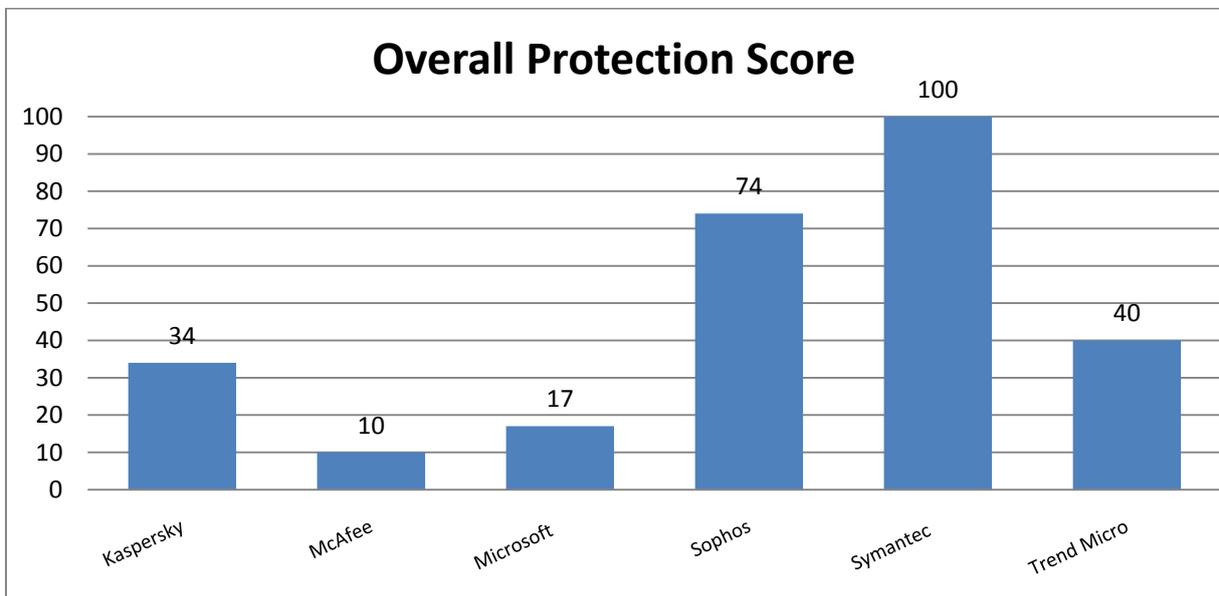


Figure 2: Overall Score

In Figure 2 the overall result is given. Out of 104 possible points, Symantec achieved 100, which was the best result in the test. This product is closely followed by Sophos with a score of 74. The other four products are considerably behind, with a score below the average of 46. This is partly due to the configuration of the products. Since all tests have been performed with default settings, some protection mechanisms were not explicitly enabled or modified to a different configuration.

When looking at the individual scores, several observations can be made. Depending on the test set, some products perform better or worse than others, while other products remain at a consistent level.

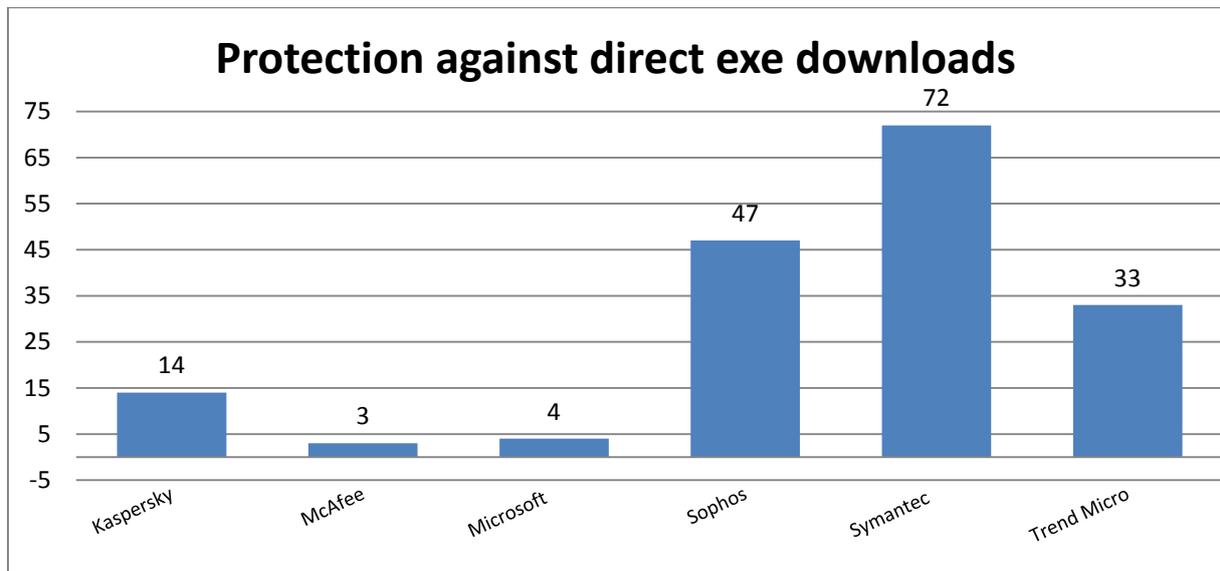


Figure 3: Protection against direct exe downloads

In Figure 3, the protection against direct exe downloads is shown. The best result in this section has been achieved by Symantec, which scored 72 out of 76 points. It was followed by Sophos with 47 and Trend Micro with 33 points. The worst result was 3 points. The average was at 29 and the median at 24. Three products were able to score better than the average, while the other three products scored worse.

The scores for the protection against drive-by-downloads are given in Figure 4. The best result with 28 out of 28 possible points comes from Symantec. Sophos and Kaspersky scored well too, with 27 resp. 20 points.

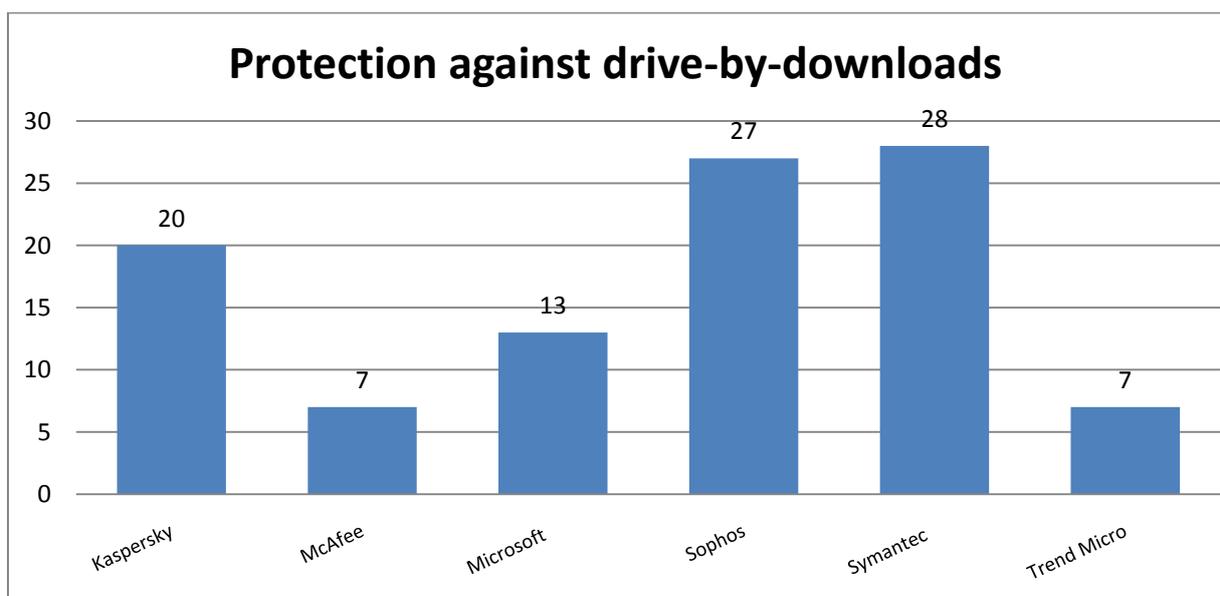


Figure 4: Protection against drive-by-downloads

The worst score here is 7, the average score as well as the median was at 17. Three products were able to score better than the average and three products were below the average.

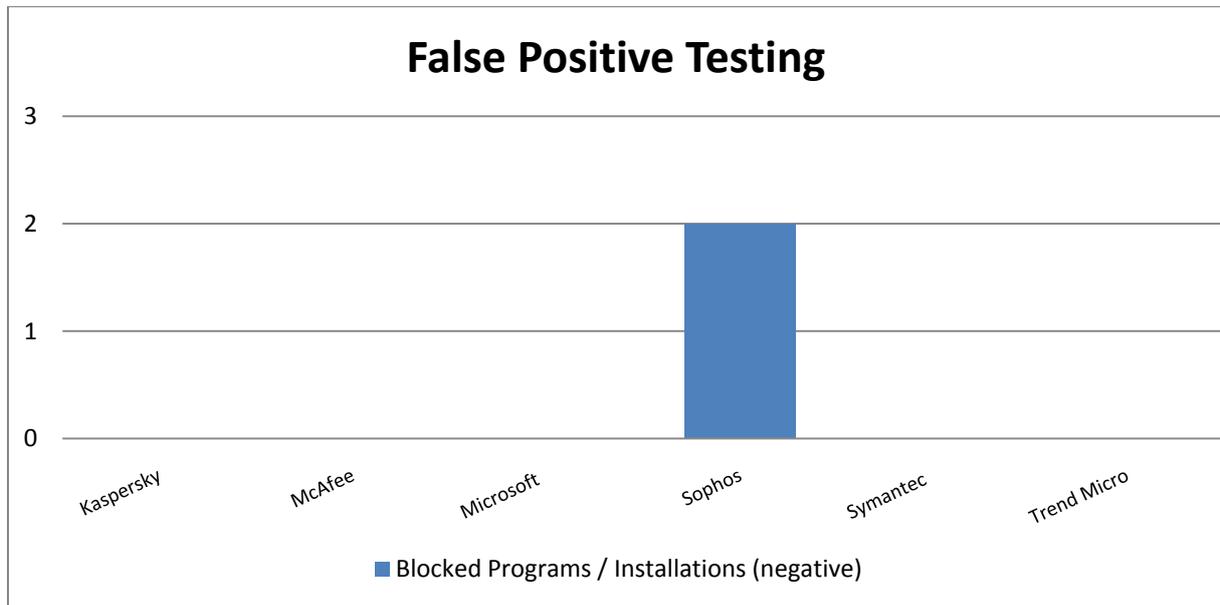


Figure 5: False positive results

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, 50 widely known applications were used to determine whether any product would report them as being suspicious or malicious. Besides Sophos, no product reported any of the applications and therefore didn't cause any false positives. Sophos reported two applications and blocked the execution of one of it.

The individual scores clearly show that there exist big differences between the tested products, depending on the test set and what features the products can utilize. There are a few products that successfully combine static and dynamic detection with URL blocking or exploit detection. These achieve, not surprisingly, the best scores in the test and provide the most reliable protection: Symantec and Sophos. While most of the other products do offer similar features, not all of them could be used in this test, since they may require additional configuration, which cannot be reflected in this test that has been performed in default settings only. Therefore it is important to remember, that the products which did score bad in this test, may achieve much different scores, when configuring them differently. Therefore this test primarily shows which product protects you best, without the need for additional configuration.

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Kaspersky Lab	Kaspersky Anti-Virus 6.0 for Windows Workstations	6.0.4.1424d	n/a
McAfee	McAfee VirusScan Enterprise	8.7.0i	5400.1158 / 6196.0000
Microsoft	Microsoft Forefront Client Security	2.0.522.0	1.1.6402.0 / 1.95.1764.0
Sophos	Sophos Endpoint Security and Control	9.5.4	3.14.1 / 4.60G
Symantec	Symantec Endpoint Protection (Pre-Beta Release)	12.1.175.3818	20101.3.0.103 / 121213ah
Trend Micro	Trend Micro OfficeScan	10.5.1083	9.205.1002 / 1.271.00

List of used malware samples

Direct Downloads	
(020) http://89.187.50.229/setup.exe	(172) http://www.derany.com/2010/media/Ver.php?DowloadClient=DepositoOnLine
(025) http://harmatan.pl/img/%2C%2C%2C/DSC862010.scr	(187) http://www.zxekm.info/1/yk.exe
(028) http://cypbet.com/kel.exe	(188) http://206.217.196.220/flash.exe
(030) http://84.127.113.164/1/load/load.exe	(190) http://tgong.co.kr/mall/updir/md/pds.exe
(035) http://188.65.73.243/v2/update_adobe_flash.exe	(196) http://72.11.141.220:38250/img/fmenzegna.exe
(041) http://www.completochave.com/img/Cobranca.php	(204) http://a-cipher.com/pidgin.exe
(052) http://www.nar0tix.info/servers/PaypalHack.exe	(205) http://prodep.ir/.hubf5zp/?getexe=rb.exe
(055) http://www.solvex.spb.ru/uploads/media/exe.exe	(238) http://h1.ripway.com/okn0101/b.exe
(056) http://h1.ripway.com/bros/cash-full.exe	(241) http://www8.4fjj.com/2.exe
(060) http://erayzan.com/Jennifer-Sexy.jpg	(242) http://tvnews.server.tl/OFUXICOTVNEWS/PLUGIN/Install-Tv-FlashPlayer.exe
(065) http://ohgirls.omiki.com/videos/Play_Video83294_Click_Run.exe	(263) http://performancecarcompany.com/stock/car4/OLDBTN.exe
(067) http://qnlogger.cba.pl/Server/Server(1.0.0.7).exe	(270) http://mpuq.net/anide.exe
(118) http://cushyhost.com/files/878476990ecb3a1e43bf7c06a6706cb4.exe	(272) http://2b.perfectexe.com:88/gd.exe?t=3D0.3495956
(123) http://tualimforum.com/images/christmas.scr	(274) http://www.siquiero.com.uy/Connections/gusanito/teamo/Adobe_Flash_Player10.0.45.2.exe
(130) http://www.darwinfoundation.org/galapedia/images/1/1b/img.exe	(282) http://www.estilobordado.com.br/includes/local/imagem.exe
(137) http://www.fernspaeh.de/cac.exer	(304) http://fusiontechad.com/images/facebook-pic000934519.exe
(142) http://versionstring.com/version/check.php?ver=9024&app=snv-timer-3.0.4	(328) http://fo.qvad.info/gvod_onlinefo03.exe
(149) http://65.254.51.46/~repot127/imvu_smileys.exe	(336) http://206.217.196.220/sys.exe
(169) http://mailing.servehttp.com/modules/mod_banners/Open_comprovante.com?retorno_j.santos@ct1jib.com	(337) http://pornocomsexo.com/VideoLoira.com
Drive-by-Downloads (Exploits)	
(001) http://mavericonjk.co.cc/c1358d9072	(015) http://ceweyaki.info/tre/LALA.asp/xH13e9762eV0100f055006R81fc905c106T5ec334bb20310009329
(003) http://www.rb16888.com/csw/Skin/index.htm	(018) http://192.49.222.67/help.html
(004) http://iis.dengyan520.com/iis/nb.htm	(020) http://yahoocommerce.info/nte/avorp1boba.asp
(006) http://174.128.242.250/iis/apr/nb.htm	(021) http://af2t.cz.cc/imgurl.php?hl=2477c69b3cad8b0c
(007) http://donette.info/tre/PENA.py	(022) http://www.middleeastnews.com/info.html
(008) http://cartgovernment.co.cc/other/alyppfjqitdisena.php	(024) http://www.heliosingenieria.com/admin/proceso-de-planeacion-estrategica/gordan-ramsey-recipe.html
(010) http://tomklotin.zapto.org/tonkis/	(025) http://www.monhon.com.tw/product_reviews.php?cPath=55_45&products_id=178&osCsid=eu0q6r58g3gq4cj2v4m04tic01

List of used clean samples

Program name	Distribution
Sandra 2010 v17.25	Hundreds of users
Skype 5.0	Hundreds of users
Thunderbird 3.1.7	Hundreds of users
eMule 050a	Hundreds of users
MP3 Rocket Download 2.1.3.2	Hundreds of users
Sandra 2010 v17.25	Hundreds of users
Orbit Downloader 4.0.0.5	Thousands of users
Free Mp3 Wma Converter 1.91	Thousands of users
Total Commander 7.56	Thousands of users
Wise Registry Cleaner Free 5.88	Thousands of users
FreeZ Online TV 1.40	Thousands of users
Trillian Astra 4.2.0.23	Thousands of users
7-Zip 9.20	Tens of thousands of users
Divx 8.1.2 Build 10.2.1-20	Tens of thousands of users
GIMP 2.6.11	Tens of thousands of users
mIRC 7.15	Tens of thousands of users
Notepad++ 5.8.5	Tens of thousands of users
Paint.NET 3.5.6	Tens of thousands of users
TeamViewer 6.0.9947	Tens of thousands of users
True Crypt 7.0a	Tens of thousands of users
Winamp 5.6	Tens of thousands of users
AutoIT 3.3.6.1	Tens of thousands of users
Download Accelerator Plus 9.5.0	Tens of thousands of users
EA Download Manager 7.2.0.32	Tens of thousands of users
Filezilla 3.2.7.1	Tens of thousands of users
FlashGet 3.5.0.1126	Tens of thousands of users
FoxTab FLV Player	Tens of thousands of users
Free Recorder 4.1	Tens of thousands of users
Foxit Reader 4.3.0.1110	Tens of thousands of users
Hamachi 2.0.3.89	Tens of thousands of users
AIMP 2.61 Build 583 Final	Tens of thousands of users
Virtual DJ 7.0	Tens of thousands of users
jDownloader 0.9579	Tens of thousands of users
Picasa 3.8.0 build 117.29.0	Tens of thousands of users
Safari 5.0.3	Tens of thousands of users
uTorrent 2.2 build 23703	Tens of thousands of users
YouTube Downloader 2.6.4	Tens of thousands of users
CCCleaner 3.01.1327	Hundreds of thousands of users
DAEMON Tools Lite 4.35.6.0091	Hundreds of thousands of users
Google Talk 1.0.0.104 Beta	Hundreds of thousands of users
iTunes 10.1.0.56	Hundreds of thousands of users
IrfanView 4.27	Hundreds of thousands of users
Open Office 3.2.1	Hundreds of thousands of users
Photoscape 3.5	Hundreds of thousands of users
VLC Player 1.1.5	Hundreds of thousands of users
WinRAR 3.93	Hundreds of thousands of users
net Framework 4.0	Hundreds of thousands of users
DVD Shrink 3.2.0.15	Hundreds of thousands of users
RocketDock 1.3.5	Hundreds of thousands of users
Google Desktop 5.9.1005.12335	Millions of users
Spybot Search & Destroy 1.6.2	Millions of users