Real World Testing Report

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

Date of the report: August 18th, 2010, last update: August 24th, 2010

Executive Summary

During August 2010, AV-Test performed a comparative review of 13 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 57 samples, including direct downloads, drive-by-downloads and malicious mail attachments. The false positive corpus consisted of 25 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, 25 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 Norton 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.

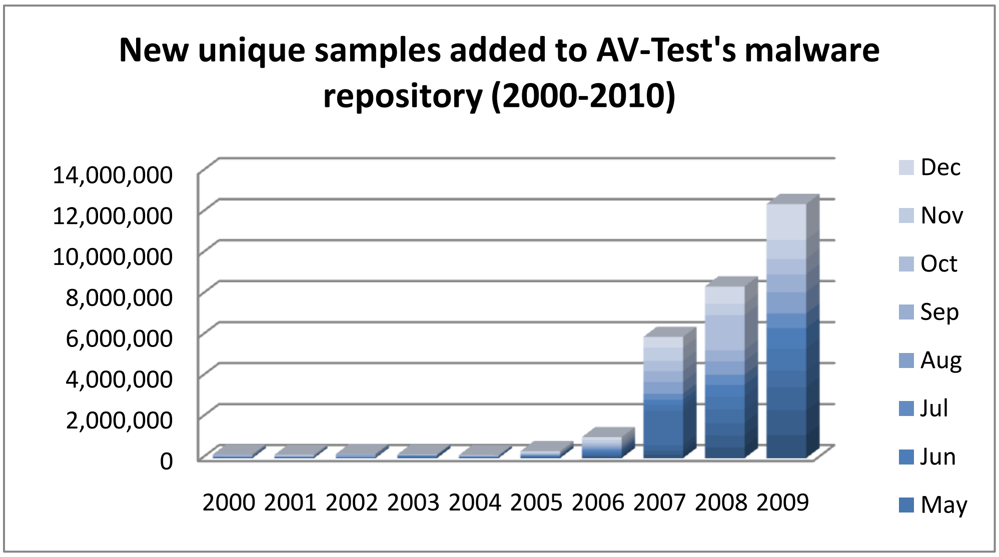

Figure 1: New samples added per year

In the year 2000, AV-Test received more than 170,000 new samples. In 2009 the number of new samples has grown to over 12,000,000 and the numbers continue to grow in the year 2010. 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 latest versions (at the time of the test) of each of the following 13 products were tested:

- Avast! Free AntiVirus 5.0
- AVG Anti-Virus Free Edition 9.0
- Avira Antivir Personal Version – Free Antivirus 10.0
- BitDefender Internet Security 2010
- ESET Smart Security 4
- GDATA Internet Security 2011
- K7 Total Security 10.0
- Kaspersky Internet Security 2011
- McAfee Internet Security 2010
- Microsoft Security Essentials 1.0
- Norton Internet Security 2011
- Panda Internet Security 2011
- TrendMicro Internet Security 2010 Pro

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 2 with only those hotfixes that were part of SP2. 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 57 samples which are split into 33 direct downloads, 18 drive-by-downloads and 6 malicious mail attachments. In addition to this, 25 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 Norton Internet Security 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.

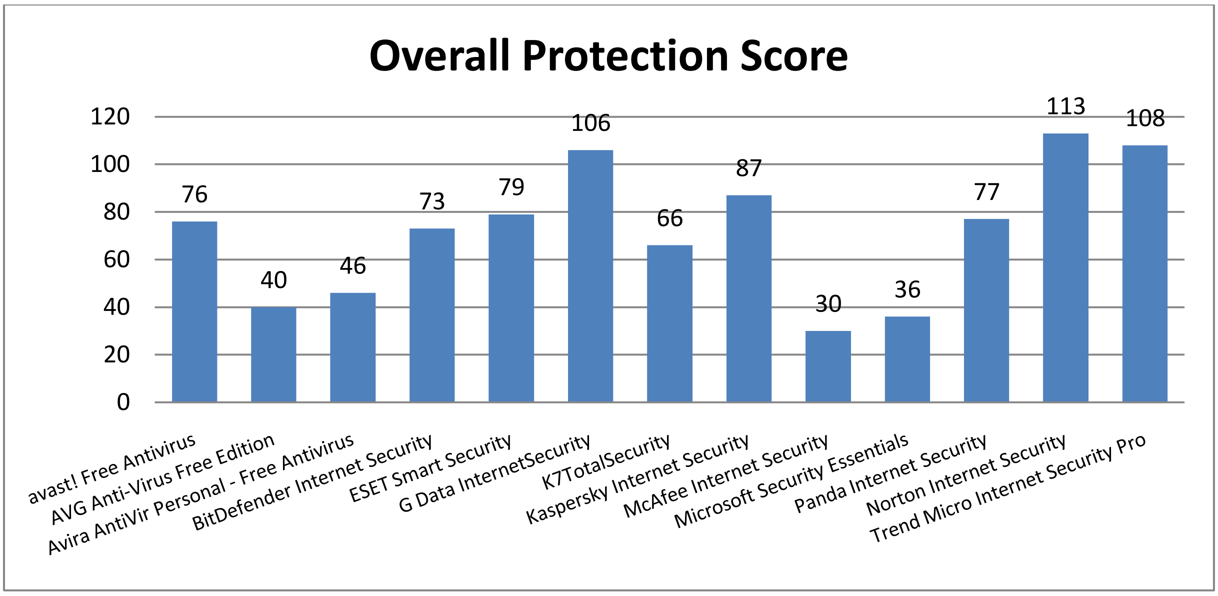

Figure 2: Overall Score

In Figure 2 the overall result is given. Out of 114 possible points, Norton achieved 113, which was the best result in the test. This product is closely followed by Trend Micro Internet Security Pro with 108 and G Data Internet Security with 106 points. The worst overall result was 30. The average result was 75 and the median was at 76 points. Seven products scored above the average, while six products scored worse than the average.

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.

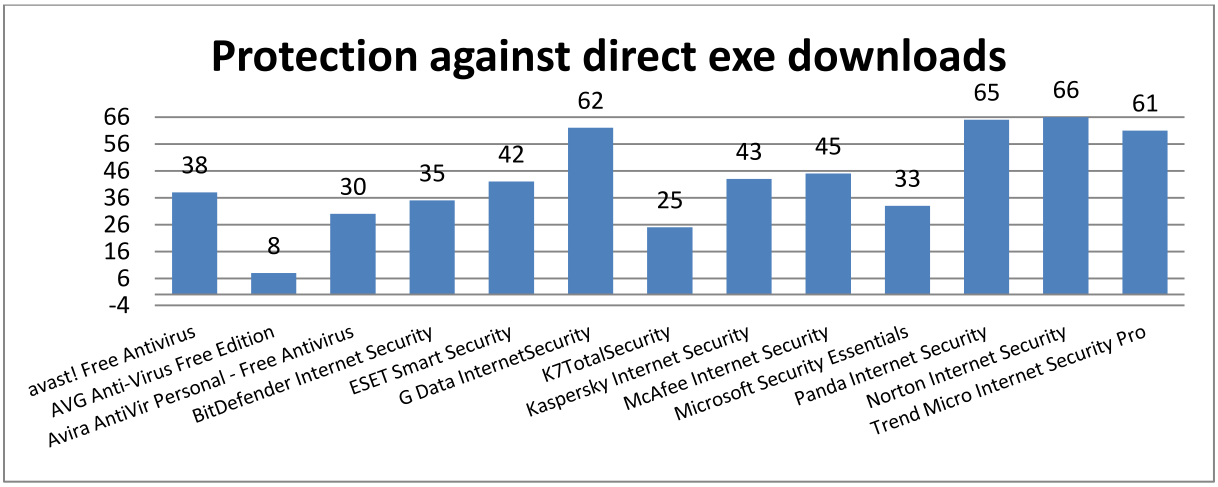

Figure 3: Protection against direct exe downloads

In Figure 3, the protection against direct exe downloads is shown. The best result in this section has been achieved by Norton, which scored 66 out of 66 points. It was closely followed by Panda with 65, G data with 62 and Trend Micro with 61 points. The worst result was 8 points. The average was at 44 and the median at 42. Only five products were able to score better than the average, while eight products scored worse. In fact, besides the 4 mentioned products, all others had scores lower or equal to 45.

The scores for the protection against drive-by-downloads are given in Figure 4. The best results with 35 or 36 out of 36 possible points come from several products. Avast, AVG, Eset, Kaspersky, Norton and Trend Micro succeeded in blocking all or nearly all threats in this category.

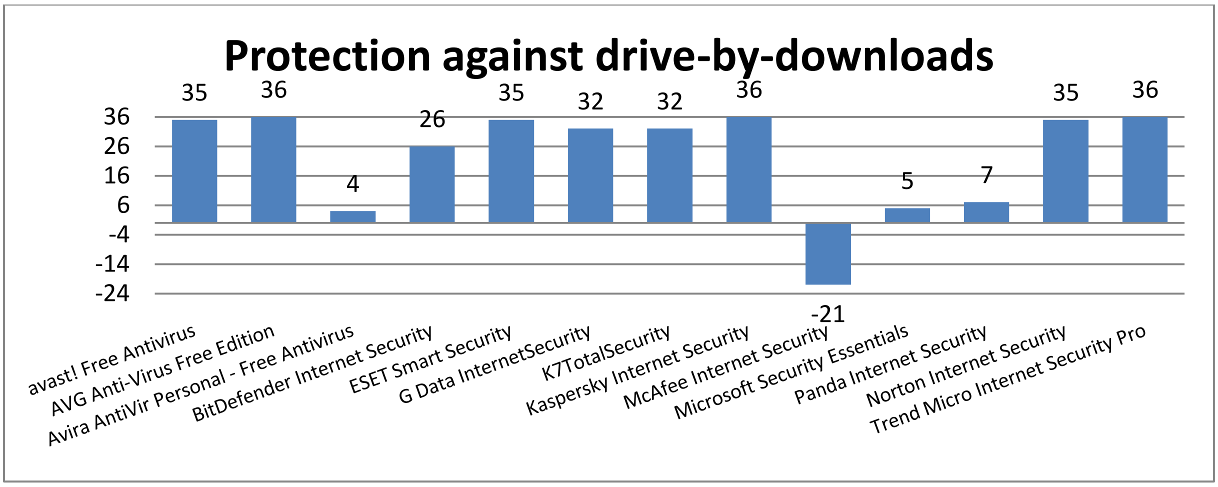

Figure 4: Protection against drive-by-downloads

The worst score here is -21, which indicates that the majority of the attacks were successful when using that product. The average score was at 24 and the median at 32. Nine products were able to score better than the average and only 4 products were below the average.

In Figure 5, the protection against malicious mail attachments is shown. Again, several products were able to reach a 100% score with 12 out of 12 points. This included Avira, BitDefender, G Data and Norton. Trend Micro lost only one point and reached a score of 11. The worst result in this test was -4. The average was at 7 and the median at 8. Seven products scored better than the average and 6 products were below the average.

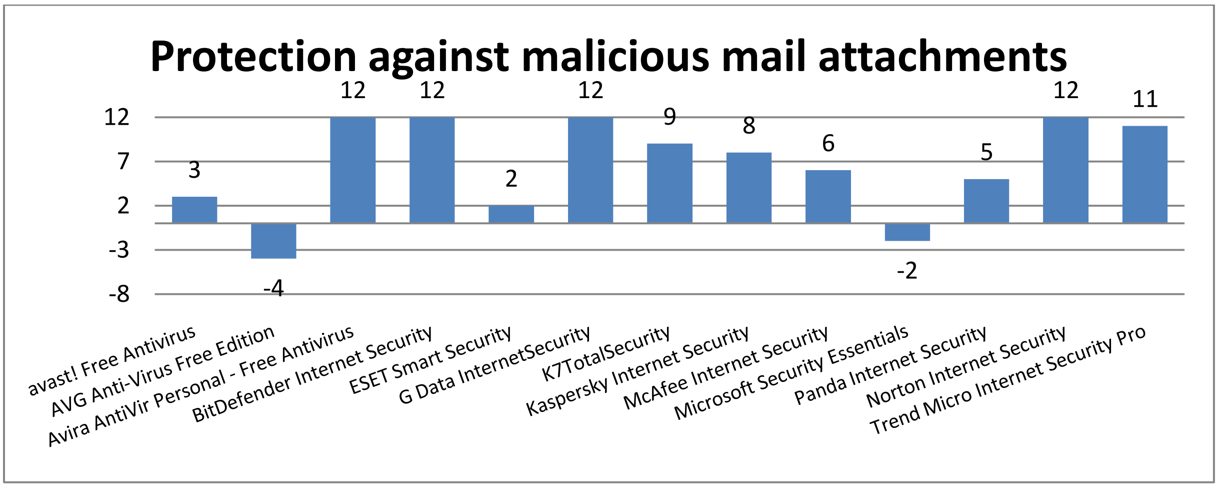

Figure 5: Removal score for Fake AV

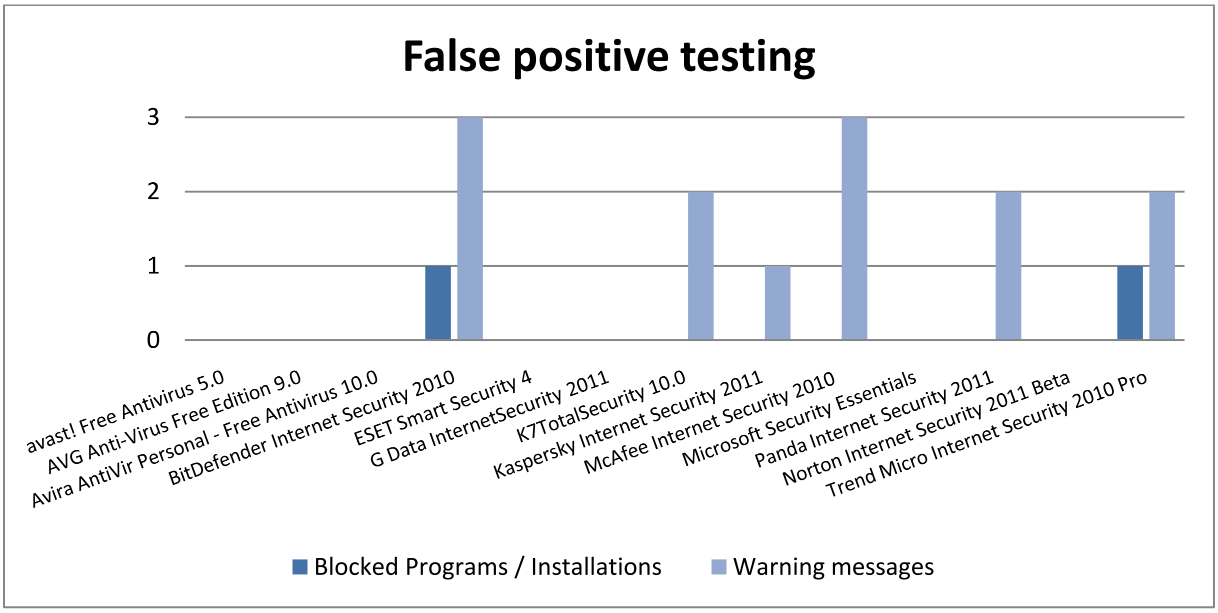

Figure 6: False positive results

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, 25 widely known applications were used to determine whether any product would report them as being suspicious or malicious. Avast, AVG, Antivir, Eset, G Data, Microsoft and Norton didn't report any of the applications and therefore didn't cause any false positives. Two products did block one application: these were BitDefender and Trend Micro. Furthermore BitDefender and McAfee warned about 3 applications, but didn't block them. K7, Panda and Trend Micro warned about 2 applications and Kaspersky warned about 1 application.

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: Norton, Trend Micro, G Data and Kaspersky. Other tested products do have their strong sides but either lack some of the other features or need to improve them. Examples are products that have very strong static detection, e.g. by using in-the-cloud queries. They score high on the test set which consists of direct exe downloads, because static signatures are a perfect way to catch these. However, the results for the drive-by-downloads show, that those detection mechanisms don't work that good here. Either dynamic detection or blocking at an earlier stage (URL/exploit blocker) is required.

Sometimes, good protection is accompanied by a higher risk for false positives. While Trend Micro protects about as good as Norton and G Data, it had some false warnings and even blocked one legitimate application. Norton and G Data didn't cause any problems in that respect and combine a very good protection with a zero false positive score.

Appendix

Version information of the tested software

Developer, Distributor	Product name	Program version	Engine/ signature version
Alwil Software	avast! Free Antivirus 5.0	5.0.594	100802-0
AVG	AVG Anti-Virus Free Edition 9.0	9.0.851	271.1.1/3045
Avira	Avira AntiVir Personal - Free Antivirus 10.0	10.0.0.567	8.02.04.32/ 7.10.10.26
BitDefender	BitDefender Internet Security 2010	13.0.21.347	7.33151
ESET	ESET Smart Security 4	4.2.58.3	5334
G Data	G Data InternetSecurity 2011	21.0.2.1	Engine A (AVA 21.1806), Engine B (AVB 21.229)
K7 Computing	K7TotalSecurity 10.0	10.0.0039	10.0.0039/ 10.0.0039
Kaspersky Lab	Kaspersky Internet Security 2011	11.0.1.400 (a)	n/a
McAfee	McAfee Internet Security 2010	10.5.194	5400.1158/ 6061.0000
Microsoft	Microsoft Security Essentials	1.0.1963.0	1.1.6004.0/ 1.87.1016.0
Panda Security	Panda Internet Security 2011	16.00.00	2.3.1511.0
Symantec	Norton Internet Security 2011	18.1.0.22	n/a
Trend Micro	Trend Micro Internet Security 2010 Pro	17.50.1647	9.120.1004/ 7.355.50

List of used malware samples

Direct Downloads	
(049) http://95.211.132.20/s/3150.exe	(108) http://info.collectionerrorreport.com/dead.exe
(053) http://gepare.com/ddt/exe.exe	(109) http://license.itsaol.com/Free.Movie.License.exe
(065) http://ferdinandi.ru/localhost/nat.exe	(111) http://server2.codienviet.com/bot/svihost.exe
(068) http://williandbilly.net/bot.exe	(113) http://termsoftraffic.co.cc/installer.0042.exe
(069) http://garst33.com/setup/aaa.exe	(120) http://fksa.net/server.exe
(071) http://deilaeyeew.ru/bin/saejuogi.exe	(121) http://tubehotmix.info/Flash.HD.exe
(073) http://ootaivilei.ru/bin/baiquaad.exe	(122) http://www.host1ng.com/Daemon.exe
(075) http://yeeshiedot.ru/bin/oomiephe.exe	(127) http://www.chatroulettem.com/videoizlemekicinindir.exe
(077) http://208.53.183.113/mq.exe	(130) http://mydeli.ru/1/1.exe
(078) http://www.asiawholesalers.net/c.exe	(132) http://www.zhongweifeed.com/sx.exe
(079) http://91.216.215.77/uk/win7.exe	(143) http://113.11.194.167/us2070/usa-dase.exe
(080) http://spainfoodandwine.com/_outhES.exe	(155) http://113.11.194.167/us2070/usa-dase.exe
(081) http://188.65.74.161/mrmun_sgjlgdsjrthrtwg.exe	(158) http://69.50.221.188/x44/load/load.exe
(083) http://188.65.74.161/varag_sdfgkwlkgadfshn.exe	(160) http://benassibrosmihael.com/xman/spm2.exe
(096) http://58.215.240.218/qd.netkill.com.cn/da.exe	(161) http://colloquialewfe.info/retn/sqjcmb4/load/kt0rs9rn3.exe
(098) http://91.216.215.77/uk/win7.exe	(163) http://file-sharing-new.co.cc/sp/install-166.exe
(099) http://ad.ghura.pl/mm.exe	
Drive-by-Downloads (Exploits)	
ajileconsulting.com	faerymist.com/pamelor

belkosmetik.com.ua	galerie.proaudiosystems.ro
chocomana.com	goodacnetreatments.com
clickpyramid.com	laxfights.com
delhirealtyservices.com	penis-enlargement-male-enhancement.atspace.com
demoparty.us	przyslowia.gentelmen.net
dmem-mecanique.com	sp3s.org
eraserinc.narod.ru	splintercell.gamefan.cz
faerymist.com/minuteviagra	stuffedanimals.barelyfunky.com
Malicious E-Mail attachments	
(01) "You have received a file from…"	(04) "Lance Armstrong paper"
(02) " DHL Delivery Service"	(05) "Resume as discussed"
(03) "Financials"	(06) "Picture sizes"

List of used clean samples

Program name	Distribution
DaemonTools 4.36.0310.0089	Fewer than 10 users
GoogleEarth 5.2.1.1329	Fewer than 10 users
DriveImage XML 2.14	Hundreds of users
Secunia PSI 1.5.0.2	Hundreds of users
Thunderbird 3.1.1	Hundreds of users
Firefox 3.6.8	Thousands of users
Foxit Reader 4.1.1.0804	Thousands of users
FreeYouTubeToMp3Converter 3.7.17.183	Thousands of users
Logitech SetPoint 4.80.103	Thousands of users
Notepad ++ 5.7	Thousands of users
Defragler 1.20.201	Tens of thousands of users
FileZilla 3.3.3	Tens of thousands of users
FlashGet 3.5.0.1126	Tens of thousands of users
Hamachi 2.0.2.85	Tens of thousands of users
InfraRecorder 0.50.0.0	Tens of thousands of users
OpenOffice 3.2.1 (build 9502)	Tens of thousands of users
Opera 10.60 (3445)	Tens of thousands of users
Recuva 1.38.504	Tens of thousands of users
utorrent 2.0.3 (build 20664)	Tens of thousands of users
Yahoo! Widgets 4.5.2 (build 10A50)	Tens of thousands of users
Ccleaner 2.34.1200	Hundreds of thousands of users
DVD Shrink 3.2.0.15	Hundreds of thousands of users
Picasa 3.6.0 (build 105.67, 0)	Hundreds of thousands of users
Skype 4.2.0.169	Hundreds of thousands of users
Windows Live 14.0.8117.416	Hundreds of thousands of users