PC Total Protection Suites 2011

A Dynamic Anti-Malware Comparison Test

Dennis Technology Labs, 26/01/2011
www.DennisTechnologyLabs.com

This test aims to compare the effectiveness of the most recent releases of popular security suites. These programs typically include anti-virus and firewall features alongside a collection of other utilities and services.

A total of 11 products were exposed to genuine internet threats that real customers could have encountered during the test period. Crucially, this exposure was carried out in a realistic way, reflecting a customer's experience as closely as possible. For example, each test system visited genuinely infected websites and downloaded pages, exploits and malicious files exactly as an average user would.

We also tested how each product handled legitimate applications. These were downloaded from Download.com or the original site as directed by Download.com. The popularity of each program was taken into account.

Products are awarded marks for detecting real threats and providing adequate protection. Points are deducted for failing to protect the system and for falsely condemning legitimate software.

Executive summary

Products tested

- Avira Premium Security Suite 2011
- BitDefender Total Security/Internet Security 2011
- ESET Smart Security 4
- F-Secure Internet Security 2011
- G Data TotalCare/InternetSecurity 2011
- Kaspersky PURE/Internet Security 2011
- McAfee Total Protection/Internet Security 2011
- Panda Global Protection/Internet Security 2011
- Symantec Norton 360 v5/Internet Security 2011
- Trend Micro Titanium Maximum Security/ Internet Security 2011
- Webroot Internet Security Complete 2011

- **There is a vast difference between the effectiveness of anti-virus programs**

This test's results show that different anti-virus products have very different protection capabilities. The Norton product protected against all of the threats, but this was the only one to do so. Trend Micro Titanium Maximum Security 2011 finished a close second, having been compromised just once. McAfee's was the least effective product, allowing nearly half of the threats to infect the system.

- **Some threats are so aggressive that they disable anti-virus scanners**

Some of the most visible threats, including fake anti-virus and hard disk utility programs, prevented legitimate applications from running. Most notably the malware blocked the anti-virus products themselves, as well as our monitoring tools and other programs installed on the test systems.

- **Some security products are so aggressive or paranoid that they block popular legitimate applications**

The ideal successful security product blocks threats and allows useful software to run. Security vendors need to balance their products' behavior so that most threats are blocked and most legitimate programs will run unhindered. While Webroot's product prevented many threats, it also blocked or warned against a large number of legitimate applications. ESET's product was notable for its combination of good protection and ability to allow all of the genuine software to install and run.

Simon Edwards, Dennis Technology Labs

About This Test

What is total protection?

Most major anti-virus brands come packaged in a range of products. Typically these fall into three main areas: a basic anti-virus program; an 'internet security' bundle; and a premium package that includes extra services and tools. In this test we concentrate mainly on the protection afforded by the premium 'total protection' suites.

Common features

Before we explore the test's results, let's look a little further into what makes a suite into a premium product. Usually a vendor will add features to its established internet security application, which in turn is a more fully-featured version of the basic anti-virus program. These features may include backup services or software, system optimization tools and parental controls.

For example, Symantec sells an anti-virus program called Norton Antivirus, a more fully-featured application called Norton Internet Security and a premium product called Norton 360. Norton Internet Security includes Norton Antivirus and adds a firewall and identity protection features. Norton 360 further adds data backup services and PC tuning utilities.

McAfee takes a similar approach. McAfee Internet Security includes all of the features found in the less expensive McAfee AntiVirus Plus and adds parental controls, anti-spam measures and online backup. The more fully-featured McAfee Total Protection contains these elements plus the capability to block intruders to the home network and a web reputation system that blocks potentially dangerous websites (its other products warn, rather than block).

Trend Micro's Titanium Internet Security product adds further levels of protection to those provided by its Titanium AntiVirus+ program, including 'unauthorized change protection', which is designed to stop the computer's underlying operating system from being altered by malware. It also adds anti-spam, additional protection via the existing Windows firewall, parental controls and data theft protection. The Titanium Maximum Security product includes system optimization tools, a secure file deletion utility, Smartphone protection and backup services.

The same goes for many other vendors, which provide the same core anti-malware protection at the heart of each product and then add data safety features for an additional cost. The three main vendors mentioned above, plus BitDefender, G Data, Kaspersky, Panda and Webroot all share this approach. Avira's range is similar, except that its basic product is both free and lacking some protection features. These include the behavioral detection (AntiVirProActiv), web reputation (WebGuard) and anti-exploit (AntiDrive-by) systems that are found in Avira's paid-for products.

No total protection available?

F-Secure is one exception, providing online backup as a completely separate product to its Anti-Virus and Internet Security software. ESET's range includes NOD32 Antivirus and Smart Security, which is the equivalent of the internet security products available from other vendors (in terms of included features). We have included these products because they are the most fully-featured available from ESET and F-Secure.

Comparing products

In terms of malware protection there should be little or no difference between internet security and total protection programs within the same product range. This means that upgrading from one to another, using the same vendor, makes sense only if you want the extra features provided, such as extra backup capacity or new tools.

This is true for most of the vendors whose products we tested for this report, although there is a difference in protection levels between McAfee Internet Security 2011 and McAfee Total Protection 2011. The internet security version includes a web reputation system called Site Advisor, which produces a toolbar alert in the web browser when users visit a site that it classifies as being dangerous. The total protection version has a Protection Mode that will actually block this site and its potentially-malicious content, while the internet security version will only issue an alert. By default this mode is not enabled so the results here show what would happen if either product in their default state encountered the threats we used.

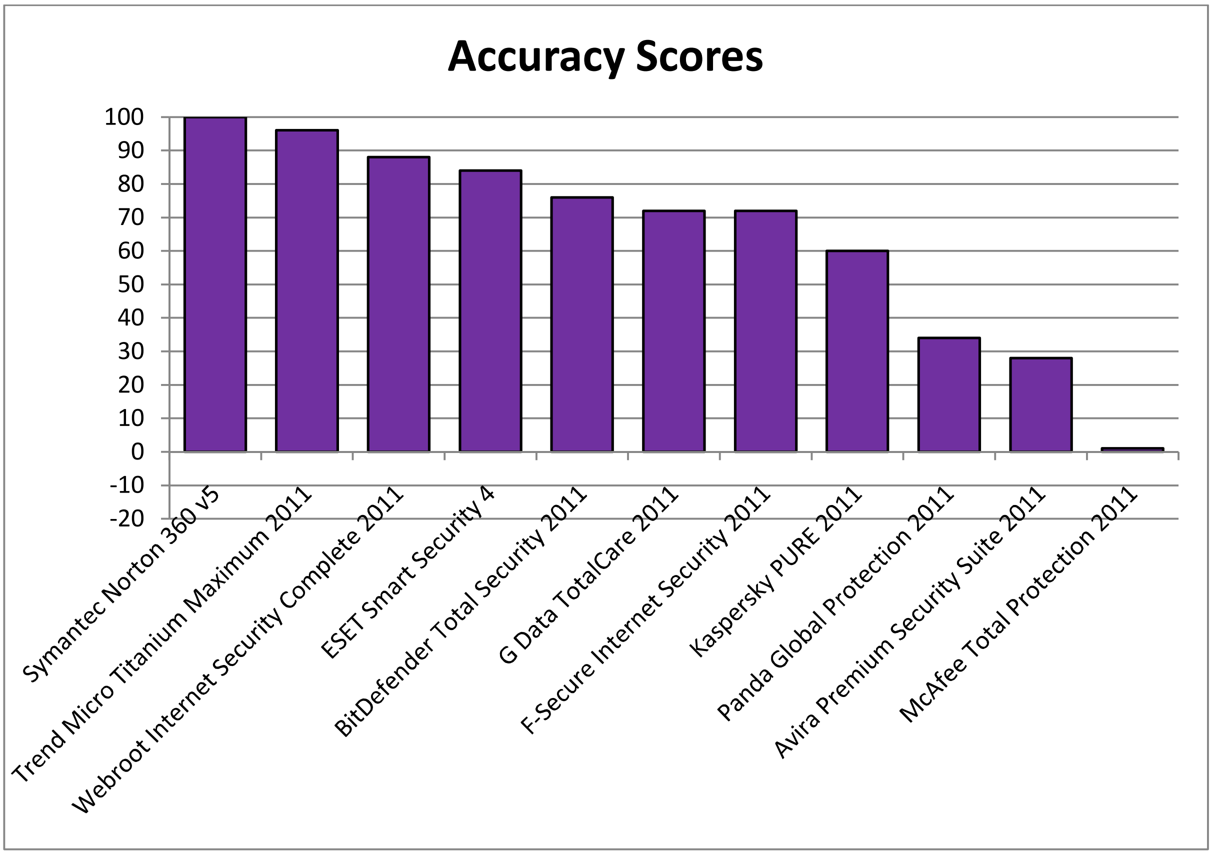
Contents

1. Overall Accuracy

Each product has been scored for accuracy. We have awarded two points for defending against a threat, one for neutralizing it and removed two points every time a product allowed the system to be compromised.

The reason behind this score weighting is to give credit to products that deny malware an opportunity to tamper with the system and to penalize those that allow malware to damage it. In some of our test cases a compromised system was made unusable, and in more than one case the pre-installed security software was disabled.

The graph below does not take false positives into account. See the Total Accuracy Scores graph and table below to see a combined set of results.



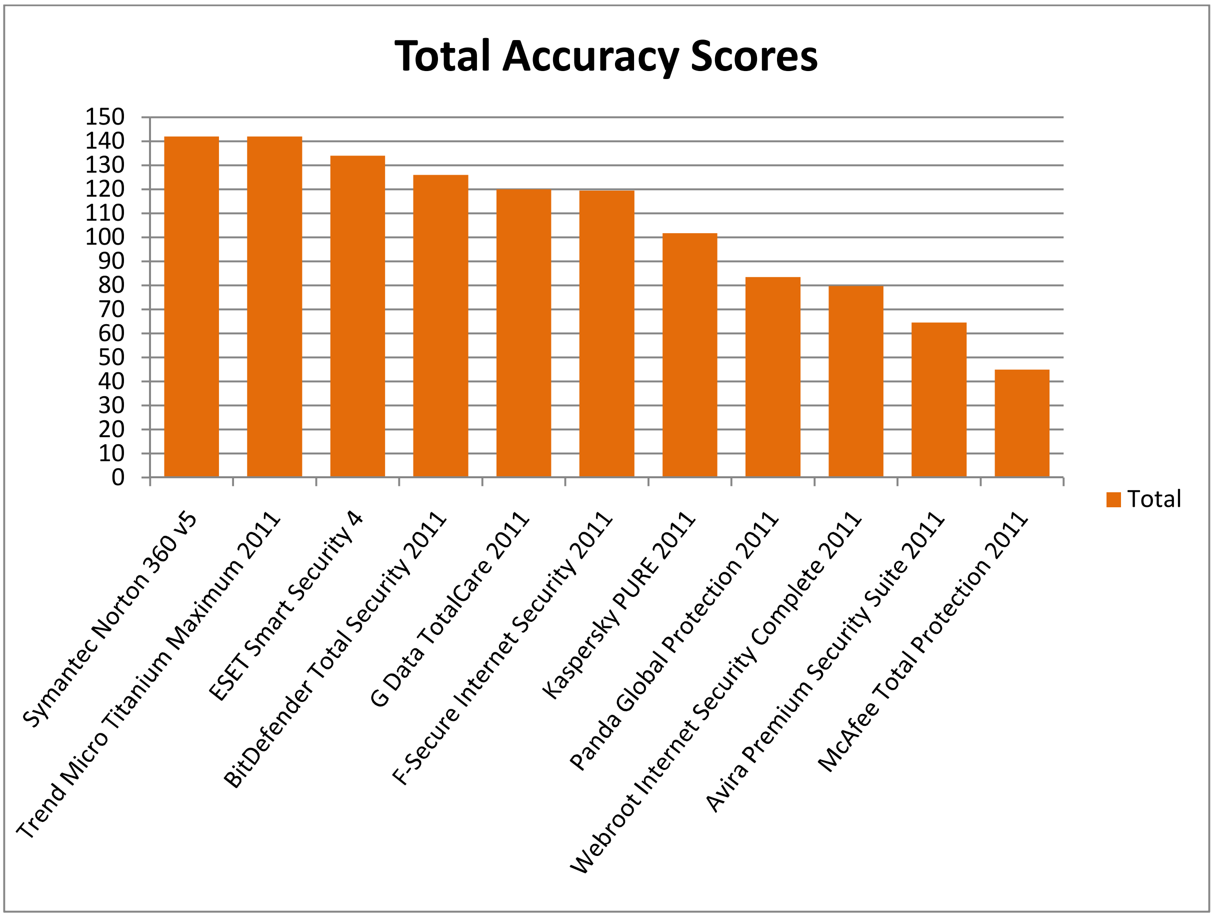
The Norton and Trend Micro products score highly as they generally defended the system against threats. Products from McAfee, Avira and Panda were compromised the most frequently and so their scores suffer accordingly.

ACCURACY SCORES

PRODUCT	DEFENDED	NEUTRALIZED	COMPROMISED	ACCURACY
Symantec Norton 360 v5	50	0	0	100
Trend Micro Titanium Maximum Security 2011	49	0	1	96
Webroot Internet Security Complete 2011	44	4	2	88
ESET Smart Security 4	46	0	4	84
BitDefender Total Security 2011	41	4	5	76
F-Secure Internet Security 2011	43	0	7	72
G Data TotalCare 2011	40	4	6	72
Kaspersky PURE 2011	40	0	10	60
Panda Global Protection 2011	29	6	15	34
Avira Premium Security Suite 2011	29	4	17	28
McAfee Total Protection 2011	20	7	23	1

The following results show a combined accuracy score, taking into account each product's performance with both threats and non-malicious software. There is a maximum possible score of 150 and a minimum of -350.

See **4. False positive incidents** for detailed results and **6.9 False positives** for an explanation on how the false positive accuracy scores are calculated.



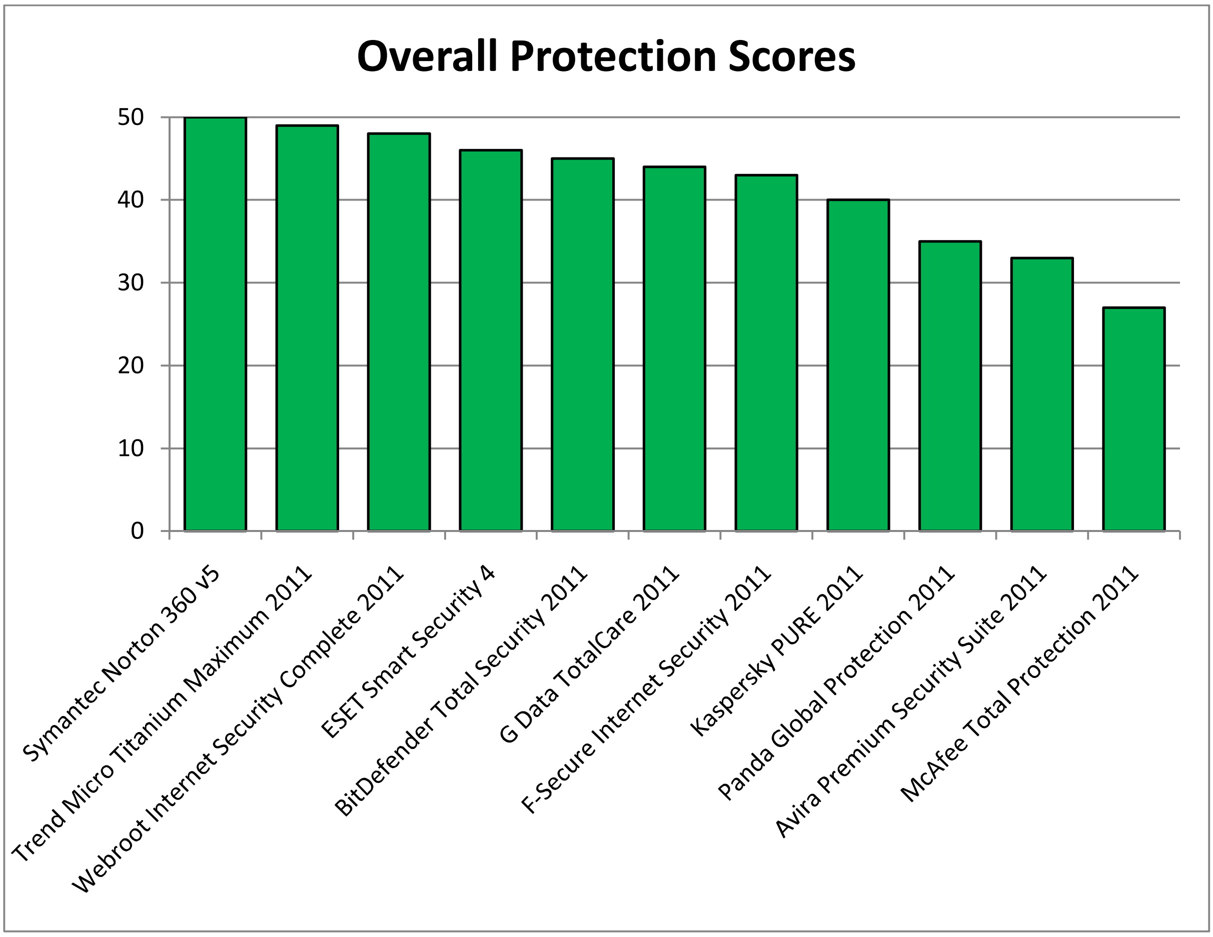
When false positives are taken into account Webroot's accuracy score slides from third position to ninth.

TOTAL ACCURACY SCORES

PRODUCT	THREAT ACCURACY	FALSE POSITIVE ACCURACY	TOTAL ACCURACY
Symantec Norton 360 v5	100	42	142
Trend Micro Titanium Maximum Security 2011	96	46	142
ESET Smart Security 4	84	50	134
BitDefender Total Security 2011	76	50	126
G Data TotalCare 2011	72	48	120
F-Secure Internet Security 2011	72	47.5	119.5
Kaspersky PURE 2011	60	41.75	101.75
Panda Global Protection 2011	34	49.5	83.5
Webroot Internet Security Complete 2011	88	-8.3	79.7
Avira Premium Security Suite 2011	28	36.5	64.5
McAfee Total Protection 2011	1	44	45

2. Overall Protection

The following illustrates the general level of protection provided by each of the security products, combining the defended and neutralized incidents into an overall figure. This figure is not weighted with an arbitrary scoring system as it was in **1. Overall accuracy**.



Even without weighted scores to help differentiate performance, the top three products are clearly in a separate league to the others. The Kaspersky, Panda, Avira and McAfee products were awarded protection ratings below the average of this group.

OVERALL PROTECTION SCORES

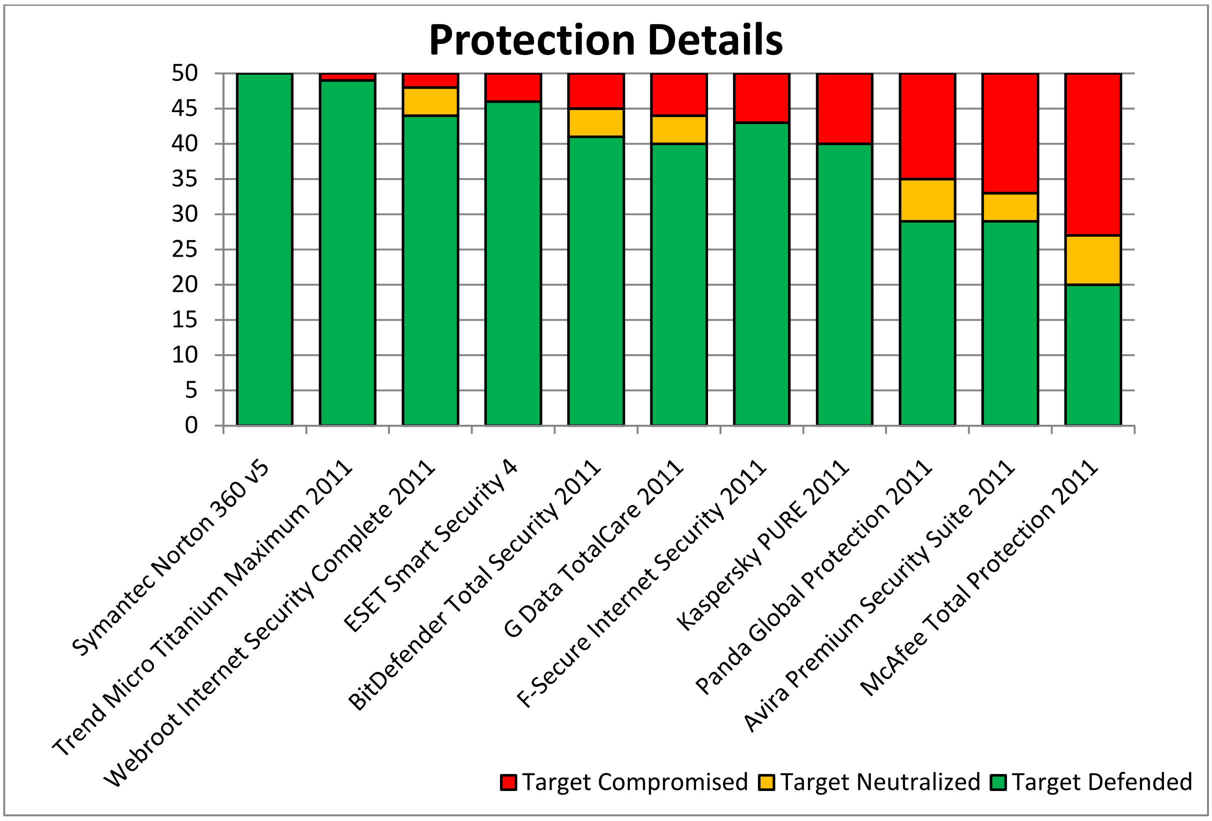
PRODUCT	COMBINED PROTECTION SCORE	PERCENTAGE
Symantec Norton 360 v5	50	100%
Trend Micro Titanium Maximum Security 2011	49	98%
Webroot Internet Security Complete 2011	48	96%
ESET Smart Security 4	46	92%
BitDefender Total Security 2011	45	90%
G Data TotalCare 2011	44	88%
F-Secure Internet Security 2011	43	86%
Kaspersky PURE 2011	40	80%
Panda Global Protection 2011	35	70%
Avira Premium Security Suite 2011	33	66%
McAfee Total Protection 2011	27	54%

(Average: 84 per cent)

3. Protection Details

The security products provided different levels of protection. When a product **defended** against a threat, it prevented the malware from gaining a foothold on the target system. A threat might have been able to infect the system and, in some cases, the product **neutralized** it later. When it couldn't, the system was **compromised**.

The graph below shows that the most two successful products defended rather than neutralized the threats.



Symantec's Norton 360, Trend Micro Titanium Maximum and Webroot Internet Security provided the most effective protection.

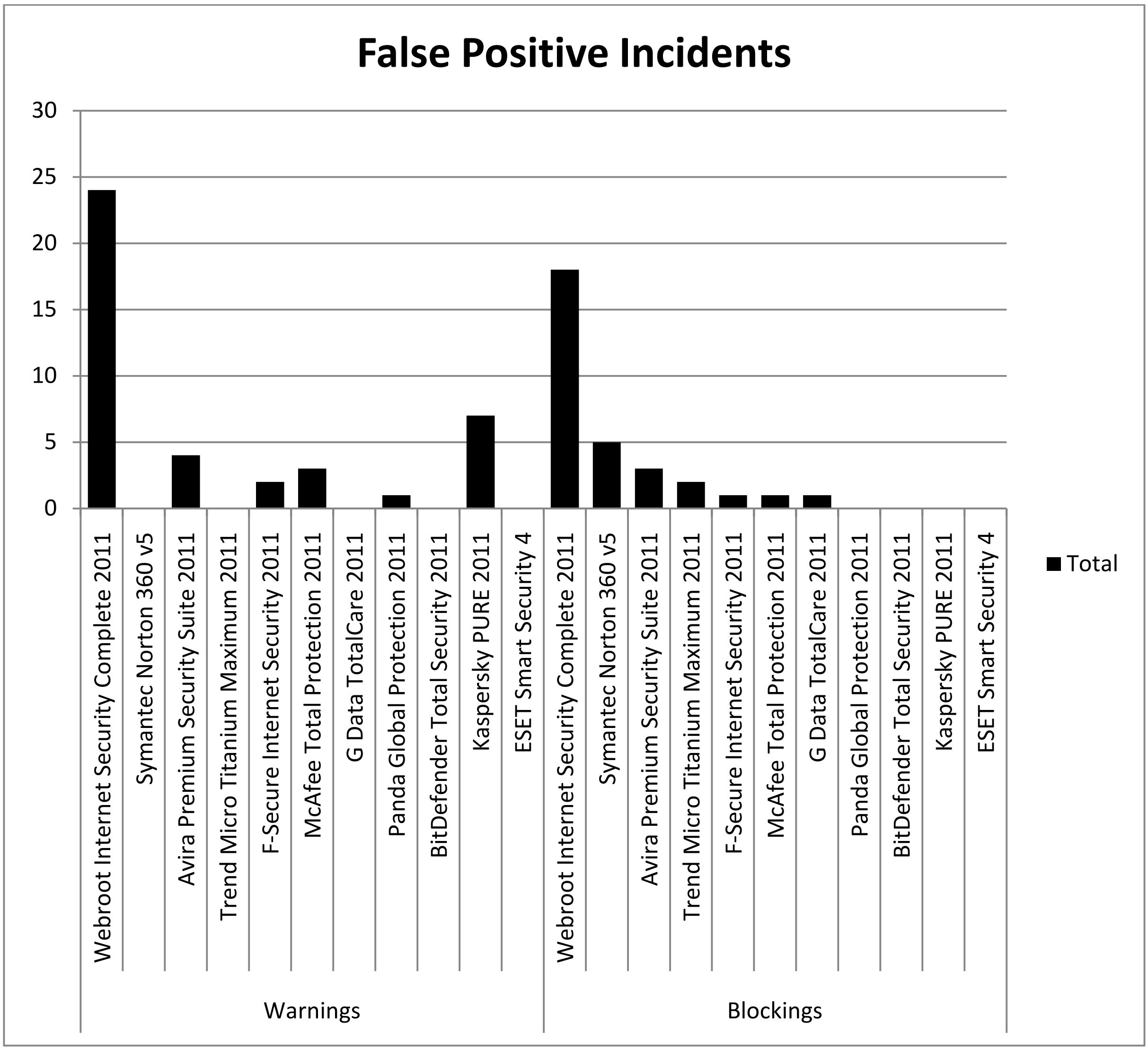
PROTECTION DETAILS

PRODUCT	DEFENDED	NEUTRALIZED	COMPROMISED
Symantec Norton 360 v5	50	0	0
Trend Micro Titanium Maximum Security 2011	49	0	1
ESET Smart Security 4	46	0	4
Webroot Internet Security Complete 2011	44	4	2
F-Secure Internet Security 2011	43	0	7
BitDefender Total Security 2011	41	4	5
G Data TotalCare 2011	40	4	6
Kaspersky PURE 2011	40	0	10
Avira Premium Security Suite 2011	29	4	17
Panda Global Protection 2011	29	6	15
McAfee Total Protection 2011	20	7	23

4. False Positive Incidents

A security product needs to be able to protect the system from threats, while allowing legitimate software to work properly. When legitimate software is misclassified a **false positive** is generated. We split the results into two main groups, as the products all took one of two approaches when attempting to protect the system from the legitimate programs. They either warned that the software was suspicious or took the more decisive step of blocking it.

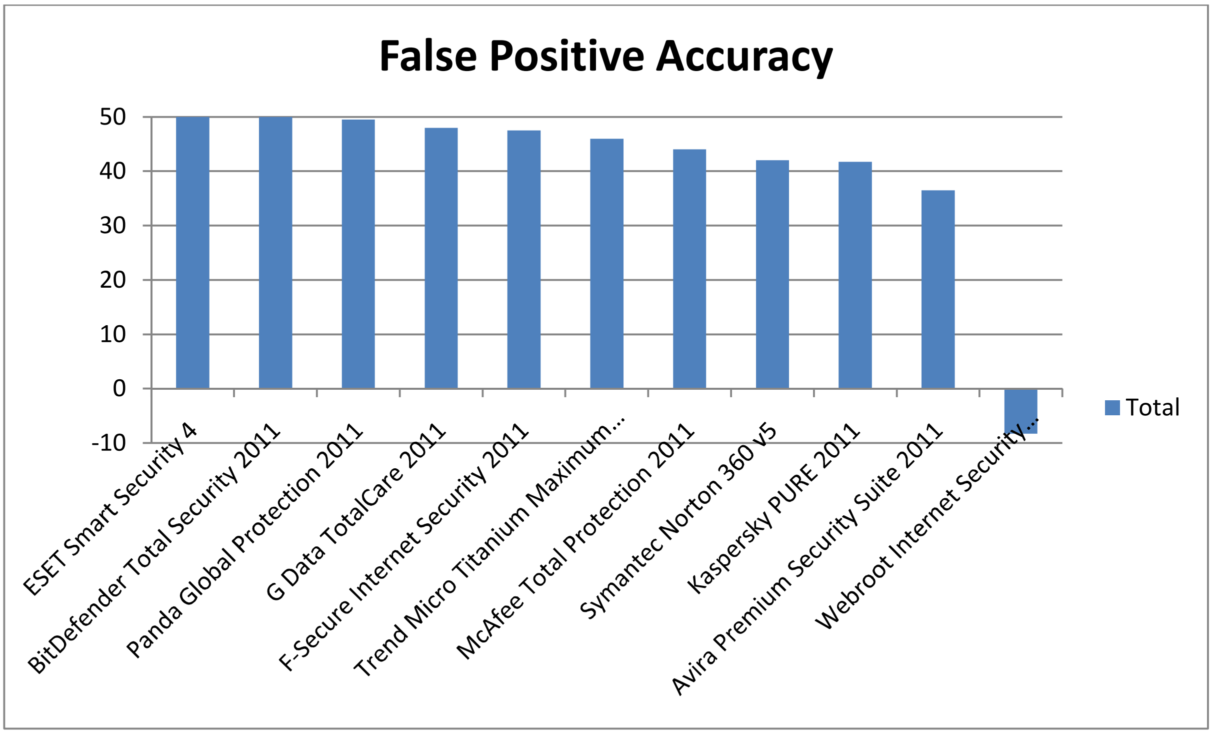
The graph below includes the products that generated false positives. All but two products generated false positives. BitDefender and ESET were the notable exceptions. Webroot's product produced by far the largest number of false positives, alerting the user or blocking the software in the vast majority of cases.



BitDefender and ESET neither warned nor blocked the legitimate software, but all of the other programs tested made errors. Webroot Internet Security Complete 2011 was the least accurate.

FALSE POSITIVE INCIDENTS

PRODUCT	THREAT WARNING	PRODUCT BLOCKED
Webroot Internet Security Complete 2011	24	18
Symantec Norton 360 v5	0	5
Avira Premium Security Suite 2011	4	3
Trend Micro Titanium Maximum Security 2011	0	2
G Data TotalCare 2011	0	1
McAfee Total Protection 2011	3	1
F-Secure Internet Security 2011	2	1
Kaspersky PURE 2011	7	0
Panda Global Protection 2011	1	0
ESET Smart Security 4	0	0
BitDefender Total Security 2011	0	0



FALSE POSITIVE ACCURACY SCORES

ESET Smart Security 4	50
BitDefender Total Security 2011	50
Panda Global Protection 2011	49.5
G Data TotalCare 2011	48
F-Secure Internet Security 2011	47.5
Trend Micro Titanium Maximum Security 2011	46
McAfee Total Protection 2011	44
Symantec Norton 360 v5	42
Kaspersky PURE 2011	41.75
Avira Premium Security Suite 2011	36.5
Webroot Internet Security Complete 2011	-8.3

To learn how these scores were calculated please see **6.9. False Positives**.

5. The Tests

5.1 The threats

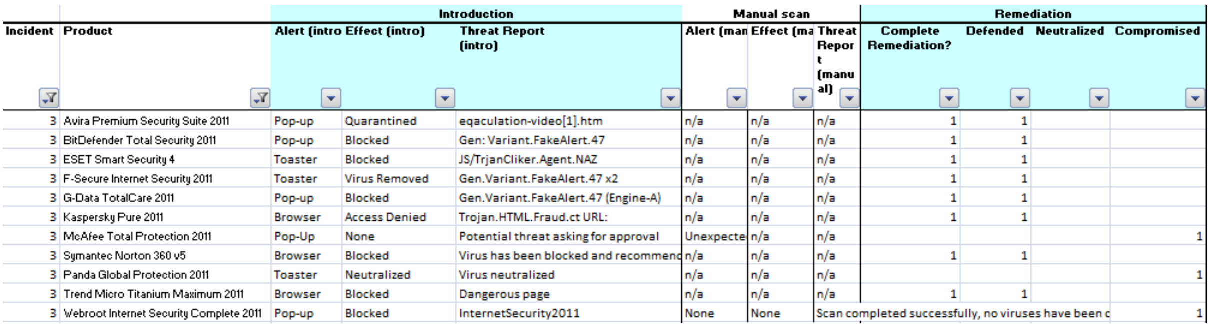
Providing a realistic user experience was important in order to illustrate what really happens when a user encounters a threat on the internet. For example, in these tests web-based malware was accessed by visiting an original, infected website using a web browser, and not downloaded from a CD or an internal test website.

All target systems were fully exposed to the threats. This means that malicious files were run and allowed to perform as they were designed, subject to checks by the installed security software. A minimum time period of five minutes was provided to allow the malware an opportunity to act.

5.2 Test rounds

Tests were conducted in rounds. Each round recorded the exposure of every product to a specific threat. For example, in 'round one' each of the products was exposed to the same malicious website.

At the end of each round the test systems were completely reset to remove any possible trace of malware before the next test began.



		Introduction			Manual scan			Remediation			
Incident	Product	Alert (intro	Effect (intro)	Threat Report (intro)	Alert (man	Effect (ma	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
3	Avira Premium Security Suite 2011	Pop-up	Quarantined	eqaculation-video[1].htm	n/a	n/a	n/a	1	1		
3	BitDefender Total Security 2011	Pop-up	Blocked	Gen: Variant.FakeAlert.47	n/a	n/a	n/a	1	1		
3	ESET Smart Security 4	Toaster	Blocked	JS/TrjanCliker.Agent.NAZ	n/a	n/a	n/a	1	1		
3	F-Secure Internet Security 2011	Toaster	Virus Removed	Gen.Variant.FakeAlert.47 x2	n/a	n/a	n/a	1	1		
3	G-Data TotalCare 2011	Pop-up	Blocked	Gen.Variant.FakeAlert.47 (Engine-A)	n/a	n/a	n/a	1	1		
3	Kaspersky Pure 2011	Browser	Access Denied	Trojan.HTML.Fraud.ct URL:	n/a	n/a	n/a	1	1		
3	McAfee Total Protection 2011	Pop-Up	None	Potential threat asking for approval	Unexpecte	n/a	n/a				1
3	Symantec Norton 360 v5	Browser	Blocked	Virus has been blocked and recommend	n/a	n/a	n/a	1	1		
3	Panda Global Protection 2011	Toaster	Neutralized	Virus neutralized	n/a	n/a	n/a				1
3	Trend Micro Titanium Maximum 2011	Browser	Blocked	Dangerous page	n/a	n/a	n/a	1	1		
3	Webroot Internet Security Complete 2011	Pop-up	Blocked	InternetSecurity2011	None	None	Scan completed successfully, no viruses have been c				1

Each 'round' exposed every product to one specific threat. The set of records for round three (above) shows a range of responses to a particular threat.

In the example above Kaspersky PURE, Norton 360 and Trend Micro Titanium Maximum Security all blocked the threat at the browser ('Browser'), before it could cause any harm. ESET and F-Secure popped up temporary 'Toaster' alerts to confirm that the malware had been dealt with, while Avira and BitDefender used Pop-Up alerts, which required the user to perform an action, such as clicking 'Quarantine' or 'Block'.

Despite offering warnings, the McAfee, Panda and Webroot programs allowed the system to become compromised. The malware actually disabled the real-time and on-demand scanning capabilities of both the McAfee and Panda products.

5.3 Monitoring

Close logging of the target systems was necessary to gauge the relative successes of the malware and the anti-malware software. This included recording activity such as network traffic, the creation of files and processes and changes made to important files.

5.4 Levels of protection

The products displayed different levels of protection. Sometimes a product would prevent a threat from executing, or at least making any significant changes to the target system. In other cases a threat would perform some tasks on the target, after which the security product would intervene and remove some or all of the malware. Finally, a threat may have been able to bypass the security product and carry out its malicious tasks unhindered. It may even have been able to disable the security software. Occasionally Windows' own protection system might handle a threat, while the anti-virus program can ignore it. Another outcome is that the malware may crash for various reasons. The different levels of protection provided by each product were recorded following analysis of the log files.

5.5 Types of protection

All of the products tested provided two main types of protection: real-time and on-demand. Real-time protection monitors the system constantly in an attempt to prevent a threat from gaining access. On-demand protection is essentially a ‘virus scan’ that is run by the user at an arbitrary time.

The test results note each product’s behavior when a threat is introduced and afterwards. The real-time protection mechanism was monitored throughout the test, while an on-demand scan was run towards the end of each test to measure how safe the product determined the system to be.

6. Test Details

6.1 The targets

To create a fair testing environment, each product was installed on a clean Windows XP Professional target system (Target Client System - TCS). The operating system was updated with Windows XP Service Pack 3 (SP3) and Internet Explorer 7, although no later patches or updates were applied. The high prevalence of internet threats that rely on Internet Explorer 7, and other vulnerable Windows components that have been updated since SP3 was released, suggest that there are many systems with this level of patching currently connected to the internet. We used this level of patching to remain as realistic as possible. Windows Automatic Updates was disabled.

A selection of legitimate but old software was pre-installed on the target systems. These posed security risks, as they contained known vulnerabilities. They included out of date versions of Adobe Flash Player and Adobe Reader.

A different security product was then installed on each system. Each product's update mechanism was used to download the latest version with the most recent definitions and other elements. Due to the dynamic nature of the tests, which are carried out in real-time with live malicious websites, the products' update systems were allowed to run automatically and were also run manually before each test round was carried out. The products were also allowed to 'call home' should they be programmed to query databases in real-time. At any given time of testing, the very latest version of each program was used.

Each target system contained identical hardware, including an Intel Core 2 Duo processor, 1GB RAM, a 160GB hard disk and a DVD-ROM drive. Each was connected to the internet via its own virtual network (VLAN) to avoid malware cross-infecting other targets.

6.2 Threat selection

The malicious web links (URLs) used in the tests were picked from lists generated by Dennis Technology Labs' own malicious site detection system, which uses popular search engine keywords submitted to Google. It analyses sites that are returned in the search results from a number of search engines and adds them to a database of potentially malicious websites. In all cases, a control system (Verification Target System - VTS) was used to confirm that the URLs linked to actively malicious sites. The VTSes were loaded with exactly the same software as the Target Client Systems, although they were not equipped with anti-malware software.

Malicious URLs and files were not shared with any vendors during the testing process.

6.3 Test stages

There were three main stages in each individual test:

1. Introduction
2. Observation
3. Remediation

During the *Introduction* stage, the target system was exposed to a threat. Before the threat was introduced, a snapshot was taken of the system. This created a list of Registry entries and files on the hard disk. We used Regshot (see **Appendix D: Tools**) to take and compare system snapshots. The threat was then introduced.

Immediately after the system's exposure to the threat, the *Observation* stage is reached. During this time, which typically lasted at least 10 minutes, the tester monitored the system both visually and using a range of third-party tools. The tester reacted to pop-ups and other prompts according to the directives described below (**see 6.6 Observation and intervention**).

In the event that hostile activity to other internet users was observed, such as when spam was being sent by the target, this stage was cut short. The *Observation* stage concluded with another system snapshot. This 'exposed' snapshot was compared to the original 'clean' snapshot and a report was generated. The system was then rebooted.

The *Remediation* stage is designed to test the products' ability to clean an infected system. If it defended against the threat in the *Observation* stage then there should be few (if any) legitimate alerts during this procedure. An on-demand scan was run on the target, after which a 'scanned' snapshot was taken. This was compared to the original 'clean' snapshot and a report was generated. All log files, including the snapshot reports and the product's own log files, were recovered from the target. The target was then reset to a clean state, ready for the next test.

6.4 Threat introduction

Malicious websites were visited in real-time using Internet Explorer. This risky behavior was conducted using live internet connections. URLs were typed manually into Internet Explorer's address bar.

Web-hosted malware often changes over time. Visiting the same site over a short period of time can expose systems to what appears to be a range of threats (although it may be the same threat, slightly altered to avoid detection). In order to improve the chances that each target system received the same experience from a malicious web server, we used a web replay system.

Many infected sites will only attack a particular IP address once, which makes it hard to test more than one product. We used an HTTP session replay system to counter this problem. It provides a close simulation of a live internet connection and allows each product to experience the same threat. Configurations were set to allow all products unfettered access to the internet.

6.5 Secondary downloads

Established malware may attempt to download further files (secondary downloads), which may be stored by the replay system and re-served to other targets in some circumstances. These circumstances include cases where:

1. The download request is made using HTTP (e.g. http://badsite.example.com/...) and
2. The same filename is requested each time (e.g. badfile1.exe)

There are scenarios where target systems will receive different secondary downloads. These include cases where:

1. The download request is made using a protocol not normally used in web transactions or
2. A different filename is requested each time (e.g. badfile2.exe; random357.exe)

6.6 Observation and intervention

Throughout each test, the target system was observed both manually and in real-time. This enabled the tester to take comprehensive notes about the system's perceived behavior, as well as to compare visual alerts with the products' log entries. At certain stages the tester was required to act as a regular user. To achieve consistency, the tester followed a policy for handling certain situations, including dealing with pop-ups displayed by products or the operating system, system crashes, invitations by malware to perform tasks and so on.

This user behavior policy includes the following directives:

1. Act naively. Allow the threat a good chance to introduce itself to the target by clicking OK to malicious prompts, for example.
2. Don't be too stubborn in retrying blocked downloads. If a product warns against visiting a site, don't take further measures to visit that site.
3. Where malware is downloaded as a Zip file, or similar, extract it to the Desktop then attempt to run it. If the archive is protected by a password, and that password is known to you (e.g. it was included in the body of the original malicious email), use it.
4. Always click the default option. This applies to security product pop-ups, operating system prompts (including Windows firewall) and malware invitations to act.
5. If there is no default option, wait. Give the prompt 20 seconds to choose a course of action automatically.
6. If no action is taken automatically, choose the first option. Where options are listed vertically, choose the top one. Where options are listed horizontally, choose the left-hand one.

6.7 Remediation

When a target is exposed to malware, the threat may have a number of opportunities to infect the system. The security product also has a number of chances to protect the target. The snapshots explained in **6.3 Test stages** provided information that was used to analyze a system's final state at the end of a test.

Before, during and after each test, a 'snapshot' of the target system was taken to provide information about what had changed during the exposure to malware. For example, comparing a snapshot taken before a malicious website was visited to one taken after might highlight new entries in the Registry and new files on the hard disk. Snapshots were also used to determine how effective a product was at removing a threat that had managed to establish itself on the target system. This analysis gives an indication as to the levels of protection that a product has provided.

These levels of protection were recorded using three main terms: defended, neutralized, and compromised. A threat that was unable to gain a foothold on the target was *defended* against; one that was prevented from continuing its activities was *neutralized*; while a successful threat was considered to have *compromised* the target.

A defended incident occurs where no malicious activity is observed with the naked eye or third-party monitoring tools following the initial threat introduction. The snapshot report files are used to verify this happy state.

If a threat is observed to run actively on the system, but not beyond the point where an on-demand scan is run, it is considered to have been neutralized. Comparing the snapshot reports should show that malicious files were created and Registry entries were made after the introduction. However, as long as the 'scanned' snapshot report shows that either the files have been removed or the Registry entries have been deleted, the threat has been neutralized.

The target is compromised if malware is observed to run after the on-demand scan. In some cases a product will request a further scan to complete the removal. For this test we considered that secondary scans were acceptable, but further scan requests would be ignored. Even if no malware was observed, a compromise result was recorded if snapshot reports showed the existence of new, presumably malicious files on the hard disk, in conjunction with Registry entries designed to run at least one of these files when the system booted. An edited 'hosts' file or altered system file also counted as a compromise.

6.8 Automatic monitoring

Logs were generated using third-party applications, as well as by the security products themselves. Manual observation of the target system throughout its exposure to malware (and legitimate applications) provided more information about the security products' behavior. Monitoring was performed directly on the target system and on the network.

Client-side logging

A combination of Process Explorer, Process Monitor, TcpView and Wireshark were used to monitor the target systems. Regshot was used between each testing stage to record a system snapshot. A number of Dennis

Technology Labs-created scripts were also used to provide additional system information. Each product was usually able to generate some level of logging itself.

Process Explorer and TcpView were run throughout the tests, providing a visual cue to the tester about possible malicious activity on the system. In addition, Wireshark's real-time output, and the display from a web proxy (see Network logging, below), indicated specific network activity such as secondary downloads.

Process Monitor also provided valuable information to help reconstruct malicious incidents. Both Process Monitor and Wireshark were configured to save their logs automatically to a file. This reduced data loss when malware caused a target to crash or reboot.

In-built Windows commands such as 'systeminfo' and 'sc query' were used in custom scripts to provide additional snapshots of the running system's state.

Network logging

All target systems were connected to a live internet connection, which incorporated a transparent web proxy and network monitoring system. All traffic to and from the internet had to pass through this system. This allowed the testers to capture files containing the complete network traffic. It also provided a quick and easy view of web-based traffic, which was displayed to the tester in real-time.

The network monitor was a dual-homed Linux system running as a bridge, passing all web traffic through a transparent Squid proxy.

An HTTP replay system ensured that all target systems received the same malware as each other. It was configured to allow access to the internet so that products could download updates and communicate with any available 'in the cloud' servers.

6.9 False positives

A useful security product is able to block threats and allow useful program to install and run. The products were tested to see how they would respond to the download and installation of legitimate applications.

The prevalence of each installation file is significant. If a product misclassified a common file then the situation would be more serious than if it failed to permit a less common one. That said, it is fair for users to expect that anti-malware programs should not misclassify any legitimate software.

The files selected for the false positive testing were organized into five groups: Very High Impact, High Impact, Medium Impact, Low Impact and Very Low Impact. These categories were based on download numbers for the previous week, as reported by Download.com at the time of testing. The ranges for these categories are recorded in the table below:

PREVALENCE CATEGORIES

CATEGORY	PREVALENCE
Very High Impact	>20,001 downloads
High Impact	>999 downloads
Medium Impact	>99 downloads
Low Impact	>24 downloads
Very Low Impact	<25 downloads

(Figures published by Download.com at time of testing)

In the false positive accuracy tests a product scored one full point when it neither warned nor blocked the legitimate application. If it warned against running or installing it then it lost points. It lost twice as many points if it blocked the software.

The actual number of points (or fraction of a point) lost depended on how prevalent the file was. For example, if a security product blocked a Very High Impact program (such as the DivX installer, which Download.com claims was downloaded 69,465 times in the previous week) then it would lose five points. If it only warned against it then it would lose 2.5 points. If it blocked a much less common program, such as Wordsearch Solver (23 downloads in the previous week) then it would lose only 0.1 points. A warning would modify the product's score by just -0.05 points.

The score modifiers are as follows:

FIXED SCORING MODIFIERS

Blocked	Very High Impact	-5
	High Impact	-2
	Medium Impact	-1
	Low Impact	-0.5
	Very Low Impact	-0.1
Warning	Very High Impact	-2.5
	High Impact	-1
	Medium Impact	-0.5
	Low Impact	-0.25
	Very Low Impact	-0.05

The test included 50 legitimate applications. This means that the maximum possible score is 50 and the lowest possible score is -250.

7. Conclusions

How well did the products protect the systems?
The best-performing products, in both the malware and non-malicious tests, were Symantec Norton 360 v5, Trend Micro Titanium Maximum Security 2011 and ESET Smart Security 4. The same results apply to Norton Internet Security 2011 and Trend Micro Titanium Internet Security 2011.

The least effective products were Webroot Internet Security Complete 2011, Avira Premium Security Suite 2011 and McAfee Total Protection 2011. Webroot's product would have been the third best, beating ESET Smart Security 4, had it not performed so poorly in the false positive tests.

Where are the threats?
The threats used in this test were genuine, real-life threats that were infecting victims globally at the same time as we tested the products. In almost every case the threat was launched via a legitimate website that had been compromised by an attacker.

The most common type of threat that our malicious site detection system identified was the fake security application. We also saw a new variation of this theme involving fake hard disk utilities that claim to identify problems with the target PC's disk. In the same way as fake security products attempt to trick victims into paying for a full license (thus accessing 'protection' from the perceived threat), so the fake disk utilities try to con people into paying for a solution to a non-existent problem with the integrity of their hard disks.

The fake hard disk utilities were one of the first threats that appeared in this test, which started in mid- December 2010. This was just a few weeks after this type of threat first appeared on the internet in significant numbers[1], demonstrating that the threats used in the test were up to date and reflected what many end users were experiencing online at the same time.

These threats tended to require the user to click on a fake Remove All button or similar. However, the test also encountered some automatic (drive-by) infections too. In many cases these exploited the Windows Help and Support Center vulnerability (Help Center URL Validation Vulnerability – CVE-2010-1885). An update that fixes this problem is available from Microsoft's Automatic Update system.

Anti-virus is important (but not a panacea)
This test shows that there is a significant difference in protection performance between popular anti-virus programs. Most importantly it illustrates this difference using real threats that were attacking real computers at the time of testing.

Customers of anti-virus products would do well to note that in our results the average protection level is 84 per cent (**see 2. Overall protection**). Marketing claims implying or stating that a product protects against all known and unknown threats should clearly be treated with skepticism. Our results also contradict other third-party tests that claim the majority of desktop products are capable of detecting 100 per cent of malware.

The fact that most products tested here mistrusted at least a few legitimate applications also shows that we are not yet in a world where security software can sit quietly in the background and provide seamless protection without asking the user questions. Unfortunately users are not necessarily equipped to make the right choices. This statement is borne out by the fact that the fake anti-virus programs encountered in our test generally relied on tricking a victim into clicking a button. This strategy clearly works, otherwise the attackers would adopt a different approach.

[1] Beware of the New Fake Hard Disk Utility Scareware – Baracuda Labs, 10th December 2010 (www.barracudalabs.com/wordpress/index.php/2010/12/10/beware-of-the-new-fake-hard-disk-utility-scareware/)

Fake Disk Cleanup Utilities: The Ruse – Symantec, 30th November 2010 (www.symantec.com/connect/blogs/fake-disk-cleanup-utilities-ruse)

The drive-by threats witnessed in this test relied on the victim's PC running out of date software, such as old versions of Adobe Reader and Java. Updates to these programs, and to Windows itself, are available and would have rendered some, if not all, of the threats useless. It makes a great deal of sense to apply updates (which are almost always available for free) rather than relying solely on security software to catch the malware.

Appendix A: Technical Terms

Compromised	Malware continues to run on an infected system, even after an on-demand scan.
Defended	Malware was prevented from running on, or making changes to, the target.
False Positive	A legitimate application was incorrectly classified as being malicious.
Introduction	Test stage where a target system is exposed to a threat.
Neutralized	Malware was able to run on the target, but was then removed by the security product.
Observation	Test stage during which malware may affect the target.
On-demand (protection)	Manual 'virus' scan, run by the user at an arbitrary time.
Prompt	Questions asked by software, including malware, security products and the operating system. With security products, prompts usually appear in the form of pop-up windows. Some prompts don't ask questions but provide alerts. When these appear and disappear without a user's interaction, they are called 'toasters'.
Real-time (protection)	The 'always-on' protection offered by many security products.
Remediation	Test stage that measures a product's abilities to remove any installed threat.
Round	Test series of multiple products, exposing each target to the same threat.
Snapshot	Record of a target's file system and Registry contents.
Target	Test system exposed to threats in order to monitor the behavior of security products.
Threat	A program or other measure designed to subvert a system.
Update	Code provided by a vendor to keep its software up to date. This includes virus definitions, engine updates and operating system patches.

APPENDIX B: LEGITIMATE SAMPLES

Incident	Product	Program type	Obtained via
1	Ares Galaxy	Share any digital file.	Download.com
2	Advanced SystemCare Free	Repair Registry, tune-up, and maintain the computer system performance.	Download.com
3	Virtual DJ	Mix, scratch, and remix MP3 or music videos live.	Download.com
4	Smart-Cam CMM	Perform accurate, calibrated measurements from live video, still photos, or image files.	Download.com
5	GOM Media Player	Play video files of multiple video formats.	Download.com
6	FreeZ Online TV	Receive over 500+ free online channels of daily and live broadcasts.	Download.com
7	MyVideoConverter	Convert video files to various formats and extract audio tracks.	Download.com
8	mIRC	Chat with other people and participate in group discussions.	Download.com
9	Free YouTube Downloader	Take and convert videos from YouTube into multiple formats.	Download.com
10	PowerISO	Create, edit, and encrypt CD/DVD image files.	Download.com
11	Outlook Express Backup	Protect Outlook Express as well as your Favorites and your Windows Address Book	Download.com
12	Auslogics Emergency Recovery	Recover deleted documents, pictures, and other important files.	Download.com
13	GoodSync	Back up and synchronize your important files automatically.	Download.com
14	FileSync	Keep your Desktop and your Notebook computer up-to-date and in sync with this simple program.	Download.com
15	Unblock Facebook Proxy	Browse Facebook via a secure proxy connection.	Download.com
16	GetRight	Resume, schedule, and manage your downloads.	Download.com

17	SpeedConnect XP Internet Accelerator	Surf faster with an optimized Internet connection.	Download.com
18	Loki VPN Client	Surf the Internet and hide your IP address.	Download.com
19	VisualRoute 2010	Analyze Internet connection problems and locate IPs.	Download.com
20	Easy Diary	Write your memories or appointments with ease.	Download.com
21	Read My Mind	Get a tool that knows what you are thinking.	Download.com
22	Sure Cuts A Lot for Windows	Cut your True Type fonts and various shapes.	Download.com
23	FlyAKite	Input, edit, and update kite-flying data and save it as a log file.	Download.com
24	KScan 9 - Virtual Desktop Scanner	Stream SSB or HAM radio online.	Download.com
25	Wordsearch Solver	Search for words in a puzzle.	Download.com
26	Web CEO Free Edition	Optimize your Web site for top search engine rankings.	Download.com
27	WebSite X5 Evolution	Create professional Web sites, blogs, and online shops without prior programming skills.	Download.com
28	MagicDisc	Create and manage virtual CD drives and CD/DVD discs.	Download.com
29	Any Video Converter	Convert video files between popular formats.	Download.com
30	FreeRAM XP Pro	Increase your system performance by cleaning the content of your RAM.	Download.com
31	MemoriesOnTV	Create a DVD or a VCD from your digital photos	Download.com
32	File Scavenger Data Recovery Utility	Recover files that have been accidentally deleted or are lost due to disk corruption.	Download.com
33	Wise Disk Cleaner Free	Remove junk files from your system and free up disk space, defrag, and optimize your hard drives.	Download.com
34	Active@ ISO Burner	Burn an ISO image file to CD-R, DVD-R, DVD+R, CD-RW, DVD-RW, and DVD+RW.	Download.com

35	BitLord	Distribute and download files via Torrent P2P protocol.	Download.com
36	CompuApps SwissKnife V3	Create, format, and delete your IDE hard disk drives.	Download.com
37	ToniArts EasyCleaner	Clean your Windows Registry from orphaned entries.	Download.com
38	Apple QuickTime 7	Play MPEG-4 movies with AAC sound with latest version of Apple's premier media player	http://www.apple.com/quicktime/download/
39	History Sweeper	Protect your privacy by erasing the tracks of your offline and online activities	Download.com
40	Sync2 for Outlook	Sync Microsoft Outlook folders between PCs, share Outlook, sync Google Calendar and Gmail Contacts.	Download.com
41	Fantastic Flame Screensaver	Put a realistic flame effect on your desktop.	Download.com
42	Matrix Code Emulator Screensaver	Display the animated green Matrix code you see on dozer's screen in the movie	Download.com
43	CaptureWizPro	Capture or record everything on your PC	Download.com
44	FastStone Capture	Capture anything on your PC screen	Download.com
45	3CXPhone	Use a VoIP softphone / IP phone for Windows that works with VoIP providers, IP PBX / SIP servers.	Download.com
46	Direct MIDI to MP3 Converter	Convert MIDI files to MP3, WMA, OGG, and WAV format.	Download.com
47	Power Tab Editor	Create, play, and print tablature scores.	Download.com
48	Cool Timer	Set countdown timer, and play WAV or MP3 files with it.	Download.com
49	DivX Plus Software	Install everything you need to play and create DivX, AVI, and MKV videos.	Download.com
50	Picasa	Organize, edit, and share pictures with this free photo manager.	Download.com

APPENDIX C: THREAT REPORT

Code	Product	Code	Product	Code	Product
AVI	Avira Premium Security Suite 2011	GTC	G Data TotalCare 2011	N360	Symantec Norton 360 v5
BDF	BitDefender Total Security 2011	KPU	Kaspersky PURE 2011	TTM	Trend Micro Titanium Maximum Security 2011
ESS	ESET Smart Security 4	MTP	McAfee Internet Security 2011	WBR	Webroot Internet Security Complete 2011
FIS	F-Secure Internet Security 2011	PIS	Panda Internet Security 2011		

NOTE: The following table is a summary. The full report was provided to Symantec as an Excel spreadsheet, which includes any Notes referred to in some Threat Report entries.

Products may react against threats, logging the action without producing an alert. Such results show 'None' in the Alert records but the product still Defended or Neutralized.

There are a total of 50 malicious incidents in this test but the identifying numbers may not run as expected. Some incidents were removed due to duplicated domain names. This is why the sequence runs: 1, 3, 4-5, 7 and so on. In this example, incidents #2 and #6 were removed because they used domain names already represented in the test.

Incident	Product	Introduction			Silent log	Manual Scan			Complete Remediation	Defended	Neutralized	Compromised
		Alert	Effect	Threat Report		Alert	Effect	Threat Report				
1	AVI	Toaster	Access Denied	Fake AV userinit.exe	0	n/a	n/a	n/a				1
1	BDF	Toaster	Deleted	Gen.Variant.FakeAlert.47 x9	0	n/a	n/a	n/a	1	1		
1	ESS	Toaster	Unable to clean	Kryptik.YQ Trojan	0	n/a	n/a	n/a	1	1		
1	FIS	Toaster	Virus Removed	Gen.Variant.FakeAlert.47 x2	0	n/a	n/a	n/a	1	1		
1	GTC	Pop-up	Disinfected	Gen.Variant.FakeAlert.47 (Engine-A)	0	n/a	n/a	n/a	1	1		
1	KPU	Browser	The requested URl cannot be retrieved	Trojan.HTML.Fraud.ct	0	n/a	n/a	n/a	1	1		
1	MTP	Toaster	Removed	JS/Wonka		n/a	n/a	n/a	1	1		
1	N360	Browser	Blocked	Known malicious website has been blocked		n/a	n/a	n/a	1	1		
1	PIS	Toaster	Neutralized	Virus neutralized	0	1		n/a				1
1	TTM	None	Blocked	Dangerous Webpage	0	n/a	n/a	n/a	1	1		
1	WBR	Browser	Blocked	Potentially threatening site	0	n/a	n/a	n/a	1	1		
3	AVI	Pop-up	Quarantined	eqaculation-video[1].htm	0	n/a	n/a	n/a	1	1		
3	BDF	Pop-up	Blocked	Gen: Variant.FakeAlert.47	0	n/a	n/a	n/a	1	1		
3	ESS	Toaster	Blocked	JS/TrjanCliker.Agent.NAZ	0	n/a	n/a	n/a	1	1		
3	FIS	Toaster	Virus Removed	Gen.Variant.FakeAlert.47 x2	0	n/a	n/a	n/a	1	1		
3	GTC	Pop-up	Blocked	Gen.Variant.FakeAlert.47 (Engine-A)	0	n/a	n/a	n/a	1	1		
3	KPU	Browser	Access Denied	Trojan.HTML.Fraud.ct URL: http://fmx930.co.cc/?u=131083	0	n/a	n/a	n/a	1	1		

3	MTP	Pop-Up	None	Potential threat asking for approval		Unexpected error blocking the manual test	n/a	n/a				1
3	N360	Browser	Blocked	Virus has been blocked and recommended not to visit this site		n/a	n/a	n/a	1	1		
3	PIS	Toaster	Neutralized	Virus neutralized		n/a	n/a	n/a				1
3	TTM	None	Blocked	Dangerous page		n/a	n/a	n/a	1	1		
3	WBR	Pop-up	Blocked	InternetSecurity2011				Scan completed successfully, no viruses have been detected				1
4	AVI	Pop-up	Access Denied	JS/Agent.abx.2 x3	0	n/a	n/a	n/a	1	1		
4	BDF	Toaster	Deleted	Trojan.JS.QCK x3	0	n/a	n/a	n/a	1	1		
4	ESS	Toaster	Connection terminated, threat cleaned	TrojanDownloader.Iframe.NJL	0	n/a	n/a	n/a	1	1		
4	FIS	Toaster	Virus Removed	Trojan.JS.QCK	0	n/a	n/a	n/a	1	1		
4	GTC	Pop-up	Access Denied	Trojan.JS.QCK (Engine-A)	0	n/a	n/a	n/a	1	1		
4	KPU	Browser	The requested URl cannot be retrieved	Trojan.Script.Iframer	0	n/a	n/a	n/a	1	1		
4	MTP	None	None	None	0	n/a	n/a	n/a	1	1		
4	N360	Toaster	Blocked	HTTP CrimePack Toolkit JAR on URL: servicerecord.co.cc/ajax/jar5.php		n/a	n/a	n/a	1	1		
4	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
4	TTM	None	Blocked	http:/simillu.com/court25.php		n/a	n/a	n/a	1	1		
4	WBR	Pop-up	Quarantined	Troj/PDF Js-ML (Virus); trojan-dermodns (Trojan Horse)				1				1
5	AVI	Toaster	Blocked	WEPvYsDxdn.exe	0	None	None	None				1
5	BDF	Pop-up	Access Denied	Exploit.CVE-2010-1885.c	0	Yes	2 threats deleted 1 remain	2 threats deleted 1 remain				1

5	ESS	Toaster	Quarantined	Kryptic.IWC trojan (exe.exe)	0	n/a	n/a	n/a	1	1		
5	FIS	Browser and Pop-up	Blocked	secdot	0	n/a	n/a	n/a	1	1		
5	GTC	Pop-up	Disinfected	JS:Downloader-AJE[Trj](Engine-B); JS: Pdfka-AUO[Epl](Engine-B); JS: ScriptDc-inf;	0	n/a	n/a	n/a	1	1		
5	KPU	Toaster	Denied	Trojan-Downloader.Script.Generic	0	n/a	n/a	n/a	1	1		
5	MTP	None	None	Smart HDD	1	None	Quarantined	Artemis!D1A15D3BEC75				1
5	N360	Toaster	Blocked	HTTP Java Obe Toolkit Activity		n/a	n/a	n/a	1	1		
5	PIS	None	Disinfected	Spyware/ Suspicious operation		n/a	n/a	n/a	1	1		
5	TTM	None	Blocked	http://0000002.in/index.php		n/a	n/a	n/a	1	1		
5	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
7	AVI	Pop-up	Access Denied	Blocked HTML/FakeAV.C and HTML/Crypted.Gen	0	n/a	n/a	n/a	1	1		
7	BDF	Pop-up	Blocked	Gen.Variant.FakeAlert.47 x3	0	n/a	n/a	n/a	1	1		
7	ESS	Toaster	quarantined	Win32/Sapik trojan	0	n/a	n/a	n/a	1	1		
7	FIS	Pop-up	Virus Removed	Gen:Variant.FakeAlert.47 x2	0	n/a	n/a	n/a	1	1		
7	GTC	Pop-up	Disinfected	Gen.Variant.FakeAlert.47 (Engine-A)	0	n/a	n/a	n/a	1	1		
7	KPU	Browser and Toaster	Access Denied	Trojan.HTML.Fraud.ct	0	n/a	n/a	n/a	1	1		
7	MTP	Pop-up	None	Internet Security 2011		None	None	None				1
7	N360	Toaster	Blocked	HTTP FakeAV Scan WEebpage2 (advert381.co.cc/?u=131083)		n/a	n/a	n/a	1	1		
7	PIS	Pop-up	Quarantined	Internet Security 2011		None	None	JS_REDIR.SMR			1	
7	TTM	None	Blocked	Dangerous page		n/a	n/a	n/a	1	1		
7	WBR	Pop-up	Blocked	Internet Security 2011		none	Removed	trojan-ransom-getacc (Trojan Horse)			1	
8	AVI	Toaster	Blocked	0.8623916870279283.exe	0	Yes	HTML/Agent.16156	1 file moved to quarantine			1	
8	BDF	Pop-up	Blocked	Trojan.JS.QCK x 2 and 0.8483249241445858.exe	0	n/a	n/a	n/a	1	1		

8	ESS	Toaster	Connection terminated, threat cleaned	js/TrojanDownloader.Iframe.NJL	0	n/a	n/a	n/a	1	1		
8	FIS	Browser and Pop-up	Virus Removed	Trojan.JS.QCK x2	0	n/a	n/a	n/a	1	1		
8	GTC	Pop-up	Disinfected	HTML:Script-inf(Engine-B); Java.Trojan.Downloader.OpenConnection.AI(Engine-A); Trojan.JS.QCK (Engine-A)	0	None	None	None	1		1	
8	KPU	Browser and Toaster	Access Denied	HEUR:Trojan.Script.Iframer	0	n/a	n/a	n/a	1	1		
8	MTP	Toaster	Removed	Artemis!4CD2D5D5DFD9 (Trojan Horse)		n/a	n/a	n/a	1	1		
8	N360	Toaster	Blocked	HTTP CrimePack Toolkit JAR on URL: rapidsystem.co.cc/get/jar5.php		n/a	n/a	n/a	1	1		
8	PIS	None	Deleted	Trj/CI.A		n/a	n/a	n/a	1	1		
8	TTM	None	Blocked	Dangerous page		n/a	n/a	n/a	1	1		
8	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
9	AVI	Pop-up	Quarantined	JS/Redirector.JM; EXP/PDF.Jeka.B exploit; TR/PWS.Sinowal.Gen;	0	n/a	n/a	n/a	1	1		
9	BDF	None	None	None	0	n/a	n/a	n/a	1	1		
9	ESS	Toaster	Quarantined	JS?TrojanDownloader.Twetti.NAA	0	n/a	n/a	n/a	1	1		
9	FIS	Browser	Blocked	None	0	n/a	n/a	n/a	1	1		
9	GTC	Pop-up	Quarantined	HTML:Iframe-OM[Trj](Engine-B)	0	n/a	n/a	n/a	1	1		
9	KPU	Browser and Toaster	Access Denied	HEUR:Trojan-Downloader.Script.Generic	0	n/a	n/a	n/a	1	1		
9	MTP	None	None	None	0	None	None	None			1	
9	N360	Toaster	Blocked	HTTP Malicious Javascript Encoder 5		n/a	n/a	n/a	1	1		
9	PIS	None	Quarantined	JS/Tweety.A		n/a	n/a	n/a	1	1		

9	TTM	Browser	Blocked	Dangerous page		n/a	n/a	n/a	1	1		
9	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
12	AVI	None	None	None	0	n/a	n/a	n/a	1	1		
12	BDF	None	None	None	0	n/a	n/a	n/a	1	1		
12	ESS	Toaster	Quarantined	Win32/TrojanDownloader.FakeAlert.BBT	0	n/a	n/a	n/a	1	1		
12	FIS	Browser	Blocked	http://mytraff.com/in.cgi?17&seoref=meter=	0	n/a	n/a	n/a	1	1		
12	GTC	Pop-up	Disinfected	JS:Downloader-LP	0	n/a	n/a	n/a	1	1		
12	KPU	Toaster	Detected	Trojan.JS.Redirector.bu	0	n/a	n/a	n/a	1	1		
12	MTP	None	None	None		n/a	n/a	n/a	1	1		
12	N360	Browser	Blocked	http://greatreload.in/flash-HQ-plugin.40076.exe		n/a	n/a	n/a	1	1		
12	PIS	None	Quarantined	JS/Redirector.K		n/a	n/a	n/a	1	1		
12	TTM	None	None	None		n/a	n/a	n/a	1	1		
12	WBR	None	None	None		n/a	n/a	n/a	1	1		
13	AVI	Pop-up	Denied	JS/Agent.abx.2	0	n/a	n/a	n/a	1	1		
13	BDF	Pop-up	Blocked	Trojan.JS.QCK	0	Report	Deleted	Gen.Varient.Kazy.5842 x41			1	
13	ESS	Toaster	Quarantined	JS/TrojanDownloader.Iframe.NJL	0	n/a	n/a	n/a	1	1		
13	FIS	Pop-up	Removed	Trojan.JS.QCK	0	n/a	n/a	n/a	1	1		
13	GTC	Pop-up	Disinfected	Trojan.JS.QCK	0	n/a	n/a	n/a	1	1		
13	KPU	Browser and Toaster	Access Denied	HEUR:Trojan.Script.Iframer	0	n/a	n/a	n/a	1	1		
13	MTP	None	None	None		Your computer is at risk	2 detected/1 unable to delete	2 detected/1 unable to delete			1	
13	N360	Toaster	Blocked	HTTP CrimePack Toolkit JAR		n/a	n/a	n/a	1	1		
13	PIS	Toaster	Deleted	update.php		n/a	n/a	n/a	1	1		
13	TTM	None	None	None	1	n/a	n/a	n/a	1	1		
13	WBR	Pop-up	Blocked	wsku.exe		None	None	None			1	
14	AVI	Pop-up	Quarantined	TR/Agent.AO.17	0	n/a	n/a	n/a	1	1		
14	BDF	Pop-up	Blocked	Gen:Vriant.Kazy.5844 x2	0	n/a	n/a	n/a	1	1		
14	ESS	Toaster	Quarantined	Kryptyk.IXE trojan x2	0	n/a	n/a	n/a	1	1		

14	FIS	Browser and Toaster	Virus Removed	Gen:Variant.Kazy.5844 x2	0	n/a	n/a	n/a	1	1		
14	GTC	Pop-up	Quarantined	JS:Downloader-AJE[Trj](Engine-B); JS:Pdfka-AUO[Expl](Engine-B);	0	n/a	n/a	n/a	1	1		
14	KPU	Toaster	Detected	HEUR:Trojan-Downloader.Script .Generic	0	n/a	n/a	n/a	1	1		
14	MTP	Toaster	Removed	Artemis!E8D6B7D9409E		n/a	n/a	n/a	1	1		
14	N360	Toaster	Blocked	HTTP Java Obe Toolkit Activity		n/a	n/a	n/a	1	1		
14	PIS	None	Blocked	HELPCTR.EXE		None	None	None			1	
14	TTM	None	Blocked	http://4000000.in/index.php		n/a	n/a	n/a	1	1		
14	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
15	AVI	Toaster	Access Denied	HTML/FakeAV.C x2	0	n/a	n/a	n/a	1	1		
15	BDF	None	None	None	0	n/a	n/a	n/a	1	1		
15	ESS	Toaster	Quarantined	Sapic Trojan	0	n/a	n/a	n/a	1	1		
15	FIS	Pop-up	System modification attempt	internetsecurity2011[1].exe; us?rinit.exe;	0	n/a	n/a	n/a				1
15	GTC	None	None	None	1	n/a	n/a	n/a				1
15	KPU	Browser and Toaster	Denied	Trojan.HTML.Froud.ct	0	n/a	n/a	n/a	1	1		
15	MTP	None	None	None		None	AV has been blocked by the virus	None				1
15	N360	Browser	Blocked	Unauthorized access		n/a	n/a	n/a	1	1		
15	PIS	Toaster	Neutralized	JS/Redirector.V		None	None	None				1
15	TTM	None	Blocked	http://lineacount.info/cgl-bin/search?id29740		n/a	n/a	n/a	1	1		
15	WBR	Pop-up	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
16	AVI	Pop-up	Denied	DR/FakeAV.wut.3; TR/Shutdowner.fft x10;	0	2 threats	Moved	Moved 2 hidden objects				1
16	BDF	Pop-up	Blocked	Gen.Variant.FakeAV.18 x2; Trojan.Generic.5199541 x2	0	n/a	n/a	n/a				1

16	ESS	Toaster	Connection terminated, threat cleaned	Adware.FakeAntySpy.U	0	n/a	n/a	n/a	1	1		
16	FIS	Browser	Blocked	None	0	n/a	n/a	n/a	1	1		
16	GTC	Pop-up	Disinfected	HTML:Iframe-inf(Engine-B) x2	0	n/a	n/a	n/a	1	1		
16	KPU	Toaster	Denied	Trojan.Win32.FakeAV.wut; Shutter.fft;	0	n/a	n/a	n/a				1
16	MTP	Toaster	Removed	Trojan - Artemis!889BB0B77C73		n/a	n/a	n/a	1	1		
16	N360	Toaster	Blocked	HTTP Malicious Toolkit Variant Activity 7		n/a	n/a	n/a	1	1		
16	PIS	None	Disinfected	Generic Trojan		n/a	n/a	n/a	1	1		
16	TTM	Browser	Blocked	http://www.hottoys.com.hk/		n/a	n/a	n/a	1	1		
16	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
17	AVI	Pop-up	Denied	HTML/Small.AE x2	0	None	None	None				1
17	BDF	Pop-up	Blocked	Exploit.PDF-JS.Gen x5; Gen:Variant.Kazy.5895 x4; Exploit.CVE-2010-1885.c	0	n/a	n/a	n/a	1	1		
17	ESS	Toaster	Quarantined	PDF?Exploit.Pidied.PDS.Gen trjan x4; Kryptik.IXZ trojan x2;	0	n/a	n/a	n/a	1	1		
17	FIS	Browser and Pop-up	Blocked	Exploit.PDF-JS.Gen x6; Gen:Variant.Kazy.5895 x3	0	n/a	n/a	n/a	1	1		
17	GTC	Pop-up	Disinfected	JS:Downloader-AJD[Trj](Engine-B); dlyzcrbmjnxqeuy1[1].pdf; e4jewe4jj3[1].exe; JS:Downloader-AJD[Trj](Engine-B);	0	n/a	n/a	n/a	1	1		
17	KPU	Toaster	Denied	HEUR;exploit.SCRIPT.generic	0	n/a	n/a	n/a	1	1		
17	MTP	None	None	Antivirus Action /Innovative protection for your PC/		None	None	No threats have been detected				1
17	N360	Browser	Blocked	HTTP Fragus Toolkit Download Activity - hegeam.com/gizmod/go.php		n/a	n/a	n/a	1	1		
17	PIS	Toaster	Quarantined	Protection against unknown threats		n/a	n/a	n/a	1	1		

17	TTM	None	Blocked	Dangerous Page - http://gagll.com/gizmond/irbrbuawdtelxlfu.vbs		n/a	n/a	n/a	1	1		
17	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
18	AVI	Pop-up	Denied	istall.48728[1].exe x2		n/a	n/a	n/a	1	1		
18	BDF	Pop-up	Blocked	Trojan.Generic.KD.15088 x7	0	n/a	n/a	n/a	1	1		
18	ESS	Toaster	Quarantined	TrojanDownloader.FakeAlert.AZE	0	n/a	n/a	n/a	1	1		
18	FIS	Browser	Blocked	None	0	n/a	n/a	n/a	1	1		
18	GTC	Pop-up	Disinfected	Trojan.Generic.KD.15088(Engine-A)	0	n/a	n/a	n/a	1	1		
18	KPU	Browser and Toaster	Access Denied	Trojan-Downloader.win32.CodecPack.lsl	0	n/a	n/a	n/a	1	1		
18	MTP	Toaster	Removed	Downloader-CEW.e (Trojan)		n/a	n/a	n/a	1	1		
18	N360	Toaster	Removed	Spyware Strike (install.48728[1].exe)		n/a	n/a	n/a	1	1		
18	PIS	Toaster	Neutralized	Trj/Zlob.QL		n/a	n/a	n/a	1	1		
18	TTM	Browser	Blocked	Dangerous Page		n/a	n/a	n/a	1	1		
18	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
19	AVI	Browser and Pop-up	Warning	HTML:FakeAV.c x2	0	n/a	n/a	n/a	1	1		
19	BDF	None	None	None	0	n/a	n/a	n/a	1	1		
19	ESS	Toaster	Quarantined	Win32/Sapik trojan	0	n/a	n/a	n/a	1	1		
19	FIS	None	None	None	0	n/a	n/a	n/a				1
19	GTC	None	None	None	0	n/a	n/a	n/a				1
19	KPU	Browser and Toaster	Access Denied	Trojan.HTML.Froud.ct	0	n/a	n/a	n/a	1	1		
19	MTP	None	None	None		None	None	None				1
19	N360	Toaster	Blocked	Fake AV Scan Webpage 2		n/a	n/a	n/a	1	1		
19	PIS	None	None	Cookie/Doubleclick		None	None	None				1
19	TTM	None	Blocked	Dangerous Webpage - http://wovens.info/counter.php		n/a	n/a	n/a	1	1		
19	WBR	Pop-up	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		

20	AVI	Pop-up	Access Denied	HTNL/Crypted.Gen x5		n/a	n/a	n/a	1	1		
20	BDF	None	None	None	0	n/a	n/a	n/a	1	1		
20	ESS	Toaster	Quarantined	JS/TrojanDownloader.AgentNUH	0	n/a	n/a	n/a	1	1		
20	FIS	Pop-up	System modification attempt	internetsecurity2011[1].exe; us?rinit.exe;	0	n/a	n/a	n/a				1
20	GTC	Pop-up	Disinfected	HTML:Iframe-EP[Trj](Engine-B) x2	0	Rootkit.Siref.D(Engine-A) x3; HTML.Iframe-EP[Trj];		Disinfect (if not possible: quarantine)				1
20	KPU	Browser and Toaster	Access Denied	JS.Agent.bpb	0	n/a	n/a	n/a	1	1		
20	MTP	None	None	None		None	None	None				1
20	N360	Toaster	Blocked	HTTP FakeAV Scan Webpage 2		n/a	n/a	n/a	1	1		
20	PIS	Toaster	None	Generic Trojan		None	None	None				1
20	TTM	None	Blocked	Dangerous Page		n/a	n/a	n/a	1	1		
20	WBR	Pop-up	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
21	AVI	Pop-up	Denied	HTML:Small.AE; sefibyUYtc.exe; TR/Crypt.ZPACK.Gen;	0	Access to the file was denied	XUPuycTC.dll	Moved to quarantine			1	
21	BDF	Pop-up	Blocked	Exploit.PDF-JS.Gen; Exploit.CVE-2010-1885.C;	0	n/a	n/a	n/a	1	1		
21	ESS	Toaster	Connection terminated, threat cleaned	PDF/Exploit.Pidief.PDS.Gen x4	0	n/a	n/a	n/a	1	1		
21	FIS	Pop-up	Virus Removed	Exploit.PDF-JS. Gen x4	0	n/a	n/a	n/a	1	1		
21	GTC	Pop-up	Disinfected	JS:Downloader-AJQ[Trj](Engine-B); Exploit.PDF-JS.Gen x2; Gem;Variant.Kazy.5965(Engine-A);	0	n/a	n/a	n/a	1	1		
21	KPU	Toaster	Denied	HEUR:Exploit.Script.Generic	0	n/a	n/a	n/a	1	1		

21	MTP	Toaster	Removed	FakeAlert-SecurityTool.z (avxwgoisbmcsyr[1].exe)		n/a	n/a	n/a	1	1		
21	N360	Toaster	Blocked	HTTP Fragus Toolkit Download Activity		n/a	n/a	n/a	1	1		
21	PIS	Toaster	Blocked	Unknown Virus / Suspicious program		None	None	None				1
21	TTM	None	Blocked	Dangerous Page		n/a	n/a	n/a	1	1		
21	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
22	AVI	None	None	None	0	n/a	n/a	n/a				1
22	BDF	None	None	None	0	None	None	None				1
22	ESS	Toaster	Quarantined	Win32/Kryptik.IYU trojan	0	None	None	None	1	1		
22	FIS	Browser	Blocked	http//nudebeachcamera.com/	0	n/a	n/a	n/a	1	1		
22	GTC	Pop-up	Disinfected	JS:Pdfka-AVF [Expl] (Engine-B)	0	n/a	n/a	n/a				1
22	KPU	None	None	None	0	n/a	n/a	n/a				1
22	MTP	Toaster	Removed	FakeAlert-SecurityTool.z (avxwgoisbmcsyr[1].exe); defender.exe		n/a	n/a	n/a	1	1		
22	N360	Toaster	Blocked	HTTP Malicious Toolkit Variant Activity 7 (japawos.co.cc/byt1zqvg/?1)		n/a	n/a	n/a	1	1		
22	PIS	None	None	None		None	None	None	1	1		
22	TTM	None	None	None		NA	NA	NA				1
22	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
23	AVI	Toaster	Blocked	0.7684836026737486.exe; exe.exe; avxwgoisbmcsyr[1].exe; vWLKdLDhCL.exe	0	vWLKdLDhCL.exe has been blocked to access internet	1 object moved (OpenConnect.CF)	1 object moved (OpenConnect.CF)				1

23	BDF	Pop-up	Blocked	Exploit.PDF-JS.Gen x4	0	5 threats detected	Trojan.Downloader.JNSC, Java.Trojan. Downloader. OpenConnection, Exploit.PDF-JS.Gen - deleted; Java.Trojan. Downloader. OpenConnection x2	All issues solved			1	
23	ESS	Toaster	Connection terminated, threat cleaned	Exploit.Pidief.PDS.Gen x4	0	None	None	None				1
23	FIS	Browser	Blocked	None	0	n/a	n/a	n/a	1	1		
23	GTC	Pop-up	Blocked	Exploit.PDF-JS.Gen(Engine-A) x2; VBS:Agent-FS[Trj](Engine-B); Java Trojan.Downloader.OenConnection.AI	0	n/a	n/a	n/a	1	1		
23	KPU	Toaster	Denied	HEUR:Exploit.Script.Generic	0	Exploit.PDF-JS.Gen; VBS:Agent-FS	Desinfected	Desinfected	1	1		
23	MTP	None	None	None		None	None	Trojan/ Virus				1
23	N360	Toaster	Blocked	HTTP Fragus Toolkit Download Activity (5675.in/ 1292851092.php)		n/a	n/a	n/a	1	1		
23	PIS	Pop-up and Toaster	Blocked	avxwgoisbmcsyr[1].exe		n/a	n/a	n/a	1	1		
23	TTM	None	Blocked	Dangerous page		n/a	n/a	n/a	1	1		
23	WBR	Browser	Blocked	Potentially threatening site		n/a	n/a	n/a	1	1		
24	AVI	Pop-up	Denied	JS/Agent.abx.2 x3	0	n/a	n/a	n/a	1	1		

24	BDF	Pop-up	Blocked	Trojan.JS.QCK x2; Backdoor.Generic.534190; Gen:Variant.Kazy.6177 x2; Trojan.Generic.KD.89752 x2; Trojan.Generic.KDV.88414;	0	n/a	n/a	n/a	1	1		
24	ESS	Toaster	Quarantined	JS/TrojanDownloader.Iframe.NJL x2	0	n/a	n/a	n/a	1	1		
24	FIS	Pop-up	Virus Removed	Trojan.JS.QCK	0	n/a	n/a	n/a	1	1		
24	GTC	Pop-up	Quarantined	Trojan.JS.QCK (Engine-A); JS:Downloader-RW[Trj](Engine-B);	0	n/a	n/a	n/a	1	1		
24	KPU	Browser and Toaster	Access Denied	HEUR:Trojan.Script.Iframer	0	n/a	n/a	n/a	1	1		
24	MTP	Toaster	None	None		Toaster	Trojan Removed	Artemis!29ABEC9EEA49				1
24	N360	Browser	Blocked	HTTP Malicious Toolkit Variant Activity 7 (fbtech.cz.cc/images/scans/)		n/a	n/a	n/a	1	1		
24	PIS	Toaster	Neutralized	test.exe		n/a	n/a	n/a	1	1		
24	TTM	None	Blocked	Dangerous Page (http://simillu.com/count25.php)		n/a	n/a	n/a	1	1		
24	WBR	None	Quarantined	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
25	AVI	Pop-up	Denied	HTML/Crypted.Gen x2; HTML/Fake.AV; 56f4fa62.qua	0	n/a	n/a	n/a	1	1		
25	BDF	None	None	None	0	n/a	n/a	n/a	1	1		
25	ESS	Toaster	Blocked	JS/TrojanCliker.Agent.Naz x2	0	n/a	n/a	n/a	1	1		
25	FIS	Pop-up	Virus could not be removed	Rootkit.Serefef.D	0	n/a	n/a	n/a				1
25	GTC	None	None	None	0	n/a	n/a	n/a				1
25	KPU	Browser and Toaster	Access Denied	Trojan.HTML.Fraud.ct	0	n/a	n/a	n/a	1	1		
25	MTP	None	None	None		NA	NA	NA				1
25	N360	Browser	Blocked	Unauthorized access		n/a	n/a	n/a	1	1		

25	PIS	None	Disinfected	JS/Redirector.V; Cookie/Doubleclick		n/a	n/a	n/a	1	1		
25	TTM	None	Blocked	Dangerous Page (http://lineacount.info/cgi-bin/search?id=20010		n/a	n/a	n/a	1	1		
25	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
26	AVI	Pop-up	Access Denied	JS/Redirector.JM; TR/PWS.Sinowal.Geo; EXP/PDF.Jeka.B;	0	n/a	n/a	n/a	1	1		
26	BDF	Pop-up	Blocked	Backdoor.Generic.53955	0	n/a	n/a	n/a	1	1		
26	ESS	Toaster	Quarantined	JS/TrojanDownloader.Twetti.NAA	0	n/a	n/a	n/a	1	1		
26	FIS	Browser	Blocked	None	0	n/a	n/a	n/a	1	1		
26	GTC	Pop-up	Disinfected	JS:Prontexi-DJ[Trj](Engine-B); Exploit.PDF-JS.Gen(Engine-A);	0	n/a	n/a	n/a	1	1		
26	KPU	Browser and Toaster	Access Denied	HEUR:Trojan.Script.Generic	0	n/a	n/a	n/a	1	1		
26	MTP	Toaster	Removed	Generic.dx!tlq		n/a	n/a	n/a	1	1		
26	N360	Browser	Blocked	HTTP Malicious Toolkit Variant Avtibvity 15 (aliciakeysfan.com/)		n/a	n/a	n/a	1	1		
26	PIS	Toaster	Quarantined	Trj/CI.A / JS/Tweety.A		n/a	n/a	n/a	1	1		
26	TTM	Browser	Blocked	Dangerous Page (aliciakeysfan.com/)		n/a	n/a	n/a	1	1		
26	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
27	AVI	Pop-up	Quarantined	JS/Dldr.Agent.NBN.1 x3; EXP/PDF.Jeka.B x5	0	n/a	n/a	n/a	1	1		
27	BDF	Pop-up	Blocked	Gen.Variant.Kazy.5832	0	n/a	n/a	n/a	1	1		
27	ESS	Toaster	Quarantined	JS/TrojanDownloader.Twetti.NAA	0	n/a	n/a	n/a	1	1		
27	FIS	Browser	Blocked	None	0	n/a	n/a	n/a	1	1		
27	GTC	Pop-up	Disinfected	JS:Prontexi-DJ[Trj](Engine-B) x2	0	n/a	n/a	n/a	1	1		
27	KPU	Browser and Toaster	Access Denied	HEUR:Trpjan-Downloader.Script.Generic	0	n/a	n/a	n/a	1	1		

27	MTP	None	None	None		Not all issues are resolved	Unable to delete	TDSS.d!mem (Trojan); SUSP_IRP_MJ_CREATE				1
27	N360	Toaster	Blocked	HTTP Malicious Javascript Encoder 5		n/a	n/a	n/a	1	1		
27	PIS	Toaster	Blocked	Cookie/YieldManager		n/a	n/a	n/a	1	1		
27	TTM	None	Blocked	Dangerous Webpage		n/a	n/a	n/a	1	1		
27	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
28	AVI	Toaster	Blocked	bKNILMsCGe.Exe	0	Has been blocked to acess internet.	None	None				1
28	BDF	Pop-up	Blocked	Exploit.PDF-JS.Gen x3; Gen:Variant.Kazy.6252;	0	n/a	n/a	n/a	1	1		
28	ESS	Browser and Toaster	Connection terminated, threat cleaned	PDF/Exploit.Pidief.PDS.Gen x4	0	n/a	n/a	n/a	1	1		
28	FIS	Pop-up	Virus Removed	Exploit.PDF-JS.Gen x6	0	n/a	n/a	n/a	1	1		
28	GTC	Pop-up	Blocked	Exploit.PDF-JS.Gen(Engine-A) x2; Gen:Variant.Kazy.6252(Engine-A);	0	n/a	n/a	n/a	1	1		
28	KPU	Toaster	Denied	HEUR:Exploit.Script.Generic; Trojan-Downloader.VBS.Agent.aaf;	0	n/a	n/a	n/a	1	1		
28	MTP	None	None	None		None	None	None			1	
28	N360	Toaster	Blocked	HTTP Fragus Toolkit Download Activity		n/a	n/a	n/a	1	1		
28	PIS	Toaster	Blocked	avxwgoisbmcsyr[1].exe		n/a	n/a	n/a	1	1		
28	TTM	None	Blocked	Dangerous Page http://4322.in/1292935727.php		n/a	n/a	n/a	1	1		
28	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
29	AVI	Pop-up	Access Denied	HTML/Crypted.Gen; slogscripej.exe;	0	TR/CryptZPACK.Gen 2 x2	Moved to quarantine	Moved to quarantine			1	

29	BDF	Pop-up	Blocked	Gen:Variant.KFakeAlert.55	0	n/a	n/a	n/a	1	1		
29	ESS	Toaster	Quarantined	JS/TrojanDownloader.Agent.NVW x2; Kryptik.JBS;	0	n/a	n/a	n/a	1	1		
29	FIS	Browser	Blocked	None	0	n/a	n/a	n/a	1	1		
29	GTC	Pop-up	Disinfected	JS:Redirector-E[Trj](Engine-B); Gen:Variant.FakeAlert.55(Engine-A);	0	n/a	n/a	n/a	1	1		
29	KPU	Browser and Toaster	Access Denied	HEUR:Trojan.Win32.Generic	0	n/a	n/a	n/a	1	1		
29	MTP	None	None	None		None	None	None				1
29	N360	Toaster	Removed	inst[1].exe		n/a	n/a	n/a	1	1		
29	PIS	Toaster	Disinfected	JS/Redirect.V		n/a	n/a	n/a	1	1		
29	TTM	Browser and Toaster	Blocked	HTML_RENOS.SMD		n/a	n/a	n/a	1	1		
29	WBR	Browser	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
30	AVI	None	None	None	0	n/a	n/a	n/a	1	1		
30	BDF	None	None	None	0	n/a	n/a	n/a	1	1		
30	ESS	Toaster	Quarantined	JS/Trojanclicker.Agent.NAZ	0	n/a	n/a	n/a	1	1		
30	FIS	Pop-up	System modification attempt	internetsecurity2011[1].exe;	0	n/a	n/a	n/a				1
30	GTC	None	None	None	0	n/a	n/a	n/a				1
30	KPU	Toaster	Denied	Trpjan.JS.Redirector.bu	0	n/a	n/a	n/a	1	1		
30	MTP	None	None	None		None	None	None				1
30	N360	Browser	Blocked	Unauthorized access		n/a	n/a	n/a	1	1		
30	PIS	None	Disinfected	Cookie/Zedo; Cookie/Doubleclick		n/a	n/a	n/a	1	1		
30	TTM	None	Blocked	Dangerous Page http://82.196.5.24/js.php?2-17		n/a	n/a	n/a	1	1		
30	WBR	None	Blocked	WRFWALERTTYPE_PROCMONSTANDARD		n/a	n/a	n/a	1	1		
31	AVI	Pop-up	Access Denied	TR/Dldr.Agent.fcra		n/a	n/a	n/a	1	1		
31	BDF	Pop-up	Disinfected	Trojan.Generic.5149385		n/a	n/a	n/a	1	1		
31	ESS	Toaster	Blocked	Infected file		n/a	n/a	n/a	1	1		

31	FIS	Toaster	Removed	Trojan.Generic.5149385		n/a	n/a	n/a	1	1		
31	GTC	Pop-up	Disinfected	JavaTrojan. Downloader.OpenConnection.AI (Engine-A)		n/a	n/a	n/a	1	1		
31	KPU	Browser	Access Denied	HEUR:Trojan.Script.Iframer		n/a	n/a	n/a	1	1		
31	MTP	Pop-up	Removed	Artemis!908B8E4A4220 x2; Generic.Dropper.va.gen.g	0	None	None	None				1
31	N360	Pop-up	Blocked	HTTP Java launchJNLP DocBase BO		n/a	n/a	n/a	1	1		
31	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
31	TTM	None	Blocked	http://hostads.cn/		n/a	n/a	n/a	1	1		
31	WBR	Browser	Blocked	htttp://www.sharktale.com/	0	n/a	n/a	n/a	1	1		
32	AVI	None	None	None		n/a	n/a	n/a	1	1		
32	BDF	None	None	None		n/a	n/a	n/a	1	1		
32	ESS	None	None	None		n/a	n/a	n/a	1	1		
32	FIS	Toaster	Blocked	javafire795.exe - potentially harmful program		n/a	n/a	n/a	1	1		
32	GTC	Pop-up	Blocked	jar_cache32691.tmp		n/a	n/a	n/a	1	1		
32	KPU	Browser	Access Denied	HEUR:Trojan.Script.Iframer		n/a	n/a	n/a	1	1		
32	MTP	Pop-up	Removed	Artemis!302545366D71	0	n/a	n/a	n/a	1	1		
32	N360	Pop-up	Removed	jar_cache58808.tmp	0	n/a	n/a	n/a	1	1		
32	PIS	None	Quarantined	Trj/CI.A		n/a	n/a	n/a	1	1		
32	TTM	None	Blocked	http://vanforsaleinessex.co.uk/ media/new.html x2		n/a	n/a	n/a	1	1		
32	WBR	Toaster	Blocked	jar_cache51875.tmp	0	n/a	n/a	n/a	1	1		
33	AVI	None	Access Denied	TR/Hijacker.Gen[trojan]		n/a	n/a	n/a	1	1		
33	BDF	Toaster	Blocked	Exploit.PDF-JS.Gen		n/a	n/a	n/a	1	1		
33	ESS	Toaster	Quarantined	PDF/Exploit.Pidief.PDS.Geen trojan		n/a	n/a	n/a	1	1		
33	FIS	Toaster	Removed	Exploit.PDF-JS.Gen		n/a	n/a	n/a	1	1		
33	GTC	Pop-up	Access Denied	Exploit.PDF-JS.Gen (Engine-A)		n/a	n/a	n/a	1	1		
33	KPU	Toaster	Access Denied	URL found in the base		n/a	n/a	n/a	1	1		
33	MTP	None	None	None	0	n/a	n/a	n/a	1	1		

33	N360	Pop-up	Blocked	HTTP Fragus Toolkit Download Activity x5	0	n/a	n/a	n/a	1	1		
33	PIS	None	Disinfected	HELPCRT.EXE x2		n/a	n/a	n/a	1	1		
33	TTM	None	Blocked	x2		n/a	n/a	n/a	1	1		
33	WBR	Browser	Blocked	http://www.tutorialhero.com/tag-67-Transperant.php	0	n/a	n/a	n/a	1	1		
34	AVI	Pop-Up	Access Denied	HTML/Crypted.Gen [virus]		none	none	none				1
34	BDF	None	None	None		n/a	n/a	n/a	1	1		
34	ESS	Toaster	Quarantined	A variant of Win32/Rootkit.Kryptik.CK trojan		None	None	None	1	1		
34	FIS	Pop-up	Blocked	Iinternetsecurity2011[2].exe		n/a	n/a	n/a	1	1		
34	GTC	Pop-up	Quarantined	userinit.exe, started by internetsecurity2011[1].eze		None	None	None			1	
34	KPU	Toaster	Access Denied	HEUR:Trojan.Win32.Generic		None	None	None				1
34	MTP	None	None	None	0	n/a	n/a	n/a				1
34	N360	Toaster	Blocked	web583.co.cc	0	n/a	n/a	n/a	1	1		
34	PIS	None	Disinfected	JS/Redirector.V		n/a	n/a	n/a				1
34	TTM	Browser	Blocked	http://kires.uv.ro/page722.html	0	n/a	n/a	n/a	1	1		
34	WBR	Pop-up	Blocked	InternetSecurity2011[1].exe	0	n/a	n/a	n/a	1	1		
35	AVI	Pop-Up	Blocked	Internetsecurity2011[1].exe		None	None	None				1
35	BDF	None	None	None		None	None	None	1	1		
35	COM	None	None	None	0	n/a	n/a	n/a	1	1		
35	ESS	Toaster	Blocked	JS/TrojanDownloader.Agent.Nue trojan		N/A	N/A	N/A	1	1		
35	FIS	Pop-up	Blocked	internetsecurity[1].exe		N/A	N/A	N/A	1	1		
35	GTC	Pop-up	Access Denied	HTML:Iframe-EP [Trj] (Engine-B)		N/A	N/A	N/A	1	1		
35	KPU	Toaster	Quarantined	HEUR:Trojan.Win32.Generic		None	None	None				1
35	MTP	None	None	None	0	n/a	n/a	n/a				1
35	N360	Toaster	Blocked	web583.co.cc	0	n/a	n/a	n/a	1	1		
35	PIS	None	Neutralized	SHSVCS.dll	0	None	None	None				1
35	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
35	WBR	Pop-up	Blocked	InternetSecurity2011[1].exe; us5rinit.exe	0	n/a	n/a	n/a	1	1		
36	AVI	Pop-up	Quarantined	TR/Dldr.CodecPa.Izl [trojan]		N/a	N/a	N/a	1	1		

36	BDF	Pop-up	Disinfected	Trojan.Generic.KD.15088		n/a	n/a	n/a	1	1		
36	COM	None	None	None	0	n/a	n/a	n/a	1	1		
36	ESS	Toaster	Quarantined	Win32/TrojanDownloader.Fake Alert.AZE trojan		n/a	n/a	n/a	1	1		
36	FIS	Toaster	Removed	Trojan.Generic.KD.15088		n/a	n/a	n/a	1	1		
36	GTC	Pop-up	Quarantined	Trojan.Generic.KD.15088(Engine-A)		n/a	n/a	n/a	1	1		
36	KPU	Browser	Access Denied	Trojan-Downloader.Win32.CodecPack.Izl		n/a	n/a	n/a	1	1		
36	MTP	Pop-up	Removed	Downloader-CEW.e (Trojan)	0	n/a	n/a	n/a	1	1		
36	N360	Browser	Blocked	http://deseczka.pl/sklep/media/ichiban.html	0	n/a	n/a	n/a	1	1		
36	PIS	Pop-up	Neutralized	Trj/Zlob.QL x2	0	n/a	n/a	n/a	1	1		
36	TTM	Browser	Blocked	http://desezka.pl/sklep/media/install.48728.exe	0	n/a	n/a	n/a	1	1		
36	WBR	None	None	None	0	n/a	n/a	n/a	1	1		
37	AVI	Toaster	Quarantined	TR/Crypt.XPACK.Gen [trojan]		n/a	n/a	n/a	1	1		
37	BDF	None	None	None		None	None	None			1	
37	COM	None	None	None	0	n/a	n/a	n/a	1	1		
37	ESS	Toaster	Access Denied	JS/Exploit.Pdfka.OOW.Gen.trojan		N/a	N/a	N/a	1	1		
37	FIS	Browser	Blocked	Gen:Variant.Kazy.7655		n/a	n/a	n/a	1	1		
37	GTC	Pop-up	Quarantined	HTML:Iframe-inf(Engine-B)		n/a	n/a	n/a	1	1		
37	KPU	Toaster	Access Denied	HEUR:Exploit.Script.Generic		n/a	n/a	n/a	1	1		
37	MTP	Pop-up	Program wants internet access	Default Allow	0	n/a	n/a	n/a				1
37	N360	None	None	None	0	n/a	n/a	n/a	1	1		
37	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
37	TTM	None	None	None	0	n/a	n/a	n/a	1	1		
37	WBR	None	None	None	0	n/a	n/a	n/a	1	1		
38	AVI	Toaster	Access Denied	HTML/Crypted.Gen [virus]		None	None	None				1
38	BDF	Pop-Up	Blocked	Gen:Variant.Kazy.7723		n/a	n/a	n/a	1	1		
38	COM	None	None	None	0	n/a	n/a	n/a	1	1		

38	ESS	Toaster	Quarantined	JS/TrojanDownloader.Agent.NUE trojan		n/a	n/a	n/a	1	1		
38	FIS	Toaster	Removed	Gen:Variant.Kazy.7723		n/a	n/a	n/a	1	1		
38	GTC	Pop-up	Quarantined	HTML:IFrame-EP[Trj](Engine-B)		n/a	n/a	n/a	1	1		
38	KPU	Pop-up	Quarantined	HEUR:Trojan.Win32.Generic		None	None	None				1
38	MTP	None	None	None	0	n/a	n/a	n/a				1
38	N360	Toaster	Blocked	http://vds152.co.uk	0	n/a	n/a	n/a	1	1		
38	PIS	None	Quarantined	SHSVCS.dll		n/a	n/a	n/a				1
38	TTM	None	None	None	1	n/a	n/a	n/a	1	1		
38	WBR	Pop-up	Blocked	us5rinit.exe	0	None	Blocked	Trojan-ransome-getacc			1	
39	AVI	Toaster	Access Denied	JS/Redirect.qrk [virus]		None	None	None				1
39	BDF	Pop-up	Blocked	Trojan.JS.Redirection.EM		n/a	n/a	n/a	1	1		
39	COM	None	None	None	0	n/a	n/a	n/a	1	1		
39	ESS	Toaster	Deleted	JS/Kryptik.H trojan		n/a	n/a	n/a	1	1		
39	FIS	Toaster	Removed	Gen:Variant.Kazy. 7723		n/a	n/a	n/a	1	1		
39	GTC	Pop-up	Quarantined	HTML:Iframe-LG[Trj](Engine-B)		n/a	n/a	n/a	1	1		
39	KPU	Browser	Access Denied	Trojan.JS.Redirector.bu		n/a	n/a	n/a	1	1		
39	MTP	None	None	None	0	None	None	None				1
39	N360	Toaster	Blocked	http://vds152.co.uk	0	n/a	n/a	n/a	1	1		
39	PIS	None	None	None	0	n/a	n/a	n/a				1
39	TTM	Pop-up	Blocked	SJ_REDIR.SMR		n/a	n/a	n/a	1	1		
39	WBR	Pop-up	Blocked	InternetSecurity2011[1].exe; us5rinit.exe	0	n/a	n/a	n/a	1	1		
40	AVI	Toaster	Blocked	HTML/Crypted.Gen[virus]		None	Access denied	HTML/Crypted.Gen[virus]				1
40	BDF	Pop-up	Blocked	Gen:Variant.Kazy.7723		n/a	n/a	n/a	1	1		
40	COM	None	None	None	0	n/a	n/a	n/a	1	1		
40	ESS	Toaster	Deleted	Win32/Adware.InternetSecurity2011 application		n/a	n/a	n/a	1	1		
40	FIS	Toaster	Removed	Gen:Variant.Kazy.7723		n/a	n/a	n/a	1	1		
40	GTC	Pop-up	Access Denied	Gen:Varriant.Kazy.7723(Engine-A)		n/a	n/a	n/a	1	1		
40	KPU	Pop-up	Quarantined	HEUR:Trojan.Win32.Generic		None	None	None				1
40	MTP	None	None	None	0	n/a	n/a	n/a				1

40	N360	Toaster	Blocked	http://vds152.co.uk	0	n/a	n/a	n/a	1	1		
40	PIS	None	Disinfected	ROBOFORM[1].HTML		n/a	n/a	n/a				1
40	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
40	WBR	Browser	Blocked	http://mauracrei.w8w.pl/roboform.html	0	n/a	n/a	n/a	1	1		
41	AVI	Pop-up	Access Denied	HTML/Crypted.Gen [virus]		None	Quarantined	HTML/Crypted.Gen				1
41	BDF	None	None	None		N/a	N/a	N/a	1	1		
41	COM	None	None	None	0	n/a	n/a	n/a	1	1		
41	ESS	Toaster	Quarantined	Win32/Kryptik.JOG trojan		n/a	n/a	n/a	1	1		
41	FIS	Pop-Up	Blocked	internetsecurity2011[1].exe		n/a	n/a	n/a	1	1		
41	GTC	Pop-up	Quarantined	internetsecurity2011[1].exe		n/a	n/a	n/a	1	1		
41	KPU	Pop-up	Quarantined	HEUR:Trojan.Win32.Generic		None	None	None				1
41	MTP	None	None	None	0	n/a	n/a	n/a				1
41	N360	Toaster	Blocked	http://vds462.co.uk	0	n/a	n/a	n/a	1	1		
41	PIS	Toaster	Neutralized	JS/Redirector.V	0	n/a	n/a	n/a	1	1		
41	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
41	WBR	Browser	Blocked	http://hollifielda.narod.ru/text1099.html	0	n/a	n/a	n/a	1	1		
42	AVI	Pop-up	Quarantined	TR/Ransom.PornoBlocker.dhf		n/a	n/a	n/a	1	1		
42	BDF	Pop-up	Blocked	Exploit.PDF-JS.Gen; Trojan.generic.KD.106259		n/a	n/a	n/a	1	1		
42	COM	None	None	None	0	n/a	n/a	n/a	1	1		
42	ESS	Toaster	Quarantined	PDF/Exploit.Pidief.PDS.Gen trojan		n/a	n/a	n/a	1	1		
42	FIS	Toaster	Removed	Trojan.Generic.KD.106259		n/a	n/a	n/a	1	1		
42	GTC	Pop-up	Access Denied	JS:Downloader-AKU[Trj](Engine-B); Java.Trojan.Downloader.OpenConnection.AI(Engine-A)		N/a	N/a	N/a	1	1		
42	KPU	Toaster	Access Denied	Trojan-Downloader.Java.OpenConnection.cf		n/a	n/a	n/a	1	1		
42	MTP	None	None	None	0	n/a	n/a	n/a	1	1		
42	N360	Toaster	Blocked	HTTP Malicious Toolkit Variant Activity 13	0	n/a	n/a	n/a	1	1		
42	PIS	Toaster	Neutralized	Explorer.exe	0	n/a	n/a	n/a				1

42	TTM	Browser	Blocked	http://caleyo9.co.cc/multy/ymjwapfzbwyrincmc.php	0	n/a	n/a	n/a	1	1		
42	WBR	Pop-up	Blocked	I.vbs; jar_cash16397.tmp; kqiugmeqfwat9[2].pd x2f; cpjvipjliqclknjo1[1].vbs;		None	None	None			1	
43	AVI	Pop-up	Access Denied	HTML/Crypted.Gen [virus]		None	None	None				1
43	BDF	None	None	None		n/a	n/a	n/a	1	1		
43	COM	None	None	None	0	n/a	n/a	n/a	1	1		
43	ESS	Toaster	Quarantined	JS/TrojanDownloader.Agent.NUE trojan		n/a	n/a	n/a	1	1		
43	FIS	Pop-up	Blocked	internetsecurity2011[1].exe		n/a	n/a	n/a	1	1		
43	GTC	Pop-up	Access Denied	HTML:Iframe-EP [Trj] (Engine-B)		n/a	n/a	n/a	1	1		
43	KPU	Browser	Access Denied	Trojan.JS.Agent.bpb		n/a	n/a	n/a	1	1		
43	MTP	Pop-up	Program wants internet access	VCHOST.EXE	0	n/a	n/a	n/a				1
43	N360	Toaster	Blocked	flv90.c0.cc	0	n/a	n/a	n/a	1	1		
43	PIS	None	None	None	1	n/a	n/a	n/a				1
43	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
43	WBR	Pop-up	Blocked	InternetSecurity2011[1].exe; us5rinit.exe;	0	n/a	n/a	n/a	1	1		
44	AVI	Pop-up	Quarantined	TR/Spy.Gen [trojan]		n/a	n/a	n/a	1	1		
44	BDF	Pop-up	Blocked	Gen:Trojan.Heur.RP.duX@ayPlbsg		n/a	n/a	n/a	1	1		
44	COM	None	None	None	0	n/a	n/a	n/a	1	1		
44	ESS	Toaster	Quarantined	JS/Kryptik.N trojan		n/a	n/a	n/a	1	1		
44	FIS	Toaster	Removed	Gen:Trojan.Heur.RP.duX@ayPlbsg		n/a	n/a	n/a	1	1		
44	GTC	Pop-up	Quarantined	Exploit.PDF-TTF.Gen(Engine-A); HTML:Iframe-inf(Engine-B); JS:ScriptDC-inf[Trj] (Engine-B)		n/a	n/a	n/a	1	1		
44	KPU	Toaster	Access Denied	HEUR:Exploit.Script.Generic		n/a	n/a	n/a	1	1		
44	MTP	None	None	None	1	n/a	n/a	n/a	1	1		
44	N360	Toaster	Blocked	covast.com	0	n/a	n/a	n/a	1	1		

44	PIS	None	Blocked	HELPCTR.EXE		n/a	n/a	n/a	1	1		
44	TTM	None	Blocked	http://velport873.in/tracker/		n/a	n/a	n/a	1	1		
44	WBR	None	None	None	1	n/a	n/a	n/a	1	1		
45	AVI	Toaster	Blocked	service144.exe; service189.exe; service182.exe		Malware found	Ignored	JAVA/OpenConnect.CF	1	1		
45	BDF	Pop-Up	Disinfected	Exploit.PDF-JS.Gen; Exploit.CVE-2010-1885.C		Detected 2 threats ; affecting 3 objects; Pop-up to choose action	Disinfection failed	Exploit.CVE-2010-1885.C; Java.Trojan.Downloader.OpenConnection.Al				1
45	COM	None	None	None	0	n/a	n/a	n/a	1	1		
45	ESS	Toaster	Deleted	PDF/Exploit.Pidief.PDS.Gen trojan		n/a	n/a	n/a	1	1		
45	FIS	Browser and Toaster	Removed	Exploit.PDF-JS.Gen		n/a	n/a	n/a	1	1		
45	GTC	Pop-up	Quarantined	HTML:Iframe-inf (Engine-B)		n/a	n/a	n/a	1	1		
45	KPU	Toaster	Access Denied	HEUR:Exploit.Script.Generic		n/a	n/a	n/a	1	1		
45	MTP	None	None	None	0	Two Items detected	Issues resolved	Virus x1 and Trojan x1			1	
45	N360	Toaster	Blocked	HTTP Fragus Toolkit Download Activity	0	n/a	n/a	n/a	1	1		
45	PIS	Toaster	Blocked	0.4202517202896592.exe		None	None	None			1	
45	TTM	Pop-up	Blocked	0.5486586918643259.exe; 0,07001150668530476.exe;		n/a	n/a	n/a	1	1		
45	WBR	Browser	Blocked	http://hackingarticles.com/get-free-demonoid-invitation-codes-code-generator/	0	n/a	n/a	n/a	1	1		
46	AVI	Toaster	Access Denied	HTML/Crypted.Gen[virus]		None	None	None				1
46	BDF	None	None	None		n/a	n/a	n/a	1	1		
46	COM	None	None	None	0	n/a	n/a	n/a	1	1		
46	ESS	Toaster	Unable to clean	Probably a variant of Win32/Kryptik.YQ trojan		Detected	Unable to clean	Probably a variant of Win32/Kryptik.YQ trojan				1
46	FIS	None	None	None		None	None	None				1
46	GTC	Pop-up	Quarantined	internetsecurity2011[1].exe		n/a	n/a	n/a	1	1		

46	KPU	None	None	None		None	None	None				1
46	MTP	None	None	None	0	n/a	n/a	n/a				1
46	N360	Toaster	Blocked	bb75.co.cc	0	n/a	n/a	n/a	1	1		
46	PIS	None	None	None	0	n/a	n/a	n/a				1
46	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
46	WBR	Pop-up	Blocked	InternetSecurity2011[1].exe; us5rinit.exe;	0	n/a	n/a	n/a	1	1		
47	AVI	Pop-Up	Access Denied	HEUR/HTML.Malware[heuristic]		n/a	n/a	n/a	1	1		
47	BDF	Pop-up	Disinfected	Exploit.CVE-2010-1885.c/ Gen:Variant.Kazy.7997		n/a	n/a	n/a	1	1		
47	COM	None	None	None	0	n/a	n/a	n/a	1	1		
47	ESS	Toaster	Quarantined	a variant of Win32/Kryptik.JPK trojan; PDF/Exploit.Pidief.PFO.Gen trojan		n/a	n/a	n/a	1	1		
47	FIS	Browser and Toaster	Removed	Gen:Variant.Kazy.7997		n/a	n/a	n/a	1	1		
47	GTC	Pop-up	Quarantined	JS:Downloader-AKT[Trj](Engine-B); JS:Pdfka-gen[Expl](Engine-B)		n/a	n/a	n/a	1	1		
47	KPU	Toaster	Access Denied	HEUR:Trojan-Downloader.Script.Generic		n/a	n/a	n/a	1	1		
47	MTP	None	None	None	0	n/a	n/a	n/a				1
47	N360	Toaster	Blocked	HTTP Java Obe Toolkit Activity 1	0	n/a	n/a	n/a	1	1		
47	PIS	None	Blocked	HELPCTR.EXE		n/a	n/a	n/a	1	1		
47	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
47	WBR	Browser	Blocked	http://www.12zodic.com/	0	n/a	n/a	n/a	1	1		
48	AVI	Pop-up	Blocked	esymi.exe		n/a	n/a	n/a	1	1		
48	BDF	Pop-up	Disinfected	Gen:Variant.Kazy.2046		n/a	n/a	n/a	1	1		
48	COM	None	None	None	0	n/a	n/a	n/a	1	1		
48	ESS	Toaster	Quarantined	PDF/Exploit.Pidief.PDS.Gen trojan; Kryptik.IUD trojan		n/a	n/a	n/a	1	1		
48	FIS	Browser and Toaster	Removed	Exploit.PDF-JS.Gen; Gen:Variant.Kazy.2046		n/a	n/a	n/a	1	1		

48	GTC	Pop-up	Quarantined	JS:Pdfka-gen[Expl](Engine-B); VBS:Agent-FS[Trj](Engine-B); Gen:Variant.Kazy.2046(Engine-A)		n/a	n/a	n/a	1	1		
48	KPU	Toaster	Access Denied	HEUR:Exploit.Script.Generic		n/a	n/a	n/a	1	1		
48	MTP	None	None	None	0	None	None	None			1	
48	N360	Toaster	Blocked	MSIE Microsoft Windows Help Center Remote Code Exec	0	n/a	n/a	n/a	1	1		
48	PIS	Toaster	Blocked	EXUW.EXE x2; HELPCTR.EXE;		None	None	None			1	
48	TTM	None	Blocked	endlgvktjsys.pdf		n/a	n/a	n/a	1	1		
48	WBR	Browser	Blocked	http://www.kopfzentrum-hno-duesseldorf.de/links.html	0	n/a	n/a	n/a	1	1		
49	AVI	Pop-up	Quarantined	TR/Obfuscated.29996C [trojan]/		n/a	n/a	n/a	1	1		
49	BDF	None	None	None		Detected	Quarantined	Exploit.PDF-JS.Gen			1	
49	COM	None	None	None	0	n/a	n/a	n/a	1	1		
49	ESS	Toaster	Quarantined	PDF/Exploit.Pidief.PDS.Gen trojan		n/a	n/a	n/a	1	1		
49	FIS	Browser, Pop-up and Toaster	Removed	Exploit.PDF-JS.Gen; Foxit PDF		n/a	n/a	n/a	1	1		
49	GTC	Pop-up	Quarantined	HTML:Iframe-inf(Engine-B)		Detected	Disinfected/ Log only	VBS:Agent-FS[Trj](Engine-B); Exploit.PDF-JS.Gen(Engine-A)			1	
49	KPU	Toaster	Access Denied	HEUR:Exploit.Script.Generic		n/a	n/a	n/a	1	1		
49	MTP	Pop-up	Deleted	W32/Ramnit.a.dr	0	None	None	None			1	
49	N360	None	Blocked	MSIE Microsoft Windows Help Center Remote Code Exec		n/a	n/a	n/a	1	1		
49	PIS	Pop-up	Quarantined	izfwezhzcmk[1].exe x2;		n/a	n/a	n/a	1	1		
49	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
49	WBR	Browser	Blocked	http://www.world-of-worcraft-tipps.de/	0	n/a	n/a	n/a	1	1		
50	AVI	Toaster	Blocked	\Ybyq\yczy		n/a	n/a	n/a	1	1		
50	BDF	Pop-up	Blocked	Exploit.CVE-2010-1885.C		n/a	n/a	n/a	1	1		

50	COM	Pop-up and Toaster	Isolated then Deleted	TrojWare.Win32.PkdKrap.ai2@119075059; 0.6295285901288459.exe	0	n/a	n/a	n/a	1	1		
50	ESS	Toaster	Quarantined	PDF/Exploit.Pidief.PFO.Gen trojan; variant of Win32/Kryptik.JOM trojan		n/a	n/a	n/a	1	1		
50	FIS	Browser	Blocked	Harmful web site		n/a	n/a	n/a	1	1		
50	GTC	Pop-up	Access Denied	JS:ScriptDC-inf [Trj](Engine-B); JS:Downloader-AKT[Trj](Engine-B)		Viruses detected	Quarantined	JS:Pdfka-gen[Expl](Engine-B); VBS:Agent-FS[Trj](Engine-B)			1	
50	KPU	Toaster	Access Denied	HEUR:Trojan-Downloader.Script.Generic		n/a	n/a	n/a	1	1		
50	MTP	None	None	None	0	None	None	None			1	
50	N360	Toaster	Blocked	HTTP Java Obe Toolkit Activity 1	0	n/a	n/a	n/a	1	1		
50	PIS	None	Blocked	Explorer.exe; 0.1449799909646996.exe		n/a	n/a	n/a	1	1		
50	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
50	WBR	Pop-up	Blocked	0.7358801601033361.exe	0	n/a	n/a	n/a	1	1		
51	AVI	Toaster	Access Denied	HTML/Crypted.Gen[virus]		None	None	None				1
51	BDF	None	None	None		n/a	n/a	n/a	1	1		
51	COM	Toaster	Isolated then Deleted	InternetSecurity2011[1].exe	0	n/a	n/a	n/a	1	1		
51	ESS	Toaster	Quarantined	JS/TrojanDownloader.Agent.NUH trojan		n/a	n/a	n/a	1	1		
51	FIS	None	None	None		None	None	None				1
51	GTC	Toaster	Quarantined	HTML:Iframe-EP [Trj](Engine-B)		n/a	n/a	n/a	1	1		
51	KPU	Browser	Access Denied	Trojan.JS.Agent.bpb		n/a	n/a	n/a	1	1		
51	MTP	None	None	None	0	n/a	n/a	n/a				1
51	N360	Toaster	Blocked	id32.co.cc	0	n/a	n/a	n/a	1	1		
51	PIS	None	None	None	0	n/a	n/a	n/a				1
51	TTM	None	Blocked	None	0	n/a	n/a	n/a	1	1		
51	WBR	Pop-up	Blocked	InternetSecurity2011[1].exe; us5rinit.exe;	0	n/a	n/a	n/a	1	1		
52	AVI	Toaster	Blocked	\userinit.exe		None	None	None				1
52	BDF	None	None	None		n/a	n/a	n/a	1	1		

52	COM	None	None	None	0	n/a	n/a	n/a	1	1		
52	ESS	Toaster	Unable to clean	Probably a variant of Win32/Kryptik.YQ trojan		Infection detected	Unable to clean	Probably a variant of Win32/Kryptik.YQ trojan				1
52	FIS	Browser	Blocked	Harmful web site		n/a	n/a	n/a	1	1		
52	GTC	Pop-up	Quarantined	userinit.exe		n/a	n/a	n/a	1	1		
52	KPU	Toaster	Neutralized	All threats		None	None	None				1
52	MTP	Pop-up	Removed	JS/Wonka	0	n/a	n/a	n/a	1	1		
52	N360	Toaster	Blocked	id199.co.cc	0	n/a	n/a	n/a	1	1		
52	PIS	None	None	None	0	Resolved	Quarantined	shsvcs.dll			1	
52	TTM	None	Blocked	None	0	n/a	n/a	n/a	1	1		
52	WBR	Browser	Blocked	http://www.busavill.atspace.biz/resource1814.ht	0	n/a	n/a	n/a	1	1		
53	AVI	Pop-up	Access Denied	HTML/Infected.Webpage.Gen[virus]		Malware found	Quarantined	HTML/Infected.Webpage.Gen[virus]			1	
53	BDF	Pop-Up	Disinfected	Exploit.PDF-JS.Gen		None	None	None				1
53	COM	None	None	None	0	n/a	n/a	n/a	1	1		
53	ESS	Toaster	Quarantined	PDF/Exploit.Pidief.PDS.Gen trojan		None	None	None				1
53	FIS	Browser	Blocked	Harmful web site		n/a	n/a	n/a	1	1		
53	GTC	Pop-Up	Quarantined	JS:Illredir-DK[Trj](Engine-B); JS:Downloader-AKU[Trj](Engine-B); JS:Pdfka-gen[Expl](Engine-B); JS:ScriptDC-inf[Trj](Engine-B);		n/a	n/a	n/a	1	1		
53	KPU	Toaster	Access Denied	HEUR:Exploit.Script.Generic		n/a	n/a	n/a	1	1		
53	MTP	None	None	None	0	n/a	n/a	n/a				1
53	N360	Toaster	Blocked	HTTP Phoenix Toolkit Activity 3	0	n/a	n/a	n/a	1	1		
53	PIS	None	Blocked	HELPCTR.EXE x2		n/a	n/a	n/a	1	1		
53	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
53	WBR	Browser	Blocked	http://www.insectcamp.org/	0	n/a	n/a	n/a	1	1		
54	AVI	None	Access Denied	TR/Crypt.ZPACK.Gen[trojan]		n/a	n/a	n/a	1	1		
54	BDF	Pop-up	Disinfected	Gen:Variant.Zbot.6		n/a	n/a	n/a	1	1		
54	COM	Pop-up	Send to Sandbox	Windows-Defender 2012 Installer (OVZfQFar[1].exe); defender.exe;	0	None	None	None			1	

54	ESS	Toaster	Quarantined	Variant of Win32/Kryptik.CU trojan		n/a	n/a	n/a	1	1		
54	FIS	Browser	Blocked	Harmful web site		n/a	n/a	n/a	1	1		
54	GTC	Pop-Up	Quarantined	JS:Pdfka-gen[Expl](Engine-B); Gen:Variant.Zbot.6(Engine-A); JS:Downloader-AHR [Trj] (Engine-B)		n/a	n/a	n/a	1	1		
54	KPU	None	None	None		None	None	None				1
54	MTP	None	None	None	0	None	None	None				1
54	N360	Toaster	Blocked	HTTP Malicious Toolkit Variant Activity 7	0	n/a	n/a	n/a	1	1		
54	PIS	None	Quarantined	defender.exe		None	None	None			1	
54	TTM	None	Blocked	None		n/a	n/a	n/a	1	1		
54	WBR	Browser	Blocked	http://www.getmilfs.com/graduation.html	0	n/a	n/a	n/a	1	1		

APPENDIX D: TOOLS

Ebtables
http://ebtables.sourceforge.net
The ebtables program is a filtering tool for a bridging firewall. It can be used to force network traffic transparently through the Squid proxy.

Fiddler2
www.fiddlertool.com
A web traffic (HTTP/S) debugger used to capture sessions when visiting an infected site using a verification target system (VTS).

HTTPREPLAY
http://www.microsoft.com
A SOCKTRC plug-in enabling the analysis and replaying of HTTP traffic.

Process Explorer
http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx
Process Explorer shows information about which handles and DLLs processes have opened or loaded. It also provides a clear and real-time indication when new processes start and old ones stop.

Process Monitor
http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx
Process Monitor is a monitoring tool that shows real-time file system, Registry and process/thread activity.

Regshot
http://sourceforge.net/projects/regshot
Regshot is an open-source Registry comparison utility that takes a snapshot of the Registry and compares it with a second one.

Squid
www.squid-cache.org
Squid is a caching web proxy that supports HTTP, HTTPS, FTP and other protocols.

Tcpdump
www.tcpdump.org
Tcpdump is a packet capture utility that can create a copy of network traffic, including binaries.

TcpView
http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx
TcpView displays network connections to and from the system in real-time.

Windows Command-Line Tools
Those used included 'systeminfo' and 'sc query'. The systeminfo command "enables an administrator to query for basic system configuration information". The sc command is "used for communicating with the NT Service Controller and services.

Wireshark
www.wireshark.org
Wireshark is a network protocol analyzer capable of storing network traffic, including binaries, for later analysis.

Appendix E: Testing Terms

The following details describe the working relationship between Dennis Technology Labs and the test's sponsor, as well as answering some common questions asked about how the test was conducted.

- Who commissioned this test?

This test was requested by Symantec, which paid Dennis Technology Labs to perform the work and produce the report.

- When was the test conducted?

The test rounds were conducted between 14/12/2010 and 11/01/2011 using the most up to date versions of the software available on any given day.

- Was a live internet connection used?

Yes. All products were able to communicate with their back-end systems over the internet, downloading updates and making cloud-based transactions where appropriate.

- Who chose the products tested?

The products selected for this test were chosen by Symantec.

- Who chose the malicious websites and legitimate software?

Malicious samples were located and verified by Dennis Technology Labs. Unique URLs were used, with no repetition of domain names. False positive candidates were also selected by Dennis Technology Labs. The prevalence data for the legitimate applications was provided by Download.com.

- Were the malicious URLs used as soon as they were verified?

Products were exposed to threats within 24 hours of the same threats being verified. In practice there was usually a delay of no more than three to four hours.

- Did Dennis Technology Labs give any special information to the sponsor during and after the test?

The organization that commissions a test receives full logs for each test round, including product logs, network capture files and system monitoring logs. These logs and details of the malware samples, including their URLs and code, are provided to the organization only after the test is fully complete.

- How accurate or reliable is this sort of test?

We employed exactly the same testing methods as those used in a test we ran last year called *PC Virus Protection 2010 II*[2]. This report was analyzed by the Anti-Malware Testing Standards Organization (AMTSO) and was found to be 100 per cent compliant with AMTSO's Fundamental Principles of Testing[3].

- Was the malware sample selection statistically valid?

There is no known way to know for certain what the corpus of live malware is at any one time. The threats used in this test existed for the day on which they were used. Furthermore, regular internet users visited the malicious or infected sites on that same day. This means that not only were the threats real, but that computers belonging to members of the public were being exposed to them. Our results show what would have happened to those people's PCs had they been running computers loaded with the same software and security products as those used in the test.

[2] http://www.dennistechnologylabs.com/reports/s/a-m/symantec/DTL_PCVP2011_SYMC.pdf
[3] http://www.amtso.org/documents.html