

PC Virus Protection 2010 II

A DYNAMIC ANTI-MALWARE COMPARISON TEST (SPONSORED BY SYMANTEC)

Dennis Technology Lab, 26/10/2009
www.DennisTechnologyLabs.com

This test aims to compare the effectiveness of the most recent releases of popular anti-virus software. The list of products includes a selection of commercial and free programs (see below).

A total of 10 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 files exactly as an average user would.

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

The report is an extension of PC Virus Protection 2010, which was released for publication on 29/09/2009. This second report includes the previous data and doubles the number of malicious and false positive samples from 40 of each to 80.

EXECUTIVE SUMMARY

Products tested

Avast! Home Edition 4	McAfee Internet Security 2009
AVG Free AntiVirus (8.5)	Microsoft Security Essentials (beta)
Avira AntiVir Personal – Free Antivirus (9.0)	Norton Internet Security 2010 (Norton 360 4.0)
BitDefender Internet Security 2010	Panda Internet Security 2010
Kaspersky Internet Security 2010	Trend Micro Internet Security 201

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 product to do so. The least effective (Panda Internet Security 2010) allowed more than half of the threats to infect the system. All, however, are effective at allowing legitimate software to run.

Block threats early for best results

The programs that block the threat in the earliest stages are more likely to protect the system than those that detected unusual system behavior and reacted after an infection has started to occur.

Free anti-virus programs compete strongly with commercial products

The test includes four free anti-virus programs. These are free to download, install and use for non-commercial purposes. They lack firewall protection, which is provided by all of the commercial products. However, the results show that it is possible to get better protection when using a free program than by paying for certain other products.

Simon Edwards, Dennis Technology Lab

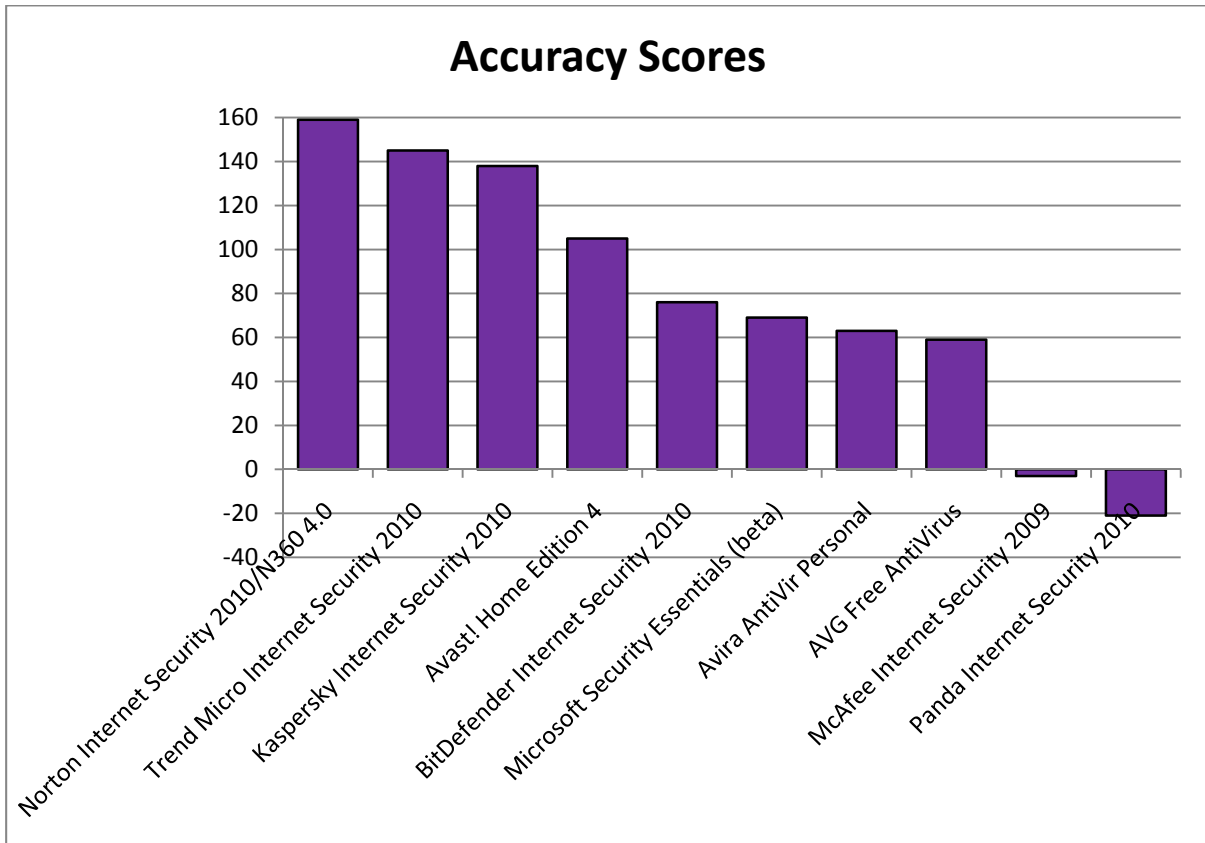
CONTENTS

1. Overall Accuracy	3	Appendix A: Terms	16
Results weighted according to different levels of effectiveness.		Definitions of technical terms used in the report.	
2. Overall Protection	5	Appendix B: Legitimate Samples	17
Combined, un-weighted protection results.		A full list of legitimate products used to test for false positive results.	
3. Protection Details	6	Appendix C: Threat Report	22
Results categorized according to different levels of protection.		Detailed notes about each product's reaction to a sample.	
4. False Positives	7	Appendix D: Tools	68
Results describing how each product handled legitimate software.		Reference to software tools used to run the test.	
5. The Tests	9		
An overview of the testing techniques used.			
6. Test Details	11		
Technical details of the testing methodology.			
7. Conclusions	15		
Observations made during testing and analysis.			

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. In one notable case (Incident #38) the malware was designed to lock down the system in an attempt to blackmail the user for financial gain.



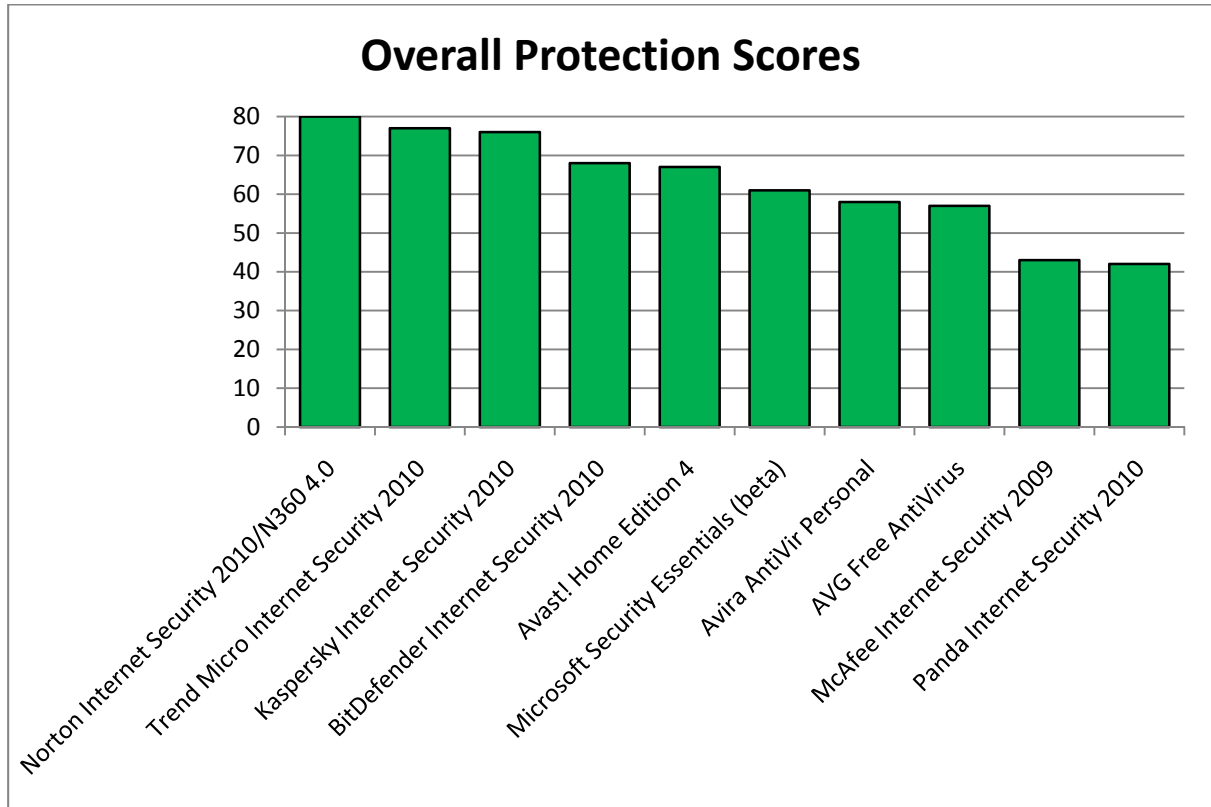
The Norton, Kaspersky and Trend Micro products score highly as they generally defended the system against threats. Panda's product was compromised the most frequently and so its score suffers accordingly.

ACCURACY SCORES

PRODUCT	DEFENDED	NEUTRALIZED	COMPROMISED	ACCURACY
Norton Internet Security 2010/N360 4.0	79	1	0	159
Trend Micro Internet Security 2010	74	3	3	145
Kaspersky Internet Security 2010	70	6	4	138
Avast! Home Edition 4	64	3	13	105
BitDefender Internet Security 2010	32	36	12	76
Microsoft Security Essentials (beta)	46	15	19	69
Avira AntiVir Personal	49	9	22	63
AVG Free AntiVirus	48	9	23	57
McAfee Internet Security 2009	28	15	37	-3
Panda Internet Security 2010	13	29	38	-21

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.

OVERALL PROTECTION SCORES

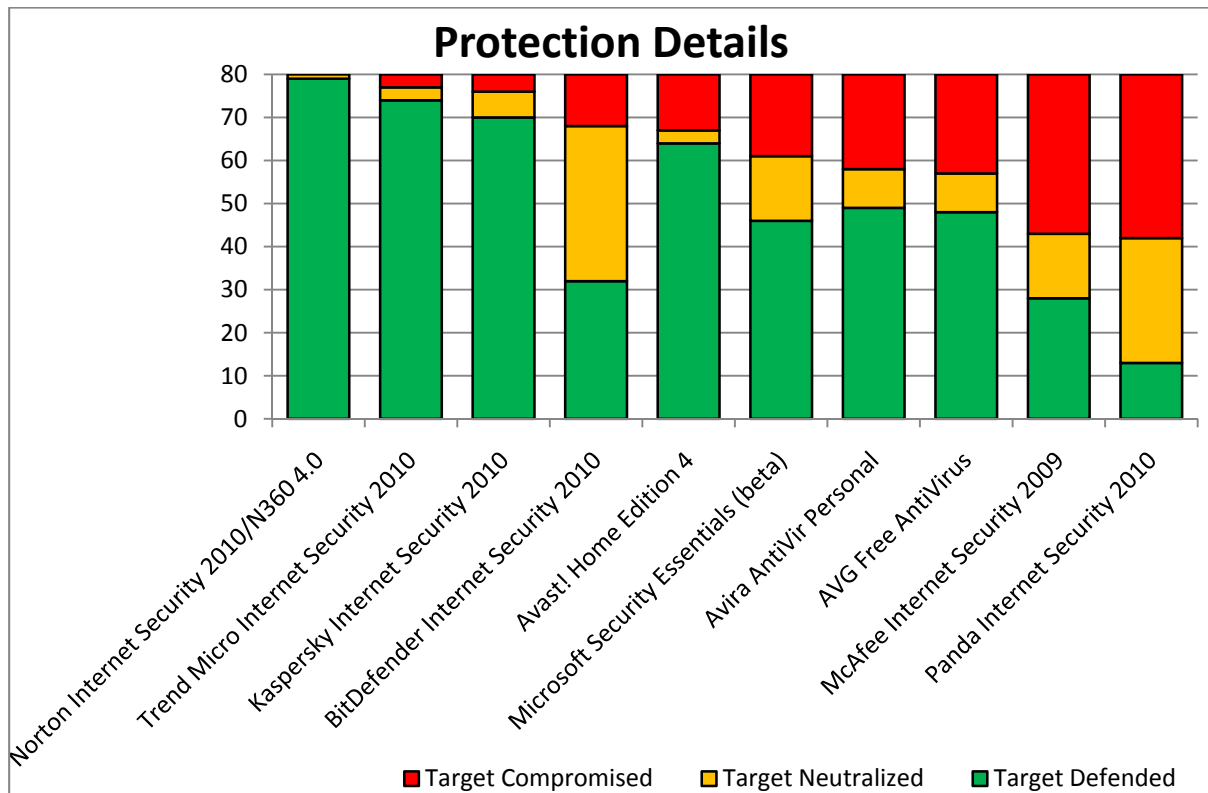
PRODUCT	COMBINED PROTECTION SCORE	PERCENTAGE
Norton Internet Security 2010/N360 4.0	80	100%
Trend Micro Internet Security 2010	77	96%
Kaspersky Internet Security 2010	76	95%
BitDefender Internet Security 2010	68	85%
Avast! Home Edition 4	67	84%
Microsoft Security Essentials (beta)	61	76%
Avira AntiVir Personal	58	73%
AVG Free AntiVirus	57	71%
McAfee Internet Security 2009	43	54%
Panda Internet Security 2010	42	53%

(Average: 78 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 successful products defended rather than neutralized the threats. The least effective hardly defended any of the threats and, when successful, neutralized them instead.



In general the most successful products prevented threats before they could start to interfere with the system.

PROTECTION DETAILS

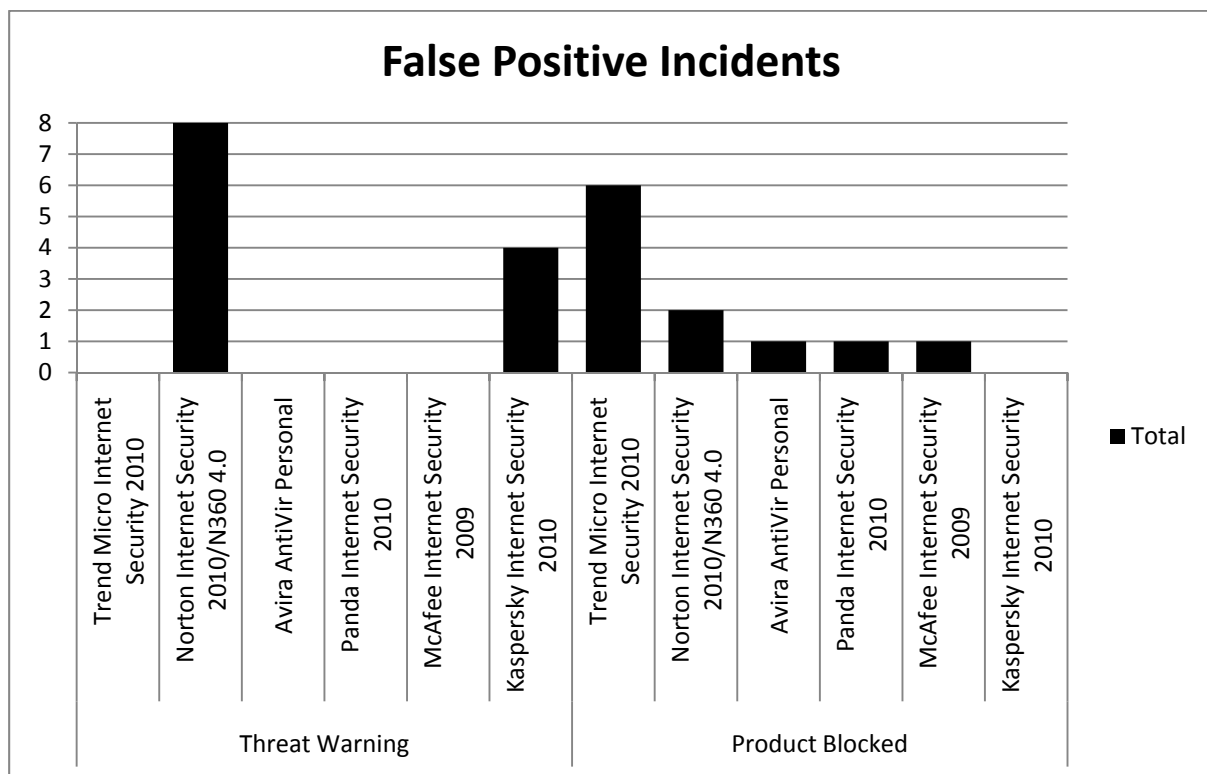
PRODUCT	DEFENDED	NEUTRALIZED	COMPROMISED
Norton Internet Security 2010/N360 4.0	79	1	0
Trend Micro Internet Security 2010	74	3	3
Kaspersky Internet Security 2010	70	6	4
BitDefender Internet Security 2010	32	36	12
Avast! Home Edition 4	64	3	13
Microsoft Security Essentials (beta)	46	15	19
Avira AntiVir Personal	49	9	22
AVG Free AntiVirus	48	9	23
McAfee Internet Security 2009	28	15	37
Panda Internet Security 2010	13	29	38

4. FALSE POSITIVES

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. Their number is low, as is the number of false positives they generated. As we'll see, the false positives were usually generated for rarely-encountered legitimate software.

The Norton product misclassified programs or detected suspicious behavior more frequently than its competitors. More often than not it warned about software rather than blocking it. Eight programs were classified this way, but were able to run regardless.



False positives were rare and those generated by the Norton product were more advisory in tone than Trend Micro Internet Security 2010's automatic blocking.

FALSE POSITIVE INCIDENTS

PRODUCT	THREAT WARNING	PRODUCT BLOCKED
Avira AntiVir Personal	0	1
Kaspersky Internet Security 2010	4	0
McAfee Internet Security 2009	0	1
Norton Internet Security 2010/N360 4.0	8	2
Panda Internet Security 2010	0	1
Trend Micro Internet Security 2010	0	6

The prevalence of each file is significant. If a product misclassified a common file then the situation would be more serious than if it failed to detect a less common one. That said, it is usually expected 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 as reported by sites including Download.com at the time of testing. The ranges for these categories are recorded in the table below:

FALSE POSITIVE CATEGORY RANGES

CATEGORY	PREVALENCE
Very High Impact	> 1m downloads
High Impact	> 500k downloads
Medium Impact	> 100k downloads
Low Impact	> 50k downloads
Very Low Impact	< 50k downloads

FALSE POSITIVE CATEGORY FREQUENCIES

CATEGORY	FREQUENCY
High Impact	2
Low Impact	5
Medium Impact	14
Very High Impact	21
Very Low Impact	38

FALSE POSITIVE RESULTS BY CATEGORY

CATEGORY	NUMBER OF FALSE POSITIVES
Very Low Impact	17
Very High Impact	3
High Impact	1
Low Impact	1
Medium Impact	1

Of the products that generated false positives, Avira AntiVir Personal, McAfee Internet Security 2010 and Panda Internet Security 2010 produced the fewest, all blocking just one file each. McAfee's product generated a false positive on a file categorised in the **Medium Impact** group, while Avira and Panda's software each misclassified a **Very Low Impact** file.

Kaspersky Internet Security generated warnings about four files. These were from a number of groups, one each from **Very Low Impact**, **Low Impact**, **High Impact** and **Very High Impact**.

Trend Micro Internet Security 2010 blocked six files, all but one of which were in the **Very Low Impact** category. The remaining file was categorized as **Very High Impact**.

The Norton product generated the most false positives overall, warning against eight files and blocking two. All of these legitimate programs were categorized as **Very Low Impact**.

5. THE TESTS

4.1 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 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.

4.2 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 were 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.

12	PIS	None	None	None
12	TIS	None	See note	None
13	AVA	Pop-up	Move to chest	VBS:Obfuscated-gen [Trj]
13	AVG	Pop-up	Threat detected	Win32/Heur
13	AVI	Pop-up	Deny access	Multiple - see notes
13	BDF	Pop-up	Multiple - see notes	Blocked
13	KIS	Browser	Blocked	HEUR:Trojan.Script.Iframer
13	MIS	Browser	Blocked	None
13	MSE	Pop-up	Suspended	PWS:Win32/Uloadis.A
13	NIS	None	None	None
13	PIS	None	None	See notes
13	TIS	None	None	None
14	AVA	Toaster	Blocked	None
14	AVG	Pop-up	Threat detected	Exploit link to known exploit site

Each 'round' exposed every product to one specific threat. The set of records for round 13 (above) shows a range of responses to a particular threat. In this example the Norton (NIS) and Trend (TIS) products did not display any alert, although they protected the system. Panda (PIS), on the other hand, failed to protect the system, which was so badly infected that it became completely unusable.

4.3 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.

4.4 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 might be able to 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 be able to bypass the security product and carry out its malicious tasks unhindered. It may even be 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.

4.5 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

5.1 The targets

To create a fair testing environment, each product was installed on a clean Windows XP Professional target system. The operating system was updated with Windows XP Service Pack 2 (SP2), although no later patches or updates were applied. The high prevalence of internet threats that rely on Internet Explorer 6, and other vulnerable Windows components that have been updated since SP2 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. Microsoft Security Essentials required one update (Windows Installer 3.1) and automatically re-enabled Windows Automatic Updates. This was disabled immediately.

A selection of legitimate but old software was pre-installed on the target systems. These posed security risks, as they contained known vulnerabilities. They include 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. Some products automatically upgraded themselves during the test. 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.

5.2 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 malicious websites. In all cases, a control system (Verification Target System - VTS) was used to confirm that the URLs linked to actively malicious sites.

5.3 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 E: 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 **5.6 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 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.

5.4 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 appear 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 caching proxy set to 'offline' mode and a web replay system. When the first target system visited a site, the page's content, including malicious code, was downloaded and stored. When each consecutive target system visited the site, it should have received the same content, with some provisos.

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.

5.5 Secondary downloads

Established malware may attempt to download further files (secondary downloads), which will also be cached by the proxy 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 HTTPS or a non-web protocol such as FTP or
2. A different filename is requested each time (e.g. `badfile2.exe`; `random357.exe`) or
3. The same filename is requested over HTTP but the file has been modified on the web server. In this case even the original download may differ between target systems

5.6 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 included 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.

5.7 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 **5.3 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 have been 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.

5.8 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 DTL-created scripts were also used to provide additional system information. Each product was 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 the 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. Further to that, all web traffic had to pass through the proxy as well. This allowed the tester 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 transparent router, passing all web traffic through a Squid proxy. This was configured in 'offline' mode during testing, with additional rules to prevent access to certain Microsoft update sites.

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.

5.9 False positives

A useful security product is able to block threats and allow useful program to install and run. The products were also tested to see how they would respond to legitimate applications. We selected files that fell into the five categories below.

CATEGORY	PREVALENCE
Very High Impact	> 1m downloads
High Impact	> 500k downloads
Medium Impact	> 100k downloads
Low Impact	> 50k downloads
Very Low Impact	< 50k downloads

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

For details on the frequency of files in each category see **4.5 False positive categories**.

7. CONCLUSIONS

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 from a legitimate website that had been compromised by an attacker. This means that the old advice of, “keep away from the dark parts of the internet” is out of date. It further demonstrates that effective anti-virus software is essential for those who want to use the web using a Windows PC, whether they are looking for pornography or information on tea.

The vast majority of the threats installed automatically when a user visited the infected webpage. This infection was usually invisible to a casual observer and rarely did the malware make itself known, unless it was installing a fake anti-virus program. These rogue applications pretend to detect viruses on the system and harass the user into paying for a full license, which the program claims will allow it to remove the ‘infections’. In reality the only infection is the fake anti-virus program itself.

Where does protection start?

The best-performing products were Norton Internet Security 2010/N360 4.0, Kaspersky Internet Security 2010 and Trend Micro Internet Security 2010. These three had one notable similarity: they all blocked threats early in the attack process, which meant that there was less opportunity for the malware to infect the systems. Avast! Home Edition worked in a similar way, although it was compromised more often.

The four least effective products usually allowed the malware to start interacting with the system before they detected anything amiss. Sometimes they would detect infected files that the malware downloaded or recognize other suspicious behavior. Even when these products were able to prevent a lasting infection, some malicious files often remained on the system’s hard disk. While we did not count this as a compromise, it’s not an ideal situation.

Sorting the wheat from the chaff

The false positive results were generally low, which shows that none of the products are tuned too aggressively to detect and block malware at the expense of regular programs.

Norton Internet Security 2010/N360 4.0 is an interesting case in that it uses a reputation-based system to help classify files. A file that has rarely been encountered by other Norton users (a large community) is considered more suspect than one that has been proven to be innocent or is more commonly encountered. In eight out of the ten false positives generated by this product, a user who was confident that they were installing legitimate software would have been able to carry on unhindered.

Trend Micro Internet Security 2010 was more aggressive and removed or blocked the misclassified legitimate software automatically six times.

Anti-virus is important (but not a panacea)

This test shows that there is a significant difference in 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 the average protection level is 78 per cent (**see 2. Overall protection**), which is at odds with marketing claims made by some anti-virus companies. It also contradicts other third-party tests that claim regularly that the majority of desktop products are capable of detection rates around the 90-100 per cent mark.

APPENDIX A: 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	RealVNC Free Edition	Remote control	www.realvnc.com
2	TeamViewer 4.1.6597	Remote control	Download.com
3	Advanced IP Scanner 1.5	Network scanner	Download.com
4	LogMeIn Free 4.0.966	Remote control	Download.com
5	Tor - Installation bundle for Windows	Anonymization	www.torproject.org
6	Keystroke Interference 2.1	Anti-keylogger	Softpedia.com
7	Radmin Viewer 3.3	Remote control	Download.com
8	WinZip 12.1 build 8519	File compression	Download.com
9	WebDrive 9.0.2199	Network storage	Download.com
10	PingFu Iris A7033	Anonymization	Download.com
11	Technitium MAC Address Changer 5.0 Release 3	Network tool	Download.com
12	UPX Version 3.04	Development tool	SourceForge.net
13	ActiveX Download Control 3.12	Development tool	Download.com
14	PSTools	System utility	Microsoft.com
15	Brightfilter Parental Control 2009 2.1.0.10	Parental control	Download.com
16	Unipeek MSN Monitor 2.0 build 321	Network monitoring	Download.com
17	mIRC	Internet chat	CSH cover disc
18	ZSNES	Games emulator	SourceForge.net
19	AutoHotkey 1.0.48.05	Automation	Download.com
20	Auto Clicker Typer 1.0	Automation	www.asoftwareplus.com
21	DeSmuME 0.9.4	Games emulator	SourceForge.net
22	Service+ CL 1.2.7	System utility	Softpedia.com
23	Ausun Scheduler 1.5	Automation	Softpedia.com

24	ECCS 1.0.0	Time management	Softpedia.com
25	Registry Trash Keys Finder 3.8.1.3	System utility	Softpedia.com
26	Active@ Disk Monitor 1.5.20	System utility	Softpedia.com
27	MING Network Monitor Home 2.5	Network monitoring	http://network.mingsoft.com
28	CommView 6.1	Network monitoring	Soft32.com
29	Auslogics Task Manager 1.5.5	System utility	Soft32.com
30	Iranian singles 1.0	Browser Toolbar	Soft32.com
31	SEO Optimization 1.0	Browser Toolbar	Soft32.com
32	Advanced Privacy Cleaner Bar 1.0.2	Browser Toolbar	Soft32.com
33	RadarSync Toolbar for IE 4.5.193.7	Browser Toolbar	Soft32.com
34	Self Defense Products 1.0	Browser Toolbar	Soft32.com
35	Hot Keyboard Pro 3.1.597	Automation	Download.com
36	Perfect Macro Recorder 1.5	Automation	Download.com
37	Pusher 5.2.7	Automation	www.fortypoundhead.com
38	Flashpaste Professional 4.5	Automation	Download.com
39	Tidy Favorites 4.15	Browser Toolbar	www.tidyfavorites.com
40	AutoIT 3.3.0.0	Automation	www.autoitscript.com
41	Google Maps Downloader 6.06	Mapping	Download.com
42	Cheetah YouTube Downloader 1.23	Download videos and save them as MP3, MP4, FLV, Audio CD and Video DVD	Download.com
43	Rapid Typing Tutor 2.9.7	Improve your typing skills.	Download.com
44	Unlocker 1.8.7	Avoid getting deletion error messages.	Download.com
45	Ghost Mouse 2	Automate mouse clicks.	Download.com

46	NeoDownloader Lite 2.1c	Download and view lots of pictures from Web sites.	Download.com
47	YADA (Yet Another Download Accelerator) 1.1	Protect, resume, and speed up your downloads.	Download.com
48	PicBlock 3	Prevent pornographic images from displaying.	Download.com
49	SmartHide 2.1.121	Stay invisible when surfing the Internet.	Download.com
50	WinPing 1.5.3553	Test your Internet connection.	Download.com
51	Dream Computer Piano 1.04	Turn your computer into piano.	Download.com
52	TrojanHunter 5.2 Build 988	This program searches for and removes trojans from your system	Softpedia.com
53	WorldTime2000 7.5	View the time in any location in the world	Download.com
54	Dink Smallwood 1.06	Travel across mystical lands and explore dark caverns in this Zelda-like RPG	Download.com
55	Token 2 2.9.5	Connect your computer to the host using Winsock Telnet client or dial-up modem terminal.	Download.com
56	CiDial 2.3	Reconnect automatically when you get disconnected from the Internet.	Download.com
57	SWF2Video 1.1	Convert Flash movies to video files.	Download.com

58	CZ-Doc2Pdf 2.0	Convert new uploading Word, RTF, text, or HTML documents to PDF files automatically.	Download.com
59	PHP Expert Editor 3.2.1	Run, test, and debug PHP scripts.	Download.com
60	Embroid 2008 build 8.4	Organize, convert, and view your designs before embroidering, and print relative documentation.	Download.com
61	Advanced Registry Optimizer 5.1	Back up, clean, and optimize your Windows registry	Download.com
62	HoosThere 0.1	A simple to use and install IM software.	Softpedia.com
63	Batch Chat 1.0	A handy chat tool	Softpedia.com
64	MRICroGL 1	An intuitive viewer for medical images	Softpedia.com
65	ImageWatcher 1.0	Automatically display, full screen, images that are downloaded from your camera	Softpedia.com
66	LimeWire	Share files online.	Download.com
67	Advanced SystemCare Free 3.3.4	Protect, repair, optimize, and clean your computer in one click.	Download.com
68	Camfrog Video Chat 5.3.215	Join live-video chat rooms from around the world.	Download.com
69	PrimoPDF 5.0.0.19	Print to PDF from Windows applications and optimize the PDF output.	Download.com














70	RealPlayer 11	Play audio and video files with a media player that lets you mix, rip, and burn CDs and MP3s fast.	Download.com
71	Adobe Reader 9.1	View, navigate, and print PDF files.	Download.com
72	Internet Download Manager 5.18 build 3	Increase your download speed and recover broken downloads.	Download.com
73	CCleaner 2.24.1010	Clean up junk files and invalid Registry entries.	Download.com
74	AntiLogger 1.9.2.159	Protect your PC against viruses, rootkits, and malware.	Download.com
75	IrfanView 4.25	View and edit most graphics formats in a fast and simple way.	Download.com
76	DivX 7 for Windows 7.2	Install the latest DivX codec and player and free your HD media	Download.com
77	UltraISO Premium 9.3.5.2716	Extract, edit, and create CD or DVD image files and make bootable CDs and DVDs.	Download.com
78	A-ToolBar 3.01	Access 45 tools from the desktop toolbar.	Download.com
79	Asmw Eraser Pro 3.5.6	Clean up traces of your online and computer activities.	Download.com
80	O&O DiskRecovery 4.1	Find and reconstruct your lost and destroyed files.	Download.com

APPENDIX C: THREAT REPORT

Code	Product	Code	Product	Code	Product
AVA	Avast! Home Edition 4	KIS	Kaspersky Internet Security 2010	PIS	Panda Internet Security 2010
AVG	AVG Free AntiVirus (8.5)	MIS	McAfee Internet Security 2009	TIS	Trend Micro Internet Security 2010
AVI	Avira AntiVir Personal – Free Antivirus (9.0)	MSE	Microsoft Security Essentials		
BDF	BitDefender Internet Security 2010	NIS	Norton Internet Security 2010		

NOTE: The following table is a summary. The full report was provided to Symantec as an Excel spreadsheet, which includes the 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.

Incident	Product code	Introduction			Manual Scan			Complete Remediation	Defended	Neutralized	Compromised
		Alert	Effect	Threat Report	Alert	Effect	Threat Report				
1	AVA	Toaster	Blocked	Network Shield	n/a	n/a	n/a				
1	AVG	Pop-up	Moved to Vault	Win32/Cryptor	None	None	None				
1	AVI	Pop-up	Deny access	WORM/IrcBot.60416.6 worm	n/a	n/a	n/a				
1	BDF	Pop-up	Terminated	Deemed harmful by Active Virus Control	Report	Quarantined	Exploit.PDF-JS.Gen				
1	KIS	Toaster	Blocked	Phishing URL denied	None	None	None				
1	MIS	Toaster	Blocked	Buffer overflow blocked	None	None	None				
1	MSE	None	None	None	None	None	None				

1	NIS	None	None	None	None	None	None					
1	PIS	Toaster	Blocked	Dangerous operation blocked!	None	None	None					
1	TIS	Browser	Blocked	Blocked	None	None	None					
2	AVA	Toaster	Blocked	Network Shield	n/a	n/a	n/a					
2	AVG	Pop-up	Heal	Trojan horse Sheur BBWU	None	None	None					
2	AVI	Pop-up	Deny access	TR/Fakealert.390144 Trojan	None	None	None					
2	BDF	None	None	None	Report	Detected	Cookies x2					
2	KIS	Toaster	Blocked	Trojan-Downloader NSI.FraudLoad denied	None	None	None					
2	MIS	Toaster	Removed	Trojan removal: Artemis!F3D4237A6630	None	None	None					
2	MSE	Toaster	Clean	Trojan Win32/FakeSmoke	None	None	None					
2	NIS	Toaster	See note	set up [1] exe	None	None	None					
2	PIS	Alert on IE Web page	blocked	Website blocked by Trend Micro Internet Security	Report	Detected	Suspicious file x2					
2	TIS	Browser	Blocked	Blocked	None	None	None					
3	AVA	None	None	None	None	None	None					
3	AVG	None	None	None	None	None	None					
3	AVI	None	None	None	Report	Repair All	EXP/Pidief.gzg					
3	BDF	None	None	None	Report	Detected	Cookies x2					
3	KIS	Toaster	Blocked	Access denied to Exploit.JS.Pdfka.xc	None	None	None					
3	MIS	None	None	None	None	None	None					
3	MSE	None	None	None	None	None	None					
3	NIS	Pop-up	Blocked	MSIE Adobe Reader GetIcon BO critical attack prevented	None	None	None					
3	PIS	None	None	None	None	None	None					
3	TIS	Browser	Blocked	Blocked	None	None	None					
4	AVA	Toaster	Blocked	Win32:Trojan-gen{Other}	None	None	None					
4	AVG	Pop-up	Heal	Multiple - see notes	None	None	None					
4	AVI	Pop-up	Deny access	TR/TDss.aggz Trojan	None	None	None					
4	BDF	Toaster	Blocked	Multiple - see notes	None	None	None					
4	KIS	Toaster	Blocked	Access denied to Trojan.Win32.Tdss.aggz	None	None	None					
4	MIS	None	None	None	None	None	None					

7	AVA	Toaster	Blocked	Malicious site	n/a	n/a	n/a				
7	AVG	Pop-up	Heal	Trojan horse SHeur2.BCJW	None	None	None				
7	AVI	Pop-up	Deny access	Multiple - see notes	None	None	None				
7	BDF	Toaster	Terminated	Deemed harmful by Active Virus Control	Report	Quarantined	Exploit.PDF-JS.Gen				
7	KIS	Toaster	Blocked	Access denied Trojan.Downloader.JS.Major.C	Report	Deleted	Trojans x4				
7	MIS	Toaster	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a				
7	MSE	Toaster	Multiple - see notes	Multiple - see notes	None	None	None				
7	NIS	Toaster	Blocked	HTTP Malicious Toolkit Download Activity	None	None	None				
7	PIS	Toaster	Blocked	Multiple (see notes)	Report	Quarantined	Suspicious file				
7	TIS	None	None	None	None	None	None				
8	AVA	Pop-up	Move to chest	HTML:Iframe-inf	n/a	n/a	n/a				
8	AVG	Pop-up	Removed	Multiple - see notes	None	None	None				
8	AVI	Pop-up	Deny access	Multiple - see notes	None	None	None				
8	BDF	Pop-up	Blocked	Multiple - see notes	Report	Failed to perform any action	Generic.PWStealer.OE96BF1A and .E9ABFACF				
8	KIS	Toaster	Blocked	Access denied Exploit: Win32.DirektShow.DL	None	None	None				
8	MIS	Toaster	Removed	Trojan Exploit M.Direct Show b	None	None	None				
8	MSE	Toaster	Removed	Multiple - see notes	Toaster	Clean	Multiple				
8	NIS	None	None	None	None	None	None				
8	PIS	Toaster	Neutralized	Multiple - see notes	Report	Deleted	Multiple				
8	TIS	None	None	None	None	None	None				
9	AVA	Pop-up	Move to chest	HTML:Iframe-inf	n/a	n/a	n/a				
9	AVG	Pop-up	None	See note	Report	None	Multiple - see note.				
9	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a				
9	BDF	None	None	None	Report	Quarantined	Multiple				
9	KIS	Toaster	Blocked	Multiple - see notes	None	None	None				

9	MIS	Pop-up	Blocked	JS/Tenia.d (Trojan)	Report	Scanned	10 cookies scanned.					
9	MSE	Toaster	Removed	Trojan Downloader: HTML/Iframe.I	None	None	None					
9	NIS	None	See note	None	None	None	None					
9	PIS	Toaster	Blocked	Dangerous operation blocked!	Report	Deleted	Adware					
9	TIS	None	See note	None	None	None	None					
10	AVA	Pop-up	Move to chest	HTML:Iframe-JI [Trj]	n/a	n/a	n/a					
10	AVG	Pop-up	Healed	Trojan horse Generic 14.AHVF	Report	Removed	1 infection					
10	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a					
10	BDF	Pop-up	Blocked	Trojan.Generic.CJ.OYN x4	n/a	n/a	n/a					
10	KIS	Toaster	Blocked	http://adultping.net/index.php	None	None	None					
10	MIS	Toaster	Removed	FakeAlert WinwebSecurity.gen (Trojan) x 2	None	None	None					
10	MSE	Toaster	Removed	Trojan: Win32/Winwebsec	None	None	None					
10	NIS	Toaster	Blocked	HTTP Nine-Ball Mass Injection	None	None	None					
10	PIS	Toaster	Neutralized	Trj/Zlob.KH	n/a	n/a	n/a					
10	TIS	Browser	Blocked	Blocked	None	None	None					
11	AVA	Pop-up	Abort connection	HTML:Script-inf	n/a	n/a	n/a					
11	AVG	Pop-up	Removed	Multiple - see notes	Report	Quarantined	4 cookies					
11	AVI	Pop-up	Deny access		n/a	n/a	n/a					
11	BDF	Pop-up	Blocked	Multiple - see notes								
11	KIS	Toaster	Removed	Trojan-Downloader.JS Iframe.bpz	None	None	None					
11	MIS	None	None	None	None	None	None					
11	MSE	Toaster	Multiple - see notes	Multiple - see notes	None	None	None					
11	NIS	Toaster	Blocked	HTTP Suspicious Domain Request SQL Inject. Auto Protect blocked downloader.	Report	Detected	5 cookies					
11	PIS	Toaster	Blocked	Dangerous operation blocked!	n/a	n/a	n/a					
11	TIS	None	None	None	Report	Detected	5 cookies					
12	AVA	Pop-up	Abort connection	S:Obfuscated-DQ (Trj)	Report	Move to Chest	Multiple					
12	AVG	Pop-up	Removed	Multiple - see notes	None	None	None					

12	AVI	None	None	See notes	None	None	None						
12	BDF	None	None	None	None	None	None						
12	KIS	Pop-up	See note	BEBEGF,EXE	Pop-up	See note	wbhwin32.exe						
12	MIS	Toaster	Removed	Exploit-MS06-014 (Virus)	Report	Scanned	14 cookies						
12	MSE	Toaster	Multiple - see notes	Multiple - see notes	None	None	None						
12	NIS	Pop-up	Blocked - see note	Site is unsafe. Browser threat.	None	None	None						
12	PIS	None	None	None	Report	Quarantined	Multiple						
12	TIS	None	See note	None	None	None	None						
13	AVA	Pop-up	Move to chest	VBS:Obfuscated-gen [Trj]	n/a	n/a	n/a						
13	AVG	Pop-up	Threat detected	Win32/Heur	None	None	None						
13	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a						
13	BDF	Pop-up	Multiple - see notes	Blocked	n/a	n/a	n/a						
13	KIS	Browser	Blocked	HEUR:Trojan.Script.Iframer	None	None	None						
13	MIS	Browser	Blocked	None	n/a	n/a	n/a						
13	MSE	Pop-up	Suspended	PWS:Win32/Uloadis.A	None	None	None						
13	NIS	None	None	None	None	None	None						
13	PIS	None	None	See notes	n/a	n/a	n/a						
13	TIS	None	None	None	Report	Quarantined	Mal_Hifrm-3						
14	AVA	Toaster	Blocked	None	None	None	None						
14	AVG	Pop-up	Threat detected	Exploit link to known exploit site	None	None	None						
14	AVI	Pop-up	Deny access	Multiple - see notes	None	None	None						
14	BDF	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a						
14	KIS	Pop-up	Suspicious activity	Suspicious driver installation	Report	Quarantined	Multiple						
14	MIS	Toaster	Multiple - see notes	Trojan detected	Report	Quarantined	Trojan						
14	MSE	None	None	None	None	None	None						
14	NIS	Browser	Blocked	JS.Downloader	n/a	n/a	n/a						
14	PIS	None	None	None	None	None	None						

14	TIS	None	None	None	None	None	None				
15	AVA	Pop-up	Move to chest	HTML:Iframe-inf	n/a	n/a	n/a				
15	AVG	Pop-up	Removed	Multiple - see notes	None	None	None				
15	AVI	Pop-up	Deny access	Multiple - see notes	Report	** FP **	** FP **				
15	BDF	Pop-up	Blocked	Multiple - see notes	Report	Deleted	Generic.PWStealer.0E96BF1A and .145E4496				
15	KIS	Toaster	Deny access - see note	Exploit Win 32.DirektShow.a	None	None	None				
15	MIS	Toaster	Removed	Exploit-MSDirectShow b	Report	Quarantined	Artemis!57EB775B6C75				
15	MSE	Toaster	Removed	Multiple - see notes	None	See note	None				
15	NIS	None	Blocked - see note	None	None	None	None				
15	PIS	Pop-up	Delete	Exploit/DirektShow.A	Report	Multiple - see notes	Multiple - see notes				
15	TIS	None	See note	None	None	None	None				
16	AVA	Pop-up	Move to chest	JS:ScriptSH-inf [Trj]	n/a	n/a	n/a				
16	AVG	Pop-up	Moved to Vault	JSI Psyme	None	None	None				
16	AVI	Pop-up	Deny access	HTML/Infected.WebPage.Gen HTML script virus	n/a	n/a	n/a				
16	BDF	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a				
16	KIS	Toaster	Denied	Trojan-Clicker.JS.Agent.h	None	None	None				
16	MIS	Toaster	Quarantined	JS Downloader.gen (Trojan)	None	None	None				
16	MSE	Toaster	Removed	Trojan Downloader:JS/Psyme.gen	None	None	None				
16	NIS	Toaster	Removed	c:\documents and settings\victor\local settings\temporary internet files\content.ie5\mfolizal\10[1].swf	Report	Removed	2 tracking cookies				
16	PIS	None	None	None	n/a	n/a	n/a				
16	TIS	None	See note	None	None	None	None				
17	AVA	Toaster	Blocked	Blocked	n/a	n/a	n/a				
17	AVG	Pop-up	Healed	Trojan Horse Sheur2.BCVA	None	None	None				
17	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a				

17	BDF	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a		█	█		
17	KIS	Toaster	Denied	Multiple - see notes	None	None	None			█		
17	MIS	Toaster	See note	Generic Downloader xlbhf (Trojan)	None	None	None				█	
17	MSE	Toaster	Removed	Multiple - see notes	None	None	None			█		
17	NIS	Toaster	See note	Multiple - see notes	None	None	None			█		
17	PIS	Toaster	Neutralized	n/a	Report	Multiple - see notes	Multiple - see notes		█		█	
17	TIS	None	See note	None	None	None	None			█		
18	AVA	Pop-up	Deleted	Trojan Horse HTML: Irame.IE [Trj]	Report	See note	See note				█	
18	AVG	None	See note	None	None	None	None					█
18	AVI	Pop-up	Denied	Multiple - see notes	Report	Repaired	HTML/Crypted.Gen				█	
18	BDF	Multiple - see notes	Multiple - see notes	Multiple - see notes	Report	Quarantined	Exploit.PDF-JS.Gen				█	
18	KIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None			█		
18	MIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None				█	
18	MSE	Toaster	Removed	VirTool:Win32/VBInject.gen!CE	None	None	None			█		
18	NIS	Toaster	Blocked	HTTP Nine-Ball Mass Injection	None	None	None			█		
18	PIS	Toaster	Blocked	mavidctl.dll library	None	None	None			█		
18	TIS	None	See note	None	None	None	None			█		
19	AVA	None	None	None	None	None	None					█
19	AVG	None	None	None	None	None	None					█
19	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a		█	█		
19	BDF	None	None	None	None	None	None					█
19	KIS	Toaster	Denied	Exploit.Win32.DirektShow.a	None	None	None			█		
19	MIS	Toaster	Removed	Exploit-MS DirectShow.b	None	None	None			█		
19	MSE	None	None	None	None	None	None					█
19	NIS	Browser	Blocked	Malicious site	None	None	None			█		
19	PIS	Toaster	Blocked	Dangerous operation blocked!	n/a	n/a	n/a		█			
19	TIS	None	See note	None	Report	Deleted	Cookie: Apmebf			█		
20	AVA	Pop-up	Move to chest	HTML:Iframe-EJ [Trj]	n/a	n/a	n/a		█	█		
20	AVG	Pop-up	Healed	Trojan horse SHeur2.BDJN	None	None	None			█		

20	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a		█	█		
20	BDF	Pop-up	Blocked	Trojan.SWF.Dropper.C	Report	Multiple - see notes	Multiple - see notes					█
20	KIS	Toaster	Denied	Multiple - see notes	None	None	None			█		
20	MIS	Toaster	Blocked and quarantined	Obfuscated Script I (Trojan)	None	None	None				█	
20	MSE	Toaster	Multiple - see notes	Multiple - see notes	None	None	None					█
20	NIS	Toaster	Blocked - see note	HTTP Nine-Ball Mass Injection	None	None	None			█		
20	PIS	Toaster	Blocked	Dangerous operation blocked!	Report	Multiple - see notes	Multiple - see notes					█
20	TIS	Browser	Blocked	Malicious site	None	None	None			█		
21	AVA	Pop-up	Move to chest	HTML:iiiframe-B [Trj]	n/a	n/a	n/a		█	█		
21	AVG	Pop-up	Removed	Trojan horse Dropper Bravix.T	None	None	None			█		
21	AVI	None	None	None	None	None	None					█
21	BDF	Pop-up	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a		█	█		
21	KIS	Toaster	Denied	Trojan Downloader.JS.gen	None	None	None			█		
21	MIS	Toaster	Removed	FakeAlert-DZ (Trojan)	None	None	None			█		
21	MSE	Toaster	Removed	TrojanDownloader: Win32/Waledac.C	None	None	None			█		
21	NIS	None	See note	None	None	None	None			█		
21	PIS	None	None	None	Report	Quarantined	Suspicious file x2					█
21	TIS	None	See note	None	None	None	None			█		
22	AVA	Pop-up	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a		█	█		
22	AVG	Pop-up	Unable to heal	Multiple - see notes	Report	Unable to heal	20 infections					█
22	AVI	Pop-up	Deny access	HEUR/HTML.Malware x6	n/a	n/a	n/a		█	█		
22	BDF	Pop-up	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a		█	█		
22	KIS	Toaster	Denied	Multiple - see notes	None	None	None			█		

22	MIS	Toaster	Blocked and removed	Exploit-Iframe.gen.u; Artemis\ABDB5E6DC349	None	None	None						
22	MSE	Toaster	Removed	Multiple - see notes	None	None	None						
22	NIS	None	See note	None	None	None	None						
22	PIS	Toaster	Multiple - see notes	Multiple - see notes	Report	Quarantined	Suspicious file x3						
22	TIS	None	See note	None	None	None	None						
23	AVA	Pop-up	Move to chest	HTML:Illiframe-B [Trj]	n/a	n/a	n/a						
23	AVG	Pop-up	See note	Multiple - see notes	None	None	None						
23	AVI	Pop-up	Deny access	Multiple - see notes	Report	Found	Hidden objects x2						
23	BDF	Pop-up	Blocked	Dropped:Trojan.Generic.2302214	Report	No action is possible	Multiple - see notes						
23	KIS	Toaster	Denied	HEUR: Trojan.Script.Iframe	None	None	None						
23	MIS	Toaster	Blocked and removed	Exploit.MSDirectShow.b	Report	Detected and quarantined	Artemis!57EB775B6C75						
23	MSE	Toaster	See note	TrojanDownloader: Win32/Bredolab.A	None	None	None						
23	NIS	None	See note	None	None	None	None						
23	PIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None						
23	TIS	None	See note	None	None	None	None						
24	AVA	Toaster	Blocked	Network Shield	n/a	n/a	n/a						
24	AVG	None	See note	None	Report	See note	Multiple - see note						
24	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a						
24	BDF	Pop-up	Blocked	Trojan.SWF.Dropper.Gen	Report	Quarantined	Exploit.PDF-JS.Gen						
24	KIS	Toaster	Denied	http://213.163.89.54/lib/index.php	None	None	None						
24	MIS	Toaster	See note	Multiple - see notes	None	None	None						
24	MSE	Toaster	See note	Multiple - see notes	None	None	None						
24	NIS	None	See note	None	Report	Removed	2 tracking cookies						
24	PIS	Toaster	Blocked	Dangerous operation blocked!	Report	Deleted	systemguard2009						
24	TIS	None	See note	None	Report	Deleted	1 tracking cookie						
25	AVA	Toaster	Blocked	xratedj.com	n/a	n/a	n/a						

















25	AVG	Pop-up	Denied	Trojan horse SHeur2.BEAW	None	None	None					
25	AVI	Pop-up	Deny access	Multiple - see notes	None	None	None					
25	BDF	Toaster	Multiple - see notes	Multiple - see notes	None	None	None					
25	KIS	Toaster	Denied	HEUR: Exploit.Script.Generic	None	None	None					
25	MIS	Toaster	Quarantined	Exploit-CVE 007-0071	Report	Quarantined	Multiple - see note					
25	MSE	Toaster	Removed	Multiple - see notes	None	None	None					
25	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None					
25	PIS	None	None	None	Report	Multiple - see notes	Multiple - see notes					
25	TIS	Toaster	Blocked	Multiple - see notes	Report	Deleted	Cookie Stat Counter					
26	AVA	Toaster	Blocked	http://embrari-1.cn/giri2/index.php	n/a	n/a	n/a					
26	AVG	Pop-up	Healed	Trojan horse Sheur.BDVD	None	None	None					
26	AVI	Pop-up	Denied	Multiple - see notes	Report	Repaired	SWF/Drop.Small.WI					
26	BDF	Toaster	Deleted	Trojan.Generic.CJ.XFO	None	None	None					
26	KIS	Toaster	Neutralized	Multiple - see notes	None	None	None					
26	MIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None					
26	MSE	Toaster	Multiple - see notes	Multiple - see notes	None	None	None					
26	NIS	Toaster	Blocked	HTTP Nine-Ball Mass Injection	None	None	None					
26	PIS	Toaster	Blocked	Dangerous operation blocked!	Report	Multiple - see notes	Multiple - see notes					
26	TIS	Browser	Blocked	Blocked	None	None	None					
27	AVA	Pop-up	Move to chest	Win32:FakeAV-NO [Rtk]	None	None	None					
27	AVG	Pop-up	Healed	Trojan horse Sheur.BDVD	None	None	None					
27	AVI	Pop-up	Deny access	Multiple - see notes	None	None	None					
27	BDF	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a					
27	KIS	Toaster	Denied	Trojan.Exploit.SW.downloads.ks	None	None	None					
27	MIS	Toaster	See note	Exploit CVE 2007-0071	Report	Quarantined	Multiple - see note					
27	MSE	Toaster	Removed	Multiple - see notes	None	None	None					

27	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None						
27	PIS	None	None	None	Report	Multiple - see notes	Multiple - see notes						
27	TIS	None	See note	None	None	None	None						
28	AVA	Toaster	Blocked	Multiple - see notes	n/a	n/a	n/a						
28	AVG	Pop-up	Healed	Trojan horse SHeur2.BEGM	None	None	None						
28	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a						
28	BDF	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a						
28	KIS	Toaster	Denied	Multiple - see notes	None	None	None						
28	MIS	Toaster	Quarantined	Exploit-CVE 007-0071	Report	Quarantined	Multiple - see note						
28	MSE	Toaster	Removed	Multiple - see notes	None	None	None						
28	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None						
28	PIS	None	None	None	Report	Deleted	Trj/CL.A x7						
28	TIS	None	See note	None	None	None	None						
29	AVA	Pop-up	Move to chest	HTML:Iframe-inf	n/a	n/a	n/a						
29	AVG	Pop-up	Healed	TrojanHorse Generic14.AWYS x2	Report	Moved to virus vault	TrojanHorse Generic14.AWYS x2						
29	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a						
29	BDF	Pop-up	Blocked	Trojan.Generic.2428125 x5	n/a	n/a	n/a						
29	KIS	Toaster	Denied	http://erotic-baby-girl/white/index.php	None	None	None						
29	MIS	Toaster	Removed	Generic.Downloader.ap	None	None	None						
29	MSE	Toaster	Removed	Trojan:Win32/Oficla.E x2	None	None	None						
29	NIS	None	See note	None	Report	Removed	2 tracking cookies						
29	PIS	Toaster	Blocked	Dangerous operation blocked!	Report	Quarantined	Suspicious file x2						
29	TIS	None	See note	None	Report	Deleted	Cookied_DoubleClick						
30	AVA	Pop-up	Deleted	HTML:Iframe-JP [Trj]	None	None	None						
30	AVG	Pop-up	Healed	Trojan horse Sheur.BEKX	None	None	None						
30	AVI	None	None	None	None	None	None						

32	TIS	None	See note	None	None	None	None					
33	AVA	Pop-up	Move to chest	Multiple - see notes	n/a	n/a	n/a					
33	AVG	Pop-up	Moved to Vault	Multiple - see notes	Report	Cannot be removed or healed	Trojan Horse Generic II.ADSJ					
33	AVI	Pop-up	Deny access	EXP/DirektShow.A exploit x3	n/a	n/a	n/a					
33	BDF	None	None	None	Report	Multiple - see notes	Multiple - see notes					
33	KIS	Toaster	Denied	Exploit.JS.Agent.aw	None	None	None					
33	MIS	Toaster	See note	Exploit-MS DirectShow.b	n/a	n/a	n/a					
33	MSE	Toaster	See note	Trojan:Win32/Trafog!	n/a	n/a	n/a					
33	NIS	None	None	None	n/a	n/a	n/a					
33	PIS	Pop-up	Deleted	Exploit/DirektShow.A	Report	Multiple - see notes	Multiple - see notes					
33	TIS	Browser	Blocked	Blocked	None	None	None					
34	AVA	Toaster	Blocked	Network Shield: gaysex365.com	n/a	n/a	n/a					
34	AVG	Pop-up	Healed	Trojan horse Sheur.BFFL	None	None	None					
34	AVI	Pop-up	Deny access	Multiple - see notes	None	None	None					
34	BDF	Pop-up	Blocked	Trojan.Spy.Zbot.BQT x2	n/a	n/a	n/a					
34	KIS	Toaster	Denied	http://gaysex365.com/st/css/z/static.php	None	None	None					
34	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	None	None					
34	MSE	Toaster	See note	TrojanDownloader:Win32/Reno	Report	Removed	TrojanDownloader:Win32/Reno					
34	NIS	Browser	Blocked	Lists URL. See notes for additional toaster info.	n/a	n/a	n/a					
34	PIS	None	None	None	Report	Quarantined	Multiple - see notes					
34	TIS	None	See note	None	None	None	None					
35	AVA	Toaster	Blocked	Network Shield: bookrave.com	n/a	n/a	n/a					
35	AVG	Pop-up	Healed	Trojan horse Sheur BFFL	None	None	None					
35	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a					
35	BDF	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a					
35	KIS	Toaster	Denied	Multiple - see notes	None	None	None					
35	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	None	None					

















35	MSE	Toaster	See note	None	Report	Removed	Trojan: Downloader/Win32/Renos						
35	NIS	Multiple - see notes	Blocked	Multiple - see notes	n/a	n/a	n/a		█	█			
35	PIS	None	None	None	Report	Quarantined	Multiple - see notes						█
35	TIS	None	See note	None	None	None	None			█			
36	AVA	Toaster	Blocked	Network Shield x2	n/a	n/a	n/a		█	█			
36	AVG	Pop-up	Healed	Trojan horse SHeur2.BFFL	None	None	None			█			
36	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a		█	█			
36	BDF	Pop-up	Blocked	Trojan.Spy.Zbot.BQT	n/a	n/a	n/a		█	█			
36	KIS	Toaster	Denied	http://hexabomb.com/files/z/static.php	None	None	None			█			
36	MIS	Toaster	See note	Exploit-CVE 2007-0071	None	None	None						█
36	MSE	Toaster	See note	TrojanDownloader:Win32/Renos	Report	Removed	TrojanDownloader:Win32/Renos					█	
36	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a		█	█			
36	PIS	None	None	None	Report	Quarantined	Suspicious file x10						█
36	TIS	None	See note	None	None	None	None			█			
37	AVA	Toaster	Blocked	Network Shield: bookrave.com	n/a	n/a	n/a		█	█			
37	AVG	None	See note	None	None	None	None						█
37	AVI	Pop-up	Deny access	HTML/Crypted.Gen HTML script virus	None	None	None						█
37	BDF	Multiple - see notes	Blocked	Multiple - see notes	Report	Quarantined	Exploit.PDF-JS.Gen					█	
37	KIS	Toaster	Denied	Multiple - see notes	None	None	None			█			
37	MIS	Toaster	See note	Exploit-Iframe.gen.c	None	None	None						█
37	MSE	Toaster	Multiple - see notes	Multiple - see notes	Report	Multiple-see note	Multiple - see note						█
37	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a		█	█			

40	MIS	Pop-up	Blocked	Buffer overflow	Report	Quarantined	Artemis!59EBBE31B3AF						
40	MSE	Pop-up	Removed	Multiple - see notes	None	None	None						
40	NIS	Browser	Blocked	Malicious Web Page Blocked	n/a	n/a	n/a						
40	PIS	Toaster	Blocked	Dangerous operation blocked!	Report	Multiple-see note	Multiple - see note						
40	TIS	None	None	None	n/a	n/a	n/a						
41	AVA	Toaster	Blocked	Network Shield: xrateddj.com	n/a	n/a	n/a						
41	AVG	Pop-up	Healed	Trojan horse Downloader Generic 8.BTSI	None	None	None						
41	AVI	Pop-up	Blocked	Multiple - see notes	None	None	None						
41	BDF	Pop-up	Blocked	Exploit.SWF.Shellcode.Gen	Report	Multiple - see notes	Multiple - see notes						
41	KIS	Toaster	Denied	HEUR:Exploit.Script.Generic	None	None	None						
41	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	See note	None						
41	MSE	Toaster	Removed	TrojanDownloader:Win32/Renos	Report	Removed	TrojanDownloader:Win32/Swif.M						
41	NIS	Multiple - see notes	Multiple - see notes	Blocked	None	None	None						
41	PIS	None	None	None	Report	Deleted	Multiple - see notes						
41	TIS	None	See note	None	None	None	None						
42	AVA	Toaster	Blocked	Network Shield: http://bookrave.com/tmp/z/static.php	n/a	n/a	n/a						

43	KIS	Toaster	Denied	http://glaport.ru/ip/news.php?s=1c878cf766	None	None	None				
43	MIS	None	See note	None	None	None	None				
43	MSE	Toaster	Quarantined	VirTool:Win32/Obfuscator.FI	None	None	None				
43	NIS	Browser	Blocked	Blocked	None	None	None				
43	PIS	Pop-up	Blocked	Multiple - see notes	None	None	None				
43	TIS	Browser	Blocked	Blocked	None	None	None				
44	AVA	Pop-up	Move to chest	JS:FakeAV-BI [Trj] x2	n/a	n/a	n/a				
44	AVG	None	None	None	None	None	None				
44	AVI	Pop-up	Blocked	TR/Dldr.FraudLoad.fqb	n/a	n/a	n/a				
44	BDF	Pop-up	Firewall alert	see notes	None	None	None				
44	KIS	Toaster	Denied	http://mycompsscanner02.com/scan1/?pid=2428.engine=%3DHmy9DTuMzg5LjtXOC40NS70aW1/PTEyNTE4NAkONAkN	None	None	None				
44	MIS	None	See note	None	None	None	None				
44	MSE	Toaster	Removed	Trojan:JS/FakeXPA	None	None	None				
44	NIS	Toaster	See note	Soft_242 [1].exe	None	None	None				


















44	PIS	None	None	None	None	None	None						
44	TIS	Browser	Blocked	http://217.20.127.89/~muromec/ss2.php	None	None	None						
45	AVA	Toaster	Blocked	Network Shield: blocked http://bookrave.com/tmp/z/static.php	n/a	n/a	n/a						
45	AVG	Pop-up	Healed	Trojan horse Downloader Generic8.BTSL	None	None	None						
45	AVI	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a						
45	BDF	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a						
45	KIS	Toaster	Denied	Multiple - see notes	None	None	None						
45	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	None	None						
45	MSE	Toaster	See note	Multiple - see notes	None	None	None						
45	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None						
45	PIS	None	None	None	Report	Quarantined	Suspicious files x5						
45	TIS	None	See note	None	None	None	None						
46	AVA	Multiple - see notes	Quarantined	Multiple - see notes	Report	Deleted	Multiple						


















46	AVG	None	None	None	Report	See note	Multiple - see note					
46	AVI	Pop-up	Blocked	TR/Dldr.Agent.wxk	Report	Repair all	TR.Dldr.Agent.wxk					
46	BDF	Toaster	Terminated	363.exe terminated because it was deemed harmful	None	None	None	■				
46	KIS	Toaster	Denied	http://wonicer.cn/in.php?v=br	None	None	None		■			
46	MIS	Toaster	Removed	Multiple - see notes	None	None	None		■			
46	MSE	Toaster	Removed	Trojan:Win32/Oficla.E	None	None	None		■			
46	NIS	Multiple - see notes	Multiple - see notes	HTTP Acrobat PDF Suspicious File Download	None	None	None		■			
46	PIS	Toaster	Multiple - see notes	Multiple - see notes	Report	Neutralized	Multiple - see note					
46	TIS	None	See note	None	None	None	None		■			
47	AVA	Toaster	Blocked	Site: xrateddj.com	n/a	n/a	n/a	■	■			
47	AVG	Pop-up	Healed	Trojan horse Sheur2.BGOH	None	None	None		■			
47	AVI	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a	■	■			
47	BDF	Pop-up	Blocked	Multiple - see notes	Report	Deleted	Exploit.PDF-JS.Gen					
47	KIS	Toaster	Denied	HEUR:Exploit.Script.Generic	None	None	None		■			
47	MIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None					

47	MSE	Toaster	Removed	Multiple - see notes	None	None	None				
47	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None				
47	PIS	None	None	None	Report	Neutralized	Multiple - see notes				
47	TIS	None	See note	None	None	None	None				
48	AVA	Toaster	Blocked	Network Shield: odile-marco.com/lib/index.php	n/a	n/a	n/a				
48	AVG	None	None	None	Report	See note	Trojan horse BHO.JEW				
48	AVI	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a				
48	BDF	Pop-up	Blocked	Trojan.SWF.Dropper.Gen	n/a	n/a	n/a				
48	KIS	Toaster	Multiple - see notes	Multiple - see notes	Report	See note	Trojan-Downloader.JS.ActiveX.cm				
48	MIS	Toaster	Removed	Artemis!ADI88A449COC	None	None	None				
48	MSE	Toaster	Multiple - see notes	Multiple - see notes	Report	Quarantined	Trojan:Win32/FakeSpyro				
48	NIS	None	See note	None	None	None	None				
48	PIS	None	None	None	n/a	n/a	n/a				
48	TIS	Browser	Blocked	Blocked	None	None	None				


















49	AVA	Multiple - see notes	Multiple -see notes	Multiple -see notes	n/a	n/a	n/a		█	█		
49	AVG	None	None	None	None	None	None			█		
49	AVI	Pop-up	Blocked	Multiple - see notes	Report	Quarantined	HTML/Iframe.bkz				█	
49	BDF	Pop-up and toaster	Deleted	Multiple - see notes	n/a	n/a	n/a				█	
49	KIS	Toaster	Allow	KAX.EXE	Report	See note	PDM.Trojan.Generic					█
49	MIS	Toaster	None	Exploit-MS DirektShow	None	None	None					█
49	MSE	Toaster	Removed	Trojan:JS/Redirector.AQ	None	None	None			█		
49	NIS	Browser	Blocked	Blocked	None	None	None			█		
49	PIS	None	None	None	Report	Quarantined	Multiple - see notes				█	
49	TIS	None	See note	None	None	None	None			█		
50	AVA	Toaster	Blocked	Network Shield: hexatomb.com/files/z/static.php	n/a	n/a	n/a		█	█		
50	AVG	Pop-up	Healed	Trojan horse Generic14.BIYX	Report	Moved to vault	Multiple - see note			█		
50	AVI	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a		█	█		
50	BDF	Pop-up	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a		█	█		
















50	KIS	Toaster	Denied	http://hexatomb.com/files/z/static.php	None	None	None								
50	MIS	Toaster	See note	Multiple - see notes	None	None	None								
50	MSE	Toaster	Removed	Multiple - see notes	None	None	None								
50	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	Report	Removed	3 tracking cookies								
50	PIS	None	None	None	Report	Quarantined /Deleted	Multiple - see notes								
50	TIS	None	See note	None	Report	Deleted	Cookie_Profiling								
51	AVA	Toaster	Network shield block	Multiple - see notes	none	none	none								
51	AVG	None	See note	None	None	None	None								
51	AVI	Pop-up	Blocked	Multiple - see notes	none	none	none (see notes)								
51	BDF	Pop-up	Blocked	Exploit-PDF-JS.Gen	none	none	none								
51	KIS	Toaster	Denied	Multiple - see notes	None	None	None								
51	MIS	Toaster	See note	Buffer overflow	None	None	None								
51	MSE	Toaster	Multiple - see notes	Multiple - see notes	None	None	None								
51	NIS	Browser	Blocked	Blocked	None	None	None								

51	PIS	Toaster	Virus neutralised	Trj/KillFilesBF	none	none	none					
51	TIS	None	See note	None	None	None	None					
52	AVA	None	None	None	None	None	None					
52	AVG	Pop-up	Healed	Trojan horse Agent2.THIS	Report	Moved to vault	Trojan horse Backdoor Agen ACWZ					
52	AVI	Pop-up	Blocked	Multiple - see notes	none	none	none					
52	BDF	None	None	None	n/a	n/a	n/a					
52	KIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None					
52	MIS	Toaster	Blocked	W3Akbot!A	None	None	None					
52	MSE	Toaster	Removed	Backdoor:Win32/Qakbot.gen!A	None	None	None					
52	NIS	Toaster	Removed	j[1]Downloader	Report	Removed	2 tracking cookies					
52	PIS	Toaster	Dangerous operation blocked	Protection for Internet Explorer 0 day in msvitctl.dll library	report	Neutralized	Trj/CI.A					
52	TIS	None	See note	None	Report	Quarantined	Cookie_Profiling					
53	AVA	Toaster	Network Shield Block	Blocked access to malicious site http://liveinru.com/google/index.php	n/a	n/a	n/a					
53	AVG	None	See note	None	None	None	None					




53	AVI	Pop-up	Blocked	EXP/Pidief.gug	n/a	n/a	n/a				
53	BDF	Pop-up	Blocked	Multiple - see notes	Report	Quarantined	Exploit.PDF-JS.Gen				
53	KIS	Toaster	Denied	liveinlivenru.com/google/index.php	None	None	None				
53	MIS	Toaster	Blocked	Buffer overflow	None	None	None				
53	MSE	Toaster	Removed	Trojan:Win32/Swif.D	None	None	None				
53	NIS	Toaster	Removed	etcForm[1].pdf (Trojan.Pidief.C)	None	None	None				
53	PIS	Toaster	Dangerous operation blocked	Evidence for Internet Explorer 0 day in msvidctl.dll library	None	None	None				
53	TIS	Browser	Blocked	Blocked	None	None	None				
54	AVA	Toaster	See note	HTML:Iframe.inf	None	None	None				
54	AVG	None	See note	None	None	See note	None				
54	AVI	Pop-up	Denied	Multiple - see notes	Report	Repaired	net.cap (object) in HTML/Infected Web Page.Gen				
54	BDF	Toaster	Quarantined	Trojan.SWF.Dropper.Gen	None	None	None				
54	KIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None				
54	MIS	Toaster	Removed	Artemis!	None	None	None				
54	MSE	Toaster	See note	Multiple - see notes	None	None	None				

















54	NIS	Pop-up	Blocked	MSIE Adobe Reader GetIcon BO	None	None	None				
54	PIS	None	See note	None	None	None	None				
54	TIS	None	See note	None	None	None	None				
55	AVA	Pop-up and toaster	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a				
55	AVG	Pop-up	Healed	Trojan horse Generic14.BMRE	None	None	None				
55	AVI	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a				
55	BDF	Pop-up	Blocked	Multiple - see notes	Report	Quarantined	Exploit.PDF-JS.Gen				
55	KIS	Toaster	Denied	Multiple - see notes	None	None	None				
55	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	None	None				
55	MSE	Toaster	Removed	TrojanDownloader:Win32/Renos	None	None	None				
55	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None				
55	PIS	None	None	None	Report	Quarantined /Deleted	Multiple - see notes				
55	TIS	None	See note	None	Report	Blocked	1 Web site				
56	AVA	Browser and pop-up	Deleted	HTML:Iframe-KE [Trj]	n/a	n/a	n/a				

56	AVG	Pop-up	Healed	Trojan horse Generic14.BMRE	None	None	None				
56	AVI	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a				
56	BDF	Pop-up	Blocked	Multiple - see notes	Report	Quarantined	Exploit.PDF-JS.Gen				
56	KIS	Toaster	Denied	http://hexatomb.com/files/z/static.php	None	None	None				
56	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	None	None				
56	MSE	Toaster	Removed	TrojanDownloader:Win32/Renos	None	None	None				
56	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None				
56	PIS	None	None	None	Report	Quarantined /Deleted	Multiple - see notes				
56	TIS	None	See note	None	Report	None	None				
57	AVA	Pop-up and toaster	Blocked	Multiple - see notes	None	None	None				
57	AVG	Pop-up	Healed	Trojan horse Generic14.BMRE	None	None	None				
57	AVI	Pop-up	Blocked	Multiple - see notes	none	none	none				
57	BDF	Pop-up and toaster	Blocked	Multiple - see notes	report	Quarantined	Exploit.PDF-JS.Gen				
















57	KIS	Toaster	Denied	Multiple - see notes	None	None	None				
57	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	None	None				
57	MSE	Toaster	Removed	Multiple - see notes	None	None	None				
57	NIS	Toaster	Removed	static[1].htm (JS Downloader)	Report	Removed	2 tracking cookies				
57	PIS	None	None	None	report	Quarantined /Deleted	Multiple - see notes				
57	TIS	None	See note	None	None	None	None				
58	AVA	Pop-up and toaster	Blocked	Multiple - see notes	n/a	n/a	n/a				
58	AVG	None	See note	None	None	None	None				
58	AVI	None	None	None	None	None	None				
58	BDF	Pop-up	Blocked	Multiple - see notes	report	Quarantined	Exploit.PDF-JS.Gen				
58	KIS	Toaster	Denied	http://hexatomb.com/files/z/static.php	None	None	None				
58	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	None	None				
58	MSE	Toaster	Multiple - see notes	Multiple - see notes	Report	Quarantined	TrojanDownloader:Win32/Renos				
58	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None				

60	BDF	Pop-up	Blocked	Multiple - see notes	n/a	n/a	n/a					
60	KIS	Toaster	Denied	HEUR:Trojan.Script.iframe (2x)	None	None	None					
60	MIS	Toaster	Removed	JS/Exploit.BO.gen	None	None	None					
60	MSE	Toaster	Removed	PWS:Win32/Daptdei.A (2x)	None	None	None					
60	NIS	Browser	Blocked	Blocked	None	None	None					
60	PIS	Toaster	Neutralized	Trj/CL.A	None	None	None					
60	TIS	None	See note	None	None	None	None					
61	AVA	None	See note	None	None	None	None					
61	AVG	None	See note	None	None	None	None					
61	AVI	Pop-up	Denied	Multiple - see notes	Pop-up	Moved to vault	HTML/Crypted.Gen					
61	BDF	None	See note	None	None	None	None					
61	KIS	Toaster	Denied	Trojan-Downloader.JS Iframe.bsl	None	None	None					
61	MIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None					
61	MSE	None	See note	None	None	None	None					
61	NIS	Toaster	Blocked	HTTP Malicious Toolkit Variant Activity	None	None	None					
61	PIS	None	See note	None	None	None	None					

















61	TIS	None	See note	None	None	None	None				
62	AVA	Toaster	Blocked	Network Shield: vkpainting.net	n/a	n/a	n/a				
62	AVG	Pop-up	Healed	Trojan horse Agent2.TJI	Report	Moved to vault	Trojan horse Agent2.TJI				
62	AVI	Pop-up	Deny access	TR/Inject.ajkn Trojan x2	n/a	n/a	n/a				
62	BDF	Pop-up	Blocked	Trojan.Generic.2497476 x2	n/a	n/a	n/a				
62	KIS	Toaster	Denied	http://vkpainting.net	None	None	None				
62	MIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None				
62	MSE	Toaster	Multiple - see notes	Multiple - see notes	Toaster	See note	Virus:Win32/Induc.A				
62	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None				
62	PIS	Toaster	Neutralized	Trj/Inject.K	n/a	n/a	n/a				
62	TIS	Browser	Blocked	Blocked	None	None	None				
63	AVA	None	None	None	n/a	n/a	n/a				
63	AVG	None	See note	None	None	None	None				
63	AVI	None	None	None	n/a	n/a	n/a				
63	BDF	None	None	None	n/a	n/a	n/a				

63	KIS	Toaster	Denied	HEUR:Trojan.Script.Iframer	None	None	None				
63	MIS	None	See note	None	None	None	None				
63	MSE	None	See note	None	None	None	None				
63	NIS	None	See note	None	Report	Removed	4 tracking cookies				
63	PIS	None	None	None	n/a	n/a	n/a				
63	TIS	None	See note	None	Report	Deleted	Cookie_StatCounter				
64	AVA	Multiple - see notes	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a				
64	AVG	Pop-up	Healed	Trojan horse SHeur2.BISH	n/a	See note	n/a				
64	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a				
64	BDF	None	None	None	Report	n/a	Multiple - see notes				
64	KIS	Toaster	Denied	Exploit.JS.Agent.anr	None	None	None				
64	MIS	Toaster	Removed	Exploit-MS DirektShow	Report	Multiple - see notes	Multiple - see notes				
64	MSE	Toaster	Multiple - see notes	Multiple - see notes	Report	Quarantined	PWS:Win32/Daurso.A				
64	NIS	Toaster	Removed	win[1].jpg (Downloader Fostrem)	None	None	None				


















70	AVA	Pop-up and toaster	Blocked	Multiple - see notes	n/a	n/a	n/a		█	█		
70	AVG	Pop-up	Healed	Trojan horse SHeur2.BJBU	None	None	None			█		
70	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a		█	█		
70	BDF	Pop-up	Blocked	Multiple - see notes	Report	Deleted	Exploit.PDF-JS.Gen		█		█	
70	KIS	Toaster	Denied	Multiple - see notes	None	See note	None					█
70	MIS	Toaster	Quarantined	See note	None	See note	None					█
70	MSE	Toaster	Removed	Multiple - see notes	None	None	None			█		
70	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None			█		
70	PIS	None	None	None	Report	Multiple - see notes	Multiple - see notes				█	
70	TIS	None	See note	None	None	None	None			█		
71	AVA	None	None	None	Report	Multiple - see notes	Multiple - see notes					█
71	AVG	Pop-up	Healed	Trojan horse SHeur2.BJC2	None	None	None					█
71	AVI	Pop-up	Deny access	T/Crypt.ZPACK.Gen Trojan	n/a	n/a	n/a		█	█		
71	BDF	Toaster	Terminated	file.exe has been terminated because it was deemed harmful	Report	Deleted	Application.Generic.234114		█		█	

71	KIS	Toaster	Denied	Net-Worm.Win32.Aspxor.ft	None	None	None				
71	MIS	Toaster	Removed	Exploit-PDF.genstream	None	None	None				
71	MSE	Toaster	Removed	Multiple - see notes	None	None	None				
71	NIS	Browser	Blocked	Blocked	None	None	None				
71	PIS	None	None	None	Report	Quarantined	Multiple - see notes				
71	TIS	None	See note	None	None	None	None				
72	AVA	Pop-up and toaster	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a				
72	AVG	Pop-up	See note	Multiple - see notes	None	None	None				
72	AVI	Pop-up and toaster	Deny access	Multiple - see notes	Report	Quarantined	BDS/Bredavi.WN				
72	BDF	Pop-up and toaster	Multiple - see notes	Multiple - see notes	Report	No action is possible	Multiple - see notes				
72	KIS	Toaster	Denied	Trojan-Downloader.JS.Shadraem.a	None	None	None				
72	MIS	Toaster	Removed	Exploit-MS DirectShow.b	Report	Multiple - see notes	Multiple - see notes				
72	MSE	Toaster	Removed	Multiple - see notes	None	See note	None				
72	NIS	None	See note	None	Report	Removed	2 tracking cookies				

72	PIS	Pop-up and toaster	Multiple - see notes	Multiple - see notes	Report	Multiple - see notes	Multiple - see notes						
72	TIS	None	See note	None	Report	Deleted	Cookie_DoubleClick						
73	AVA	None	None	None	n/a	n/a	n/a						
73	AVG	None	None	None	None	None	None						
73	AVI	Pop-up	Deny access	TR/Crypt.ZPACK.Gen Trojan	n/a	n/a	n/a						
73	BDF	Browser	Blocked	BitDefender Antiphishing	n/a	n/a	n/a						
73	KIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None						
73	MIS	Toaster	See note	Registry change	Report	Quarantined	Detection name: Artemis!78B20EA48299 (2x); File name: SDRA64.EXE						
73	MSE	Toaster	Removed	PWS:Win32/Zbot.gen!R	None	None	None						
73	NIS	Toaster	Multiple - see notes	Multiple - see notes	None	None	None						
73	PIS	Toaster	Blocked	Suspicious program detected	n/a	n/a	n/a						
73	TIS	Browser	Blocked	Blocked	None	None	None						

74	AVA	Toaster	Network Shield Block	Blocked access to http://hexatomb.com/files/z/static.php	n/a	n/a	n/a					
74	AVG	Pop-up	Healed	Trojan horse SHeur2.BJGT	None	None	None					
74	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a					
74	BDF	Pop-up	Blocked	Multiple - see notes	Report	Deleted	Exploit.PDF-JS.Gen					
74	KIS	Toaster	Denied	http://hexatomb.com/files/z/static.php	None	None	None					
74	MIS	Toaster	Quarantined	Exploit-CVE 2007-0071	None	None	None					
74	MSE	Toaster	Removed	Multiple - see notes	None	None	None					
74	NIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None					
74	PIS	None	None	None	Report	Quarantined	Multiple - see notes					
74	TIS	None	See note	None	None	None	None					
75	AVA	Pop-up and toaster	Deleted	HTML:Iframe-JR [Trj]	None	None	None					
75	AVG	Pop-up	Moved to Vault	Exploit	None	None	None					
75	AVI	Pop-up	Deny access	TR/Crypt.XDR.Gen Trojan	n/a	n/a	n/a					

75	BDF	None	None	None	Report	None	None					
75	KIS	Multiple - see notes	Multiple - see notes	Multiple - see notes	None	None	None					
75	MIS	Toaster	Removed	Generic.dx!fia (Trojan)	None	None	None					
75	MSE	Toaster	Removed	Trojan:Win32/Tibs.IT	None	None	None					
75	NIS	Browser	Blocked	Blocked	None	None	None					
75	PIS	Toaster	Virus neutralised	Generic trojan	n/a	n/a	n/a					
75	TIS	None	See note	None	None	None	None					
76	AVA	Multiple - see notes	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a					
76	AVG	Pop-up	Healed	Trojan horse SHeur2.BJGG	None	None	None					
76	AVI	Pop-up	Deny access	Multiple - see notes	n/a	n/a	n/a					
76	BDF	Pop-up	Multiple - see notes	Multiple - see notes	None	None	None					
76	KIS	Toaster	Denied	HEUR:Trojan.Script.Iframer	None	None	None					
76	MIS	Toaster	Removed	Multiple - see notes	Report	Quarantined	Artemis!45A7ZZ162520					
76	MSE	Toaster	Removed	TrojanDropper:Win32/Preald.B	None	None	None					

76	NIS	Browser	Blocked	Blocked	None	None	None				
76	PIS	None	None	None	Report	Multiple - see notes	Multiple - see notes				
76	TIS	None	See note	None	None	None	None				
77	AVA	Multiple - see notes	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a				
77	AVG	Pop-up	Healed	Multiple - see notes	Report	See note	See note				
77	AVI	Pop-up	Deny access	HEUR/HTML.Malware suspicious code	n/a	n/a	n/a				
77	BDF	Pop-up	Blocked	Multiple - see notes	None	None	None				
77	KIS	Toaster	Denied	Trojan-Clicker.HTML.Agent.aq	None	None	None				
77	MIS	Toaster	Removed	Generic Downloader xlbkd (3x)	None	None	None				
77	MSE	Toaster	Removed	Multiple - see notes	None	None	None				
77	NIS	None	See note	None	None	None	None				
77	PIS	Toaster	Blocked	Multiple - see notes	Report	Quarantined	Multiple - see notes				
77	TIS	None	See note	None	None	None	None				
78	AVA	Multiple - see notes	Multiple - see notes	Multiple - see notes	n/a	n/a	n/a				

APPENDIX D: TOOLS

Ebttables

<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.