PC Web Threat Protection 2010

SEVEN POPULAR ANTI-VIRUS PROGRAMS COMPARED FOR EFFECTIVENESS (SPONSORED BY TREND MICRO)

Dennis Technology Labs, 16/07/2010
www.DennisTechnologyLabs.com

This test aims to compare the effectiveness of the most recent releases of popular anti-virus software. The products include those from Kaspersky, McAfee, Microsoft, Norton (Symantec) and Trend Micro. The tests were conducted between 16/06/2010 and 29/06/2010 using the software versions available on any given day.

A total of seven products[1] 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 real, infected websites that significant numbers of internet users were encountering at the time of the test. These results reflect what would have happened if those users were using one of the seven products tested[2].

EXECUTIVE SUMMARY

Products tested

K7 Total Security 10
Kaspersky Internet Security 2011
McAfee Internet Security 2010
Microsoft Security Essentials
Panda Internet Security 2010
Norton Internet Security 2010
Trend Micro Internet Security 2010

- **Products that block attacks early tended to protect the system more fully**

The nature of web-based attacks means that the longer malware has access to a system, the more chances it has of downloading and installing further threats. Products that blocked the malicious and infected websites from the start reduced the risk of compromise by secondary and further downloads.

- **100 per cent protection is rare**

This test recorded an average protection rate of 92 per cent. New threats appear online frequently and it is inevitable that there will be times when specific security products are unable to protect from some of these threats.

- **The products rarely blocked the installation of legitimate applications**

There were a number of cases in which the anti-virus programs warned against allowing legitimate applications full access to the system and the network. However, they rarely blocked these applications from installing .

Simon Edwards, Dennis Technology Labs

[1] The test included the seven products listed here plus four others, details of which are not included in this public report. The report's sponsor have sole access to this information. Two of these excluded products were in a pre-release stage at the time of testing. The other two were products from a vendor already represented in this report. The results for these two additional products were essentially the same as for the related product included here.

[2] This also assumes that the users were using the same version and patch-level of Windows and other software.

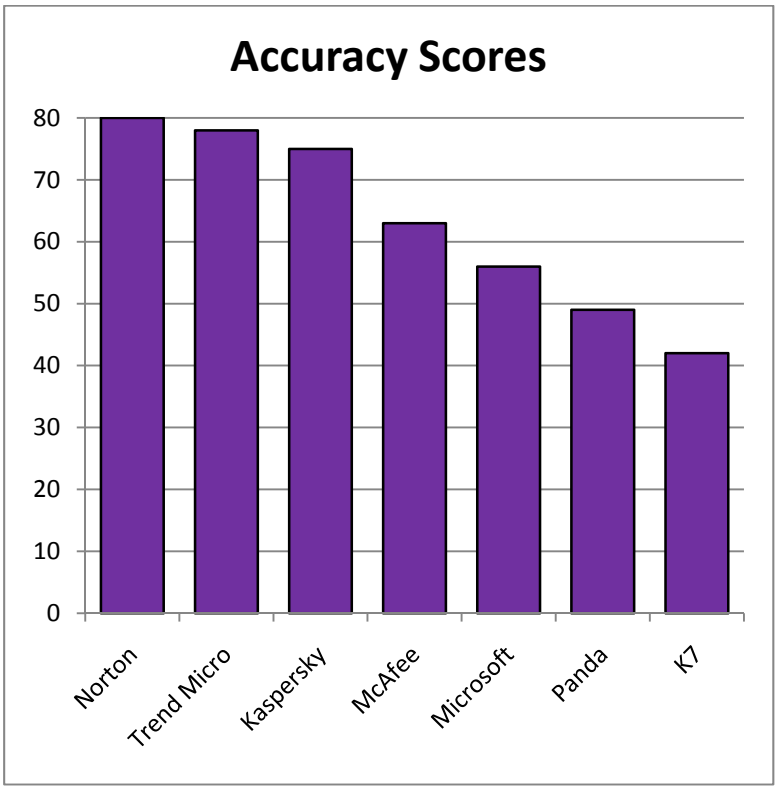
CONTENTS

1. Overall Accuracy

Each product has been scored for its accuracy in detecting and handling malware. We awarded two points for defending against a threat, one for neutralizing it and deducted 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 unstable, or even unusable without expert knowledge. Even if active malware was removed, we considered such damaged systems to count as being compromised.

The Symantec (Norton) product defended against all threats so it scores a full 80 marks. Trend Micro Internet Security 2010 scored of 78 out of 80 because it neutralized (rather than defended) two of the 40 threats. Kaspersky Internet Security 2011 defended against most threats but neutralized one and was compromised by another, so it scores 75 out of 80.



Products from Symantec (Norton) and Trend Micro protected the test systems from all threats.

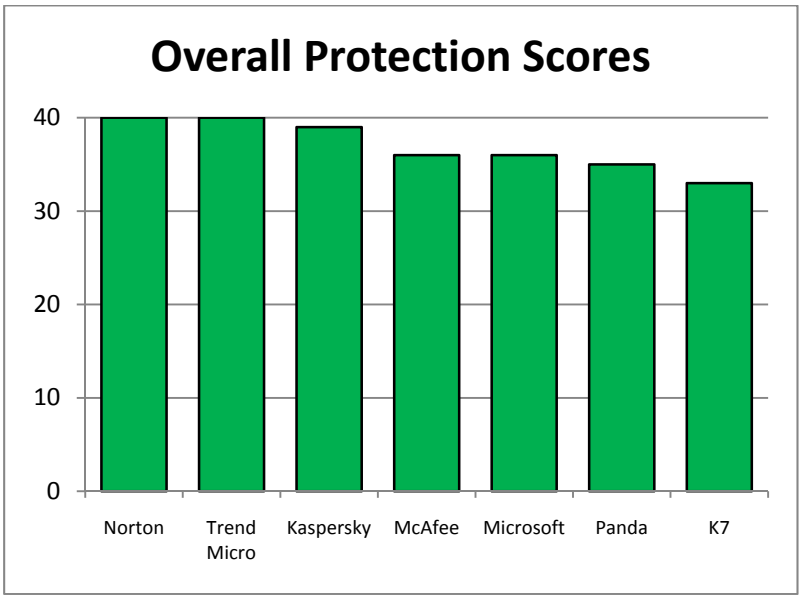
ACCURACY SCORES

PRODUCT	ACCURACY	DEFENDED	NEUTRALIZED	PROTECTED	COMPROMISED
Norton	80	40	0	40	0
Trend Micro	78	38	2	40	0
Kaspersky	75	38	1	39	1
McAfee	63	35	1	36	4
Microsoft	56	28	8	36	4
Panda	49	24	11	35	5
K7	42	23	10	33	7

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**.

The average protection levels afforded by the tested products, when exposed to the threats used in this test, was 92 per cent. The products that exceed this figure are Norton Internet Security 2010, Trend Micro Internet Security 2010 and Kaspersky Internet Security 2011.



The Norton and Trend Micro products provided complete protection.

OVERALL PROTECTION SCORES

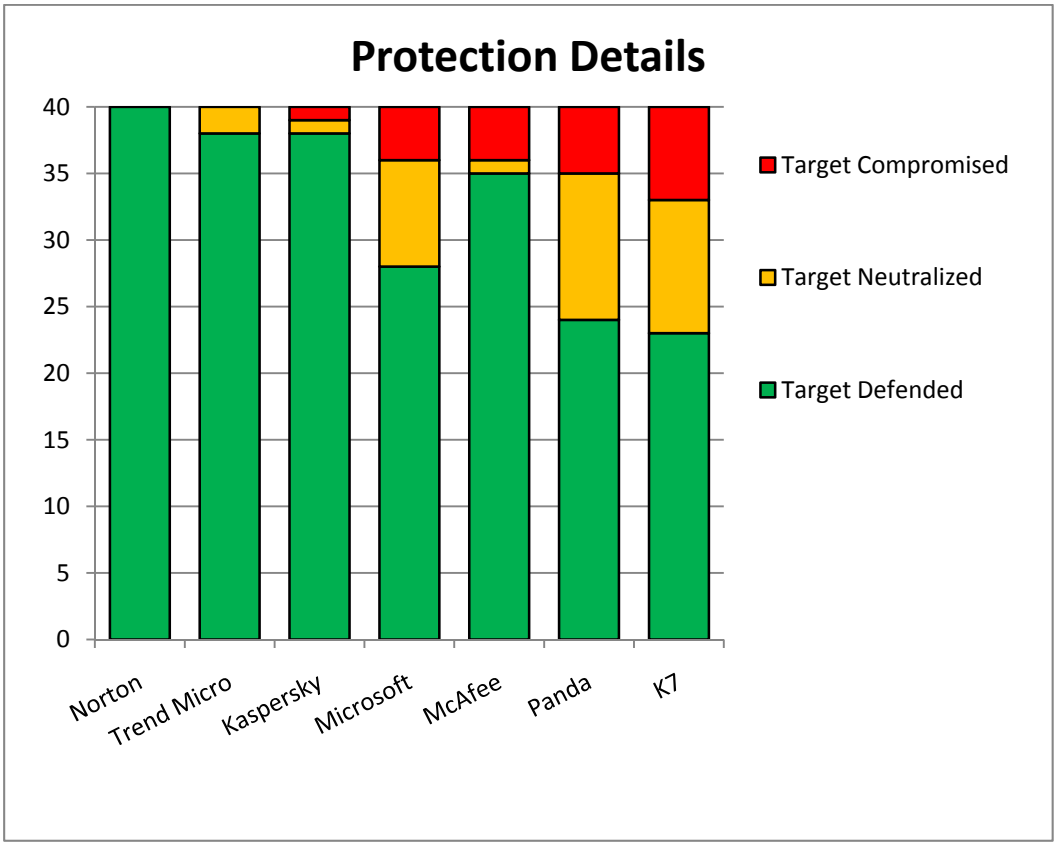
PRODUCT	COMBINED PROTECTION SCORE	PERCENTAGE
Norton	40	100%
Trend Micro	40	100%
Kaspersky	39	98%
McAfee	36	90%
Microsoft	36	90%
Panda	35	88%
K7	33	83%

(Average: 92 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 tended to defend, rather than neutralize, the threats. The Microsoft, Panda and K7 products displayed the highest numbers of neutralizations as well as the highest number of compromises. McAfee's product is the exception, having been compromised by a similar number of attacks but managing to defend, rather than neutralize, when performing successfully.



The most successful products tended to defend rather than neutralize, blocking the threats early in the attack.

PROTECTION DETAILS

PRODUCT	DEFENDED	NEUTRALIZED	COMPROMISED
Norton	40	0	0
Trend Micro	38	2	0
Kaspersky	38	1	1
Microsoft	28	8	4
McAfee	35	1	4
Panda	24	11	5
K7	23	10	7

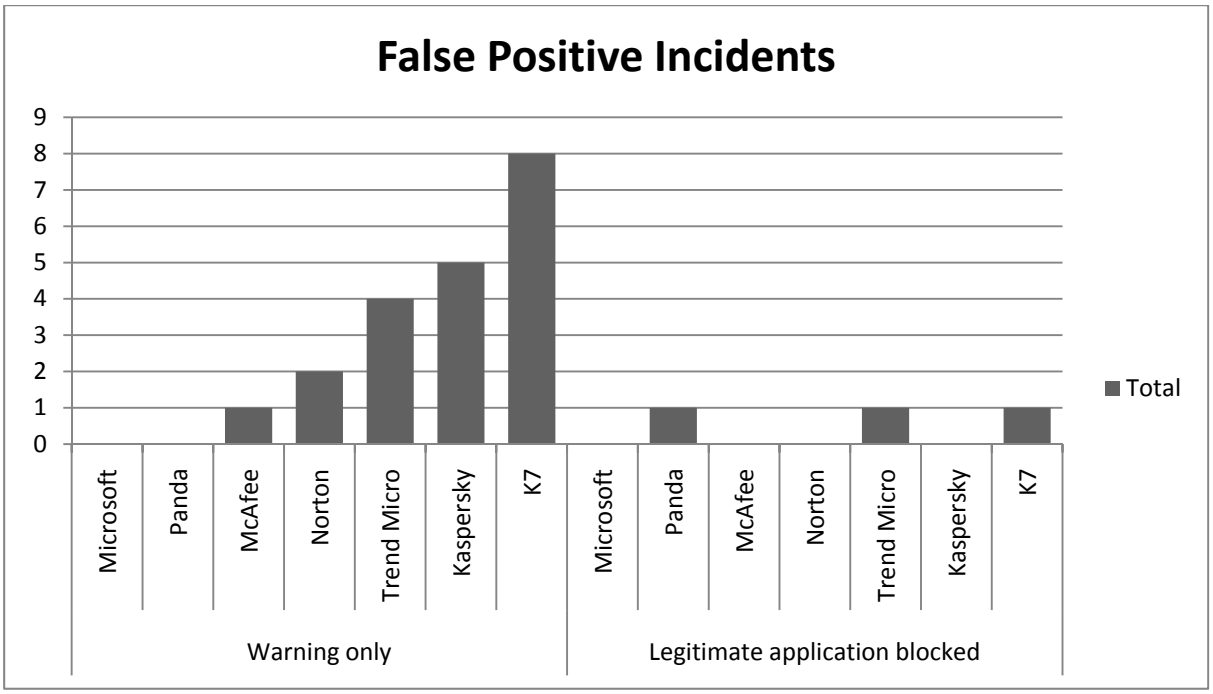
4. False Positives

4.1 False positive levels

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 because 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.

Blocking a legitimate application is more serious than issuing a warning because it directly hampers the user. Warnings may be of variable strength, sometimes simply asking if the legitimate application should be allowed to access the internet. This was true of all warnings issued by the K7 and Trend Micro products. Others, such as Norton Internet Security 2010, made explicit recommendations to prevent the application from running. One Norton alert read, "You are one of the very first Norton Users to download this file. We recommend not using this file until more is known about it." The first available user option was to stop the program from running. In three incidents a product blocked the installation of the legitimate application.

The graph below includes the number and type of false positive that each product generated.



Despite an apparently high percentage of false positives, most were light warnings.

FALSE POSITIVE INCIDENTS

PRODUCT	PRODUCT BLOCKED	THREAT WARNING
K7	1	8
Kaspersky	0	5
McAfee	0	1
Microsoft	0	0
Panda	1	0
Norton	0	2
Trend Micro	1	4

4.2 Taking file prevalence into account

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:

IMPACT CATEGORY	PREVALENCE (downloads in the previous week)
Very High Impact	> 20,000
High Impact	1,000 – 20,000
Medium Impact	100 – 999
Low Impact	25 – 99
Very Low Impact	< 25

4.3 Modifying scores

The following set of score modifiers were used to create an impact-weighted accuracy score. Each time a product allowed a new legitimate program to install and run it was awarded one point. It lost points (or fractions of a point) if and when it generated a false positive. We used the following score modifiers:

FALSE POSITIVE ACTION	IMPACT CATEGORY	SCORE MODIFIER
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

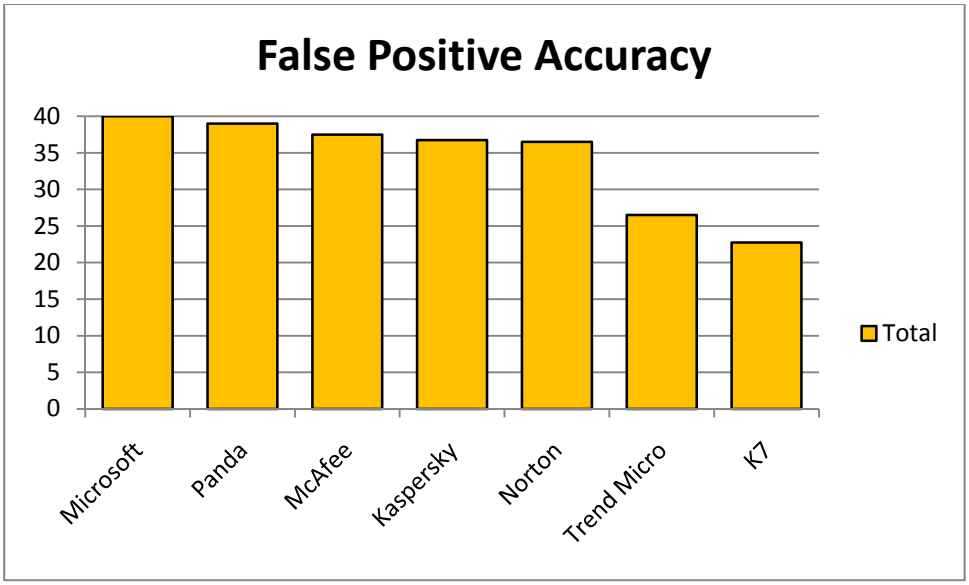
4.4 Distribution of impact categories

Products that scored highest were the most accurate when handling the legitimate applications used in the test. The best score possible is 40, while the worst would be -200 (assuming that all applications were classified as Very High Impact and were blocked). In fact the distribution of applications in the impact categories was not restricted only to Very High Impact. The table below shows the true distribution:

IMPACT CATEGORY	NUMBER OF INSTANCES
Very High Impact	16
High Impact	15
Medium Impact	7
Low Impact	2

4.5 False positive accuracy ratings

Combining the impact categories with weighted scores produces the following overall accuracy ratings.



When a product misclassified a popular program it faced a stronger penalty than if the file was more obscure.

PRODUCT	FALSE POSITIVE ACCURACY RATING
Microsoft	40
Panda	39
McAfee	37.5
Kaspersky	36.75
Norton	36.5
Trend Micro	26.5
K7	22.75

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 internal test website.

All target systems were fully exposed to the threats. This means that any exploit code was allowed to run, as were other malicious files, They were run and permitted to perform exactly as they were designed to, subject to checks made 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 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.

		Introduction				
Incide	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged detection without alert	Alert (mai
5	PIS	Toaster	Blocked	Suspicious program de	0	Report
5	NIS2010	None	None (see note)	None	1	n/a
5	TIS	None	None	None	0	n/a
6	K710	None	None (see note)	None	1	n/a
6	KIS2011	Multiple (see	Denied	Toaster reported that	0	n/a
6	MIS	None	None	None	0	None
6	MSE	None	None (see note)	None	1	n/a
6	PIS	None	None	None	0	None
6	NIS2010	None	None (see note)	None	1	n/a
6	TIS	Browser	Blocked	Opening this website i	0	n/a
7	K710	None	None (see note)	None	1	n/a
7	KIS2011	None	None (see note)	None	1	n/a
7	MIS	None	None	None	0	n/a
7	MSE	None	None (see note)	None	0	None

Each 'round' exposed every product to one specific threat. The partial set of records for round six (highlighted above) shows a range of responses to a particular threat. In this example the K7, Microsoft (MSE) and Norton (NIS2010) products did not display any alert, although they protected the system and quietly logged the fact. Trend (TIS) and Kaspersky (KIS) issued alerted when protecting, while Panda (PIS) and McAfee (MIS) failed to protect their systems.

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 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 ignored 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.

If malware failed to perform properly in a given incident, perhaps because of the very presence of the security product, rather than any specific defending action that the product took, the product was given the benefit of the doubt and a Defended result was recorded. If the test system was damaged, becoming hard to use following an attempted attack, this was counted as a compromise even if the active parts of the malware had eventually been removed by the product.

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. Manual scans were run only when a tester determined that malware had made an interaction with the target system. In other words, if the security product claimed to block the attack at the initial stage, and the monitoring logs supported this claim, the case was considered closed and a Defended result was recorded.

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. The operating system was updated with Windows XP Service Pack 3 (SP3) and Internet Explorer 7, although no later patches or updates were applied.

Usually we test with Windows XP SP2 and Internet Explorer 6, due to the high prevalence of internet threats that rely on this combination. The prevalence of these threats suggests that there are many systems with this level of patching currently connected to the internet. However, in this test we were also testing a beta product (the results for which are held privately by Trend Micro) that required the later service pack and browser version. To keep the test fair all products were installed on the same updated platform.

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 were 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 might automatically upgrade 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.

6.2 Threat selection

The malicious web links (URLs) used in the tests were picked from lists generated by Dennis Technology Labs's 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.

Malicious URLs and files are 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 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 we skipped this stage. 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. In some cases the target became so damaged that log recovery was considered impractical. 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 appear to be a range of threats (although it may be the same threat, slightly altered to avoid detection). Also, many infected sites will only attack a particular IP address once, which makes it hard to test more than one product against the same threat.

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. When the verification target systems visited a malicious site, the page's content, including malicious code, was downloaded, stored and loaded into the replay system. When each target system subsequently visited the site, it received exactly the same content.

The network configurations were set to allow all products unfettered access to the internet throughout the test, regardless of the web replay systems.

6.5 Secondary downloads

Established malware may attempt to download further files (secondary downloads), which are stored in a cache by a proxy on the network 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 in which target systems 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)

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 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.

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 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 might request a further scan to complete the removal. We considered secondary scans to be 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 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 a 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 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 testers 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, which is an aggressive caching mode that still permits internet access.

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.

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. The types of infected or malicious sites were varied, which 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, music or information on the stock market.

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, Trend Micro Internet Security 2010 and Kaspersky Internet Security 2011. 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. The two least effective products, those from K7 and Panda, often tackled the threat only once the malware had started to infect the system.

Sorting the wheat from the chaff
The false positive results were low, which shows that none of the products are tuned too aggressively to detect and block malware at the expense of regular programs. Microsoft Security Essentials was notable in that if generated no false positive results.

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.

The average protection level of the tested products is 92 per cent (**see 2. Overall protection**), which is significant. The presence of anti-virus software can be seen to decrease the chances of a malware infection even when the only sites being visited are proven to be malicious. It's worth noting, however, that a 100 per cent success rate is rare. Even those products that performed the best in this test are unlikely to be completely bullet-proof in every given situation.

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	ORIGINAL FILE NAME	PRODUCT	DESCRIPTION	OBTAINED VIA	PREVALENCE STATS (LAST WEEK)	PREVALENCE STATS SOURCE	PREVALENCE STATS DATE	PREVALENCE RATING
1	YouTubeDownloaderSetup256.exe	YouTube Downloader	Download YouTube videos and convert them to different formats.	Download.com	519,531	Download.com	30/06/2010	Very High Impact
2	wrar393.exe	WinRAR (32-bit)	Take full control over RAR and ZIP archives, along with unpacking a dozen other archive formats.	Download.com	376,240	Download.com	30/06/2010	Very High Impact
3	PhotoScapeSetup_V3.5.exe	PhotoScape	View, edit, print, or add frames to your photos.	Download.com	318,442	Download.com	30/06/2010	Very High Impact
4	asc-setup.exe	Advanced SystemCare Free	Protect, repair, optimize, and clean your computer in one click.	Download.com	284,201	Download.com	30/06/2010	Very High Impact
5	TeamViewer_Setup.exe	TeamViewer	Share your desktop with another person via the Web.	Download.com	274,963	Download.com	30/06/2010	Very High Impact
6	camfrog.exe	Camfrog Video Chat	Join live-video chat rooms from around the world	Download.com	238,718	Download.com	30/06/2010	Very High Impact
7	FoxitReader40_enu_Setup.exe	Foxit Reader 4.0.0.619	View your PDF files as PDF or as plain text.	Download.com	170,889	Download.com	30/06/2010	Very High Impact
8	mirc635.exe	mIRC	Chat with other people and participate in group discussions.	Download.com	128,973	Download.com	30/06/2010	Very High Impact
9	Firefox Setup 3.6.6.exe	Mozilla Firefox	Surf the Web, block pop-ups, and keep spyware at bay with a lean and fast open-source browser.	Download.com	102,129	Download.com	30/06/2010	Very High Impact
10	easy_cdda_extractor_2010_1_trial.exe	Easy CD-DA Extractor	Rip audio CDs, burn CDs and DVDs, convert music files, and edit metadata.	Download.com	25,240	Download.com	30/06/2010	Very High Impact
11	EasyDVDRipc.exe	Easy DVD Rip 3.0.801	Rip your DVDs into MPEG-4, AVI, DivX, XviD, MPEG-1, MPEG-2, VCD, and SVCD formats	Download.com	3,363	Download.com	30/06/2010	High Impact

INCIDENT	ORIGINAL FILE NAME	PRODUCT	DESCRIPTION	OBTAINED VIA	PREVALENCE STATS (LAST WEEK)	PREVALENCE STATS SOURCE	PREVALENCE STATS DATE	PREVALENCE RATING
12	EasyDVDtoVCD.exe	Easy DVD to VCD Burner	Copy DVD movies to VCD, SVCD, or AVI files and burn them to CD-R/RW.	Download.com	250	Download.com	30/06/2010	Medium Impact
13	anti_mosquito.zip	Anti Mosquito Software 1.0	This is a small software that shall drive the mosquitoes away fast. Simple to use and useful. No need for any external devices.	Download.com	2,424	Download.com	30/06/2010	High Impact
14	AutoClick_setup.exe	AutoClick 1.0.7.234	Have mouse clicks done for you when you're unable to click.	Download.com	1,390	Download.com	30/06/2010	High Impact
15	gardenplanner24setup.exe	Garden Planner 2.4	Design and print your own garden plan.	Download.com	1,086	Download.com	30/06/2010	High Impact
16	RealPlayerSPGold.exe	RealPlayer SP	Watch your favorite videos on your favorite devices	Download.com	120,383	Download.com	05/07/2010	Very High Impact
17	WWPC-Setup.exe	WW Points Calc	Calculate your weight watchers points.	Download.com	418	Download.com	30/06/2010	Medium Impact
18	bookcat_setup.exe	BookCAT	Catalog and manage your book collection.	Download.com	114	Download.com	30/06/2010	Medium Impact
19	newzcrawler19.msi	NewzCrawler	Web/RSS newsreader, content gatherer & browser.	Download.com	305	Download.com	30/06/2010	Medium Impact
20	TweetDeck_0_34.3.zip or air	TweetDeck 0.34.3	Social networking	Download.com	1,291	Download.com	02/07/2010	High Impact
21	cpuz_154_setup.exe	CPU-Z	Access various information about your computer.	Download.com	10,307	Download.com	02/07/2010	High Impact
22	defragsetup.exe	Smart Defrag	Defrag your hard drive in the background automatically.	Download.com	11,795	Download.com	02/07/2010	High Impact
23	PandoraRecovery2.1.1Setup.exe	Pandora Recovery	Find, preview and restore permanently deleted files.	Download.com	13,451	Download.com	02/07/2010	High Impact
24	disk-defrag-setup.exe	Auslogics Disk Defrag	Defragment your disks and improve computer performance and stability.	Download.com	44,529	Download.com	02/07/2010	Very High Impact
25	revosetup.exe	Revo Uninstaller	Uninstall unwanted and even broken applications accurately.	Download.com	18,853	Download.com	02/07/2010	High Impact
26	RegpairSetup.exe	Free Window Registry Repair	Registry repair utility	Download.com	7,681	Download.com	02/07/2010	High Impact

INCIDENT	ORIGINAL FILE NAME	PRODUCT	DESCRIPTION	OBTAINED VIA	PREVALENCE STATS (LAST WEEK)	PREVALENCE STATS SOURCE	PREVALENCE STATS DATE	PREVALENCE RATING
27	vlc-1.1.0-win32.exe	VLC Media Player	Play audio and video files in real-time and streaming modes.	Download.com	198,019	Download.com	02/07/2010	Very High Impact
28	media.player.codec.pack.v3.9.6.setup.exe	Media Player Codec Pack	Play various types of video, audio, movie, music files in Media Player	Download.com	43,780	Download.com	02/07/2010	Very High Impact
29		iPad to PC Transfer	Transfer files to the iPad	http://www.mp4converter.net/downloads/m-ipad-to-pc-transfer.exe	31	Download.com	05/07/2010	Low Impact
30	TrueCrypt%2BSetup%2B6.3a.exe	TrueCrypt	Encrypt your sensitive data with this open-source software	Download.com	1,574	Download.com	02/07/2010	High Impact
31	AdbeRdr930_en_US.exe	Adobe Reader 9.3	View, navigate, and print PDF files.	Adobe.com	97,971	Download.com	02/07/2010	Very High Impact
32	office-convert-pdf-to-jpg-jpeg-tiff-free.exe	Office Convert PDF to JPG JPEG TIFF Free	Convert your PDF files into various image formats.	Download.com	6,190	Download.com	02/07/2010	High Impact
33	-	Linksys WUSB600N Setup Wizard	Wireless router setup program	DVD	100	est	02/07/2010	Medium Impact
34	-	Billion BiPAC 6200NX(L) 3G Management Center	Wireless router setup program	DVD	100	est	02/07/2010	Medium Impact
35	ADM_en-EU.exe	Acronis Drive Monitor	Disk monitoring utility	http://www.acronis.co.uk/enterprise/download/drive-monitor/index.html	50	est	02/07/2010	Low Impact
36	mozy-2_0_12_3-12645.exe	MozyHome	Online backup	https://mozy.com/downloads/mozy-2_0_12_3-12645.exe	100	est	02/07/2010	Medium Impact

INCIDENT	ORIGINAL FILE NAME	PRODUCT	DESCRIPTION	OBTAINED VIA	PREVALENCE STATS (LAST WEEK)	PREVALENCE STATS SOURCE	PREVALENCE STATS DATE	PREVALENCE RATING
37	coreftplite.exe	Core FTP LE	Manage your files remotely and securely via FTP with SFTP, SSL, and HTTPS.	Download.com	2,374	Download.com	02/07/2010	High Impact
38	GoogleEarthSetup.exe	Google Earth	Mapping	http://earth.google.co.uk/download-earth.html	20988	est	02/07/2010	Very High Impact
39	install_bbc_alerts_news_national.exe	BBC Alerts	News ticker	http://news.bbc.co.uk/1/hi/help/4735697.stm	1000	est	02/07/2010	High Impact
40	IE8-eBay-WindowsXP-x86-ENGB.exe	IE8 for eBay	eBay Browser UK	http://www.ieaddons.com/get/?id=46&version=1	10000	est	02/07/2010	High Impact

APPENDIX C: THREAT REPORT

Code	Product	Code	Product	Code	Product
K7	K7 Total Security 10	MSE	Microsoft Security Essentials	TIS	Trend Micro Internet Security 2010
KIS	Kaspersky Internet Security 2011	NIS	Norton Internet Security 2010		
MIS	McAfee Internet Security 2010	PIS	Panda Internet Security 2010		

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

In cases where the malware fails for any reason, the product is given the full benefit of the doubt and is classified as having Defended with full remediation.

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
1	K7	None	None	None	0	None	None	None				1
1	KIS	Toaster	Denied	Denied: Trojan-Dropper.Win32.Drooptroop.cpt	0	n/a	n/a	n/a	1	1		
1	MIS	None	None	None	0	None	None	None				1
1	MSE	Toaster	Removed	Microsoft Security Essentials detected potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action. Detected items: Trojan:Win 32/Bamital.E. Alert level: Severe. Prompt to remove.	0	n/a	n/a	n/a	1	1		
1	PIS	Pop-up	Delete	Spyware detected! Spyware/Virtumonde	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
1	NIS	Toaster	Removed	SONAR detected security risk 0.054269438193954134.exe. A program was behaving suspiciously on your computer. You chose to block and remove it.	0	n/a	n/a	n/a	1	1		
1	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
2	K7	Toaster	Removed	High Security Risk Found	0	System Monitor Alert! New AutoStart Entry Found!	None	None				1
2	KIS	Toaster	Denied	Denied: HEUR:Trojan-Downloader.Script.Generic	0	n/a	n/a	n/a	1	1		
2	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
2	MSE	Toaster	Removed	TrojanDownloader:Win32/ Bredolab.AA; Exploit:JS/ CVE-2010-0886. Alert level: Severe. Prompt to remove.	0	n/a	n/a	n/a	1	1		
2	PIS	Toaster	Neutralized	A virus has been detected and the file has been disinfected	0	Report	Quarantine	Suspicious file			1	
2	NIS	Toaster	Blocked	Severity: High. An intrusion attempt by 192.168.1.18 was blocked. Risk name: HTTP Java Deployment Toolkit Input Invalidation	0	n/a	n/a	n/a	1	1		
2	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
3	K7	None	None (see note)	None	1	None	None	None	1	1		
3	KIS	Multiple (see note)	Denied	Toaster reported that HEUR:Trojan-Downloader.Script.Generic was detected. Web page was blocked with an "Access Denied" message.	0	n/a	n/a	n/a	1	1		
3	MIS	Pop-up	Removed	Detected: Exploit-PDF.bs!stream (Trojan)	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
3	MSE	None	None (see note)	None	1	None	None	None	1	1		
3	PIS	Toaster	Blocked	Unknown virus blocked	0	Report	Deleted	Trj/CI.A				1
3	NIS	Browser	Multiple (see note)	Site is Unsafe. Computer Threats: 33	0	n/a	n/a	n/a	1	1		
3	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
4	K7	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
4	KIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
4	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
4	MSE	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
4	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
4	NIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
4	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
5	K7	Toaster	Blocked	High Security Risk Found	0	n/a	n/a	n/a	1	1		
5	KIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
5	MIS	Pop-up	Blocked	Script Blocked: JS/Redirector.a (Trojan)	0	n/a	n/a	n/a	1	1		
5	MSE	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
5	PIS	Toaster	Blocked	Suspicious program detected	0	Report	Deleted	Trj/CI.A				1
5	NIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
5	TIS	None	None	None	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
6	K7	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
6	KIS	Multiple (see note)	Denied	Toaster reported that http://hqexgirl.osa.pl/ was denied (analysis according to the base of phishing web addresses). Web page was blocked with an "Access Denied" message.	0	n/a	n/a	n/a	1	1		
6	MIS	None	None	None	0	None	None	None				1
6	MSE	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
6	PIS	None	None	None	0	None	None	None				1
6	NIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
6	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1		1	
7	K7	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
7	KIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
7	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
7	MSE	None	None (see note)	None	0	None	None	None				1
7	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
7	NIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
7	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
8	K7	Toaster	Detected	High Security Risk Found	0	None	None	Scan Completed. No Viruses, spyware or other risks were found.				1
8	KIS	Toaster	Denied	Detected: Packed.JS.Agent.cl	0	n/a	n/a	n/a	1	1		
8	MIS	Toaster	Multiple (see note)	Detected: TrojanDownloader:HTML/Renos	0	n/a	n/a	n/a	1	1		
8	MSE	Toaster	Multiple (see note)	Detected: TrojanDownloader:HTML/Renos	0	n/a	n/a	n/a	1	1		
8	PIS	Toaster	Blocked	Risk Name: HTTP Fake Scan Webpage 5; Severity: High	0	n/a	n/a	n/a	1	1		
8	NIS	Toaster	Blocked	Risk Name: HTTP Fake Scan Webpage 5; Severity: High	0	n/a	n/a	n/a	1	1		
8	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
9	K7	Toaster	Removed	High Security Risk Found	0	None	None	Scan Completed. No Viruses, spyware or other risks were found.	1	1		
9	KIS	Multiple (see note)	Denied	Toaster reported that http://microsoft.msn.confu.info/?data=MigH... (analysis according to the base of suspicious URLs). Web page was blocked with an "Access Denied" message.	0	n/a	n/a	n/a	1	1		
9	MIS	Pop-up	Blocked	Generic FakeAlert (Trojan)	0	n/a	n/a	n/a	1	1		
9	MSE	Toaster	Detected	Microsoft Security Essentials detected 2 potential threats. Click 'Clean computer' to remove these threats.	0	None	None	No threats were detected on your computer during this scan.				1

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
9	PIS	Pop-up	Detected	Generic Malware	0	n/a	n/a	n/a	1	1		
9	NIS	Toaster	Blocked	Risk Name: HTTP Misleading Application Download Request. Severity: High	0	n/a	n/a	n/a	1	1		
9	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
10	K7	Toaster	Removed	High Security Risk Found	0	n/a	n/a	n/a	1	1		
10	KIS	Toaster	Denied	Denied: htp//tradbox.net/doxt/pWtl (analysis using the database of suspicious URLs)	0	n/a	n/a	n/a	1	1		
10	MIS	Pop-up	Prevented	Buffer Overflow Prevented	0	n/a	n/a	n/a	1	1		
10	MSE	Toaster	Removed	Microsoft Security Essentials detected potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action. Detected items: Exploit:HTML/IframeRef.gen . Alert level: Severe. Prompt to remove.	0	n/a	n/a	n/a	1	1		
10	PIS	Toaster	Blocked	Dangerous operation blocked	0	n/a	n/a	n/a	1	1		
10	NIS	Browser	Blocked	Critical attack prevented. Norton Internet Security has blocked a critical attack and needs to close your browser. Signature ID: UXP Detection 5900#	0	n/a	n/a	n/a	1	1		
10	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
11	K7	Toaster	Removed (see note)	High Security Risk Found	0	n/a	n/a	n/a			1	
11	KIS	Multiple (see note)	Denied	Toaster reported that http://microsoft.msn.confu.info/?data= MigH . . . (analysis using the database of suspicious URLs) was denied. Web page was blocked with an "Access Denied" message.	0	n/a	n/a	n/a	1	1		
11	MIS	Pop-up	Blocked	Generic FakeAlert (Trojan)	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
11	MSE	Toaster	Removed	Detected: TrojanSpyWin32/Chadem.A and Trojan:Win32/InternetAntiVirus	0	None	None	No threats were detected on your computer during this scan.			1	
11	PIS	Toaster	Neutralized	A virus has been detected and the file has been disinfected	0	n/a	n/a	n/a	1		1	
11	NIS	Toaster	Blocked	An intrusion attempt by TESTTPC was blocked. Risk name: HTTP Misleading Application Download Request	0	n/a	n/a	n/a	1	1		
11	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
12	K7	Toaster	Multiple (see note)	High Security Risk Found	0	None	None	Scan Completed. No Viruses, spyware or other risks were found.			1	
12	KIS	Toaster	Denied	Denied: HEUR:Trojan-Downloader.Script.Generic	0	n/a	n/a	n/a	1	1		
12	MIS	Pop-up	Removed	Artemis!DAC933490737 (Trojan)	0	n/a	n/a	n/a	1	1		
12	MSE	Toaster	Removed	Microsoft Security Essentials detected 2 potential threats. Click 'Clean computer' to remove these threats. Detected items: Trojan:Win32/Meredrop; VirTool:J5/Obfuscator.5; Exploit:JS/CVE-2010-0886		n/a	n/a	n/a	1	1		
12	PIS	Toaster	Neutralized	Suspicious file neutralized	0	n/a	n/a	n/a	1		1	
12	NIS	Toaster	Blocked	An intrusion attempt by 192.168.1.18 was blocked. Risk name: HTTP Java Deployment Toolkit Input Invalidation	0	n/a	n/a	n/a	1	1		
12	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
13	K7	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
13	KIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
13	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
13	MSE	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
13	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
13	NIS	Toaster	Blocked	An intrusion attempt by 192.168.1.18 was blocked. Risk name: HTTP Fake Scan Webpage 5	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
13	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
14	K7	Toaster	Detected	High Security Risk Found	0	TaskManager Viewing has been disabled	No action taken	Suspicious:Can cause problems!				1
14	KIS	Toaster	Denied	Denied: Packed.JS.Agent.cl and Trojan.Win32.TD55.bhli	0	n/a	n/a	n/a	1	1		
14	MIS	Browser	Close this webpage (Recommended)	Potentially Dangerous Web Site	0	n/a	n/a	n/a	1	1		
14	MSE	Toaster	Removed	Microsoft Security Essentials detected 2 potential threats. Click 'Clean computer' to remove these threats. Detected items: Trojan:Win32/Alureon.gen!3 and Trojan:Win32/FakeCog. Trojan:Win32/FakeCog	0	Yes	Removed; Quarantined; Removed; Removed	Detected items: Trojan:Win32/Alureon.gen!3; Trojan:Win32/FakeCog; Trojan:Win32/Alureon.DK; Tojan:Win32/FakeCog;				1
14	PIS	Toaster	Neutralized	Suspicious file neutralized	0	n/a	n/a	n/a			1	
14	NIS	Toaster	Blocked	An intrusion attempt by 192.168.1.18 was blocked. Risk name: HTTP Fake Scan Webpage 5	0	n/a	n/a	n/a	1	1		
14	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
15	K7	Toaster	File not found	High Security Risk Found	0	None	None	Scan Completed. No Viruses, spyware or other risks were found.			1	
15	KIS	Multiple (see note)	Denied	Denied: http://bestmediaagency.com/New-Video-Addon.45048.exe (analysis using the database of suspicious URLs)	0	n/a	n/a	n/a	1	1		
15	MIS	None	None	None	0	None	None	None				1
15	MSE	Toaster	Removed	Detected items: Trojan Downloader:Win32/Renos.KO	0	None	None	No threats were detected on your computer during this scan.	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
15	PIS	None	None	None	0	Report	Multiple	Multiple			1	
15	NIS	Toaster	Detected	new-video-addon.45048[1].exe. This Insight Network Threat has been detected. There are many indications that this file is untrustworthy and therefore not safe.	0	n/a	n/a	n/a	1	1		
15	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
16	K7	Toaster	Multiple (see note)	High Security Risk Found	0	TaskManager Viewing has been disabled	No action taken	Suspicious: Can cause problems!				1
16	KIS	Toaster	Denied	Denied: Packed.JS.Agent.cl and Trojan.Win32.TD55.bhli	0	n/a	n/a	n/a	1	1		
16	MIS	Pop-up	Blocked	JS/Redirector.a (Trojan)	0	n/a	n/a	n/a	1	1		
16	MSE	Toaster	Removed	Detected items: Trojan:Win32/Alureon.DA	0	n/a	n/a	n/a	1	1		
16	PIS	Toaster	Neutralized	Suspicious file neutralized	0	n/a	n/a	n/a	1		1	
16	NIS	Toaster	Blocked	An intrusion attempt by 192.168.1.18 was blocked. Risk Name: HTTP Fake Scan Webpage 5	0	n/a	n/a	n/a	1	1		
16	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
17	K7	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
17	KIS	Multiple (see note)	Denied	Denied: Trojan-Downloader.JS.Pegel.g	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
17	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
17	MSE	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
17	PIS	None	None	None	0	None	None	None	1	1		
17	NIS	Multiple (see note)	Blocked	Critical attack prevented. Norton Internet Security has blocked a critical attack and needs to close your browser. Signature ID: Adobe Reader GetIconBO	0	n/a	n/a	n/a	1	1		
17	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
18	K7	Toaster	Detected	High Security Risk Found	0	None	None	Scan Completed. No Viruses, spyware or other risks were found.	1	1		
18	KIS	Multiple (see note)	Denied	Denied: Trojan-Downloader.Win32.CodecPack.lzl	0	n/a	n/a	n/a	1	1		
18	MIS	Pop-up	Removed	Downloader-CEW.e (Trojan)	0	n/a	n/a	n/a	1	1		
18	MSE	Toaster	Removed	Detected items: TrojanDownloader:Win32/Renos.KO	0	n/a	n/a	n/a	1	1		
18	PIS	Toaster	Neutralized	Trj/Zlob.QL	0	n/a	n/a	n/a	1		1	
18	NIS	Pop-up	Blocked	Site is Unsafe. Computer Threats: 2	0	n/a	n/a	n/a	1	1		
18	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
19	K7	Toaster	Detected	High Security Risk Found	0	Riskware (d2f5362e0)	Removed	Scan Completed. All security risks were removed successfully.			1	
19	KIS	Multiple (see note)	Denied	Denied: http://microsoft.msn.com.eround.info/?data=MigH . . . (analysis according to the base of suspicious web addresses)	0	n/a	n/a	n/a	1	1		
19	MIS	Pop-up	Blocked	Generic FakeAlert (Trojan)	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
19	MSE	Toaster	Removed	Detected items: TrojanSpy:Win32/Chadem.A; Trojan:Win32/Internet/Antivirus and Trojna:WinNT/Alureon.H	0	None	None	No threats were detected on your computer during this scan.			1	
19	PIS	Pop-up	Detected	Trj/TDSS.EO	0	n/a	n/a	n/a	1	1		
19	NIS	Toaster	Blocked	An intrusion attempt by TESTPC was blocked. Risk name: HTTP Misleading Application Download Request	0	n/a	n/a	n/a	1	1		
19	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
20	K7	Toaster	Detected	High Security Risk Found	0	n/a	n/a	n/a	1	1		
20	KIS	Toaster	Denied	Denied: http://dmanaver.com/get.php?id=2 (analysis using the database of suspicious URLs)	0	None	None	No active threats.				1
20	MIS	None	None	None	0	None	None	None				1
20	MSE	Toaster	Removed	Detected items: TrojanDownloader:Win32/Renos.KO	0	n/a	n/a	n/a	1	1		
20	PIS	Toaster	Neutralized	Suspicious file neutralized	0	Report	Multiple	Multiple				1
20	NIS	Toaster	Blocked	An intrusion attempt by 19.168.1.18 was blocked. Risk name: HTTP Fake Codec Request Generic	0	n/a	n/a	n/a	1	1		
20	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
21	K7	Toaster	Removed	High Security Risk Found	0	n/a	n/a	n/a	1	1		
21	KIS	Toaster	Denied	Denied: http://iopap.upperdarby26.com/CD_ROM.js (analysis according to the database of phishing web addresses)	0	n/a	n/a	n/a	1	1		
21	MIS	Pop-up	Blocked	Exploit-HelpOverflow (Trojan)	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
21	MSE	Toaster	Removed	Detected items: Exploit:JS/CVE-2010-0886	0	n/a	n/a	n/a	1	1		
21	PIS	Toaster	Blocked	Dangerous operation blocked	0	n/a	n/a	n/a	1		1	
21	NIS	Toaster	Blocked	An intrusion attempt by 19.168.1.18 was blocked. Risk name: HTTP Java Deployment Toolkit Input Invalidation	0	n/a	n/a	n/a	1	1		
21	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
22	K7	Toaster	Detected	High Security Risk Found	0	n/a	n/a	n/a	1	1		
22	KIS	Multiple (see note)	Denied	Denied: http://microsoft.msn.com.eround.info/?data=MigH . . . (analysis according to the base of suspicious web addresses)	0	n/a	n/a	n/a	1	1		
22	MIS	Pop-up	Blocked	Generic FakeAlert (Trojan)	0	n/a	n/a	n/a	1	1		
22	MSE	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
22	PIS	Pop-up	Detected	Trj/TDSS.EO	0	n/a	n/a	n/a	1	1		
22	NIS	Toaster	Blocked	An intrusion attempt by 19.168.1.18 was blocked. Risk name: HTTP Misleading Application Download Request	0	n/a	n/a	n/a	1	1		
22	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
23	K7	Toaster	Removed	High Security Risk Found	0	n/a	n/a	n/a	1	1		
23	KIS	Toaster	Denied	Denied: http://08.spkey.in/x/index.php (analysis using the database of suspicious web addresses)	0	n/a	n/a	n/a	1	1		
23	MIS	Pop-up	Removed	Artemis!580DCFEF2ABE (Trojan)	0	n/a	n/a	n/a	1	1		
23	MSE	Toaster	Removed	Detected items: Trojan:Win32/Bamital.E	0	n/a	n/a	n/a	1	1		
23	PIS	Toaster	Neutralized	Virus neutralized (Trj/Dropper.WF)	0	n/a	n/a	n/a	1		1	
23	NIS	Toaster	Removed	SONAR detected security risk 0.505300327150144.exe.	0	n/a	n/a	n/a	1	1		
23	TIS	None	None	None	1	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
24	K7	Pop-up	Detected (see note)	System Monitor Alert	0	None	None	Scan completed. No viruses, spyware or other risks were found.				1
24	KIS	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
24	MIS	None	None	None	0	None	None	None	1	1		
24	MSE	None	None (see note)	None	1	n/a	n/a	n/a	1	1		
24	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
24	NIS	Toaster	Blocked	An intrusion attempt by 19.168.1.18 was blocked. Risk name: HTTP Fake Scan Webpage 5	0	n/a	n/a	n/a	1	1		
24	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
25	K7	Pop-up	Detected	Prompt to allow	0	None	None	Scan completed. No viruses, spyware or other risks were found.			1	
25	KIS	Multiple (see note)	Denied	Denied: Trojan.JS.Iframe.md	0	n/a	n/a	n/a	1	1		
25	MIS	None	None	None	0	None	None	None	1	1		
25	MSE	Toaster	Removed	Detected items: TrojanDownloader:Win32/Genome.I	0	n/a	n/a	n/a	1	1		
25	PIS	None	None	None	0	None	None	None	1	1		
25	NIS	Toaster	Removed	SONAR detected security risk 0.547153785739459.exe.	0	n/a	n/a	n/a	1	1		
25	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
26	K7	Toaster	Detected	High Security Risk Found	0	n/a	n/a	n/a	1	1		
26	KIS	Toaster	Detected	Denied: Trojan.Win32.Tdss.beea	0	n/a	n/a	n/a	1	1		
26	MIS	Pop-up	Blocked	Generic FakeAlert (Trojan)	0	n/a	n/a	n/a	1	1		
26	MSE	Toaster	Removed	Detected items: Trojan:Win32/InternetAntiVirus, TrojanSpy:Win32/ChademA and Win32/Alureon.H	0	Yes	Disinfect	Detected items: Virus:Win32/Alureon.H			1	
26	PIS	Pop-up	Detected	Trj/TDSS.EO	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
26	NIS	Toaster	Blocked	An intrusion attempt by TESTPC was blocked. Risk name: HTTP Misleading Application Download Request	0	n/a	n/a	n/a	1	1		
26	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
27	K7	Toaster	Detected	High Security Risk Found	0	n/a	n/a	n/a	1	1		
27	KIS	Multiple (see note)	Denied	Detected: Trojan-Downloader.Win32.CodecPack.lzl	0	n/a	n/a	n/a	1	1		
27	MIS	Pop-up	Removed	Downloader-CEW.e (Trojan)	0	n/a	n/a	n/a	1	1		
27	MSE	Toaster	Removed	Detected items: TrojanDownloader:Win3/Renos.KO	0	n/a	n/a	n/a	1	1		
27	PIS	Pop-up	Neutralized	Trj/Zlob.QL	0	n/a	n/a	n/a	1	1		
27	NIS	Pop-up	Removed	Site is unsafe. Computer Threats: 3. This virus has been removed: install.48728[1].exe (Trojan.FakeA!gen30)	0	n/a	n/a	n/a	1	1		
27	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerous	0	n/a	n/a	n/a	1	1		
28	K7	Toaster	Detected	High Security Risk Found	0	n/a	n/a	n/a	1	1		
28	KIS	Multiple (see note)	Denied	Denied: Trojan.Win32.Tdss.beea	0	n/a	n/a	n/a	1	1		
28	MIS	Pop-up	Blocked	Generic FakeAlert (Trojan)	0	n/a	n/a	n/a	1	1		
28	MSE	Toaster	Removed	Trojan: Win32/InternetAntiVirus	0	Yes	Removed; Removed; Quarantined	Detected items: TrojanSpy:Win32/Chadem.A; Trojan:Win32/InternetAntiVirus; Virus:Win32/Alureon.H			1	
28	PIS	Pop-up	Detected	Trj/TDSS.EO	0	n/a	n/a	n/a	1	1		
28	NIS	Toaster	Blocked	An intrusion attempt by TESTPC was blocked. Risk name: HTTP Misleading Application Download Request	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
28	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
29	K7	Toaster	Detected	High Security Risk Found	0	None	None	Scan completed. No viruses, spyware or other risks were found.			1	
29	KIS	Toaster	Detected	Detected: Trojan-Downloader.JS.Pegel.b	0	n/a	n/a	n/a	1	1		
29	MIS	Pop-up	Blocked	Exploit-HelpOverflow (Trojan)	0	n/a	n/a	n/a	1	1		
29	MSE	Toaster	Removed; Not found	Detected items: Trojan:Win32/Meredrop; Exploit:JS/CVE-2010-0886	0	None	None	No threats were detected on your computer during this scan.			1	
29	PIS	Toaster	Blocked	Dangerous operation blocked	0	None	None	None			1	
29	NIS	Toaster	Blocked	An intrusion attempt by TESTPC was blocked. Risk name: HTTP Nukesploit Request	0	n/a	n/a	n/a	1	1		
29	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
30	K7	Pop-up	Allowed	System Monitor Alert! Iexplorer Zone Settings have been modified. Prompt to allow.	0	None	None	Scan completed. No viruses, spyware or other risks were found.			1	
30	KIS	Toaster	Detected	Detected: Trojan-/spy.Win32.Zbot.akuu	0	None	None	Your computer is protected.			1	
30	MIS	Pop-up	Removed	Artemis!28E2B2498484 (Trojan)	0	None	None	None			1	
30	MSE	Toaster	Removed	Detected items: PWS:Win32/Zbot.gen!Y	0	n/a	n/a	n/a	1	1		
30	PIS	Toaster	Blocked	Dangerous operation blocked	0	n/a	n/a	n/a	1	1		
30	NIS	Toaster	Removed	SONAR removed security risk. A program was behaving suspiciously on your computer. You chose to block and remove it.	0	n/a	n/a	n/a	1	1		
30	TIS	None	None	None	1	None	None	None	1	1		
31	K7	Toaster	Detected	High Security Risk Found	0	n/a	n/a	n/a	1	1		
31	KIS	Toaster	Denied	Denied: Net-Worm.JS.Aspxor.a	0	n/a	n/a	n/a	1	1		
31	MIS	None	None	None	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
31	MSE	None	None	None	1	None	None	No threats were detected on your computer during this scan.	1	1		
31	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
31	NIS	Toaster	Blocked	An intrusion attempt by 192.168.1.18 was blocked. Risk name: HTTP Eleonore Toolkit Activity	0	n/a	n/a	n/a	1	1		
31	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
32	K7	None	None	None	1	n/a	n/a	n/a	1	1		
32	KIS	None	None	None	1	n/a	n/a	n/a	1	1		
32	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
32	MSE	None	None	None	1	n/a	n/a	n/a	1	1		
32	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
32	NIS	Toaster	Blocked	An intrusion attempt by 192.168.1.18 was blocked. Risk Name: HTTP Fake Scan Webpage 5	0	n/a	n/a	n/a	1	1		
32	TIS	None	None	None	0	n/a	n/a	n/a	1	1		
33	K7	Toaster	Detected	High Security Risk Found	0	n/a	n/a	n/a	1	1		
33	KIS	Toaster	Detected	Detected:Trojan.JS.Redirector.bu	0	n/a	n/a	n/a	1	1		
33	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
33	MSE	None	None	None	1	n/a	n/a	n/a	1	1		
33	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
33	NIS	Toaster	Blocked	An intrusion attempt by 192.168.1.18 was blocked. Risk Name: HTTP Fake Scan Webpage 5	0	n/a	n/a	n/a	1	1		
33	TIS	Pop-up	Found	JS FAKESCAN.SMI	0	n/a	n/a	n/a	1		1	
34	K7	Toaster	Detected	High Security Risk Found	0	n/a	n/a	n/a	1	1		
34	KIS	Toaster	Denied	Denied:Trojan.JS.Redirector.bu	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
34	MIS	Pop-up	Blocked	Generic FakeAlert (Trojan)	0	n/a	n/a	n/a	1	1		
34	MSE	Toaster	Removed	Detected items: Trojan:Win32/InternetAntiVirus; TrojanSpy:Win32/Chadem.A; Trojan:Win32/InternetAntiVirus	0	Yes	Removed TrojanSpy: Win32/Chadem.A; Removed Trojan:Win32/InternetAntiVirus;Quarantined: Virus:Win32/Alureon.H	Microsoft Security Essentials detected 3 potential threats on your computer.				1
34	PIS	Pop-up	Detected	Generic Malware	0	n/a	n/a	n/a	1	1		
34	NIS	Toaster	Blocked	An intrusion attempt by TESTPC was blocked. Risk Name: HTTP Misleading Application Download Request	0	n/a	n/a	n/a	1	1		
34	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
35	K7	Toaster	Detected	High Security Risk Found	0	Yes	None	Scan completed. No viruses, spyware or other risks were found.				1
35	KIS	Toaster	Denied	Denied: HEUR:Trojan.Script.Iframer	0	n/a	n/a	n/a	1	1		
35	MIS	Pop-up	Blocked	Exploit-HelpOverflow (Trojan)	0	n/a	n/a	n/a	1	1		
35	MSE	Toaster	Removed	Detected items: TrojanDownloader:Win32/Bredolab.AA ; Exploit:JS/CVE-2010-0886	0	None	None	No threats were detected on your computer during this scan.			1	
35	PIS	Toaster	Blocked	Dangerous operation blocked	0	n/a	n/a	n/a	1	1		
35	NIS	Toaster	Blocked	An intrusion attempt by TESTPC was blocked. Risk Name: HTTP Nukesploit Request	0	n/a	n/a	n/a	1	1		
35	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerou	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
36	K7	Toaster	Detected	High Security Risk Found	0	Yes	None	Scan completed. No viruses, spyware or other risks were found.			1	
36	KIS	Toaster	Detected	Detected: Exploit.JS.Agent.bav	0	n/a	n/a	n/a	1	1		
36	MIS	Pop-up	Prevented	Buffer Overflow Prevented	0	n/a	n/a	n/a	1	1		
36	MSE	Toaster	Removed	Detected items: TrojanDownloader:Win32/Genome.I	0	None	None	No threats were detected on your computer during this scan.			1	
36	PIS	None	None	None	0	None	None	None				1
36	NIS	Pop-up	Blocked	Critical attack prevented. Norton Internet Security has blocked a critical attack and needs to close your browser. Signature ID: UXP Detection 59000	0	None	None	No viruses or other security risks were found.	1	1		
36	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
37	K7	None	None	None	1	None	None	Scan completed. No viruses, spyware or other risks were found.	1	1		
37	KIS	Multiple (see note)	Detected	Detected: HEUR:Trojan.Script.Iframer	0	n/a	n/a	n/a	1	1		
37	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
37	MSE	None	None	None	1	None	None	No threats were detected on your computer during this scan.	1	1		
37	PIS	None	None	None	0	n/a	n/a	n/a	1	1		
37	NIS	None	None	None	1	None	None	No viruses or other security risks were found.	1	1		
37	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
38	K7	Toaster	Detected	High Security Risk Found	0	None	None	Scan completed. No viruses, spyware or other risks were found.			1	
38	KIS	Toaster	Denied	Denied: HEUR:Exploit.Script.Generic	0	n/a	n/a	n/a	1	1		
38	MIS	Pop-up	Blocked	Exploit-HelpOverflow (Trojan)	0	n/a	n/a	n/a	1	1		
38	MSE	Toaster	File not found	Detected items: Exploit:JS/CVE-2010-0886	0	None	None	No threats were detected on your computer during this scan.	1	1		
38	PIS	Toaster	Blocked	Dangerous operation blocked	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
38	NIS	Toaster	Blocked	An intrusion attempt by TESTPC was blocked. Risk Name: HTTP Nukesploit Request	0	n/a	it ran.	n/a	1	1		
38	TIS	None	None	None	1	n/a	n/a	n/a	1	1		
39	K7	Pop-up	Allowed	Application access with first option to allow	0	None	None	Scan completed. No viruses, spyware or other risks were found.			1	
39	KIS	Toaster	Denied	Denied: http://wepimi.in/x/?src=PsyInported&id=dm&o=o (analysis using the database of suspicious URLs)		n/a	n/a	n/a	1	1		
39	MIS	Pop-up	Prevented	Buffer Overflow Prevented	0	n/a	n/a	n/a	1	1		
39	MSE	Toaster	Removed	Detected items: TrojanDownloader:Win32/Genome.I	0	None	None	No threats were detected on your computer during this scan.			1	
39	PIS	None	None	None	0	Report	Neutralized	Suspicious file			1	
39	NIS	Pop-up	Blocked	Critical attack prevented. Norton Internet Security has blocked a critical attack and needs to close your browser. Signature ID: UXP Detection 59000	0	None	None	No viruses or other security risks were found.	1	1		
39	TIS	Browser	Blocked	Opening this website may put your security at risk: The website you wanted to see might transmit malicious software to your computer, or has done that before to someone else. It may also show signs of involvement in online scams or fraud. Rating: Dangerou	0	n/a	n/a	n/a	1	1		
40	K7	None	None	None	0	n/a	n/a	n/a	1	1		
40	KIS	Toaster	Detected	Detected: Trojan.JS.Redirector.cq	0	n/a	n/a	n/a	1	1		
40	MIS	None	None	None	0	n/a	n/a	n/a	1	1		
40	MSE	None	None	None	0	n/a	n/a	n/a	1	1		
40	PIS	None	None	None	0	n/a	n/a	n/a	1	1		

Incident	Product code	Alert (intro)	Effect (intro)	Threat Report (intro)	Logged only?	Alert (manual)	Effect (manual)	Threat Report (manual)	Complete Remediation?	Defended	Neutralized	Compromised
40	NIS	Toaster	Blocked	An intrusion attempt by 192.168.1.18 was blocked. Risk name: HTTP Misleading Application Page Request	0	n/a	n/a	n/a	1	1		
40	TIS	None	None	None	1	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.