MRG Effitas

Efficacy Assessment & Assurance

Comparative Assessment of GFI VIPRE Antivirus Premium

September 2011

Contents:

Introduction 3

Security Applications Tested 3

Methodology Used in the Test 3

Test Results 4

Conclusions 9

Introduction:

This report has been commissioned by GFI Software to serve as an independent, comparative efficacy assessment of the market leading internet security products including their own application, VIPRE Antivirus Premium, against a range of malware types which are representative of those prevalent in the current threat landscape.

In order to assess the applications under test in a way that most accurately maps to their usage in the real world and therefore yield the most meaningful results, three types of test were conducted:

- By malware type, i.e. assessing how each application performed against specific categories of malware, such as PUAs, exploits, worms etc.
- By malware age, i.e. assessing applications ability to detect early life to mid-life samples, giving an indication of their responsiveness to new threats.
- Static and dynamic tests. Dynamic testing represents how, in the real world, malware enters and infects a system. Static testing allows the use of a large number of samples and in so doing increases statistical significance.

Security Applications Tested:

The security applications tested and their versions were as follows:

1. Avast Avast Professional 6.0.1203
2. AVG Antivirus 10.0.1392/812
3. Avira AntiVir Premium 10.2.0.728
4. BitDefender Antivirus 15.0.16.280
5. Eset Nod32 Antivirus 4.2.71.2
6. GFI VIPRE Antivirus Premium 4.0.4210
7. Kaspersky AntiVirus 12.0.0.374
8. McAfee VirusScan Plus 4.5.147
9. Microsoft Security Essentials 2.1.116.0
10. Symantec Nortoan Antivirus 18.6.0.29
11. Trend Micro Titanium Antivirus+ 3.1.1109
12. Webroot Secure Anywhere 7.0.11.21

Methodology Used in the Test:

1. Windows 7 Service Pack 1 32 bit operating system is installed on a virtual machine and all updates are applied. Adobe Reader is installed.
2. An image of the operating systems is created.
3. Two clones of the imaged systems are made for each of the 12 security applications to be used in the test. One set of clones has a folder containing the samples for the static / age test copied to it.
4. An individual security application is installed using default settings on each of the systems created in step 3 and then updated.
5. A clone of the system as it is at the end of 4 is created.
6. The dynamic test is conducted by:
    a. Downloading the sample using Internet Explorer to the desktop, closing Internet Explorer and then executing the sample.
7. A test is deemed to have been passed by the following criteria:
    a. The security application detects the sample whilst it is being downloaded to the desktop.
    b. The security application detects the sample when it is executed according to the following criteria:

i. It identifies the sample as being malicious and either automatically blocks it or postpones its execution and warns the user that the file is malicious and awaits user input.

ii. In the case of PUAs, it automatically blocks the application, if allowed to install, from executing and warns the user of its malicious nature.

8. A test is deemed to have been failed by the following criteria:

    a. The security application fails to detect the sample under conditions 7a, 7b(i) or 7b(ii)

9. The static test is conducted by:

    a. Performing a context menu or on demand scan of a folder containing the samples which was placed on the desktop during stage 3. The security application is allowed to scan the system as many times as it requests in order to remove all the samples it is able to detect.

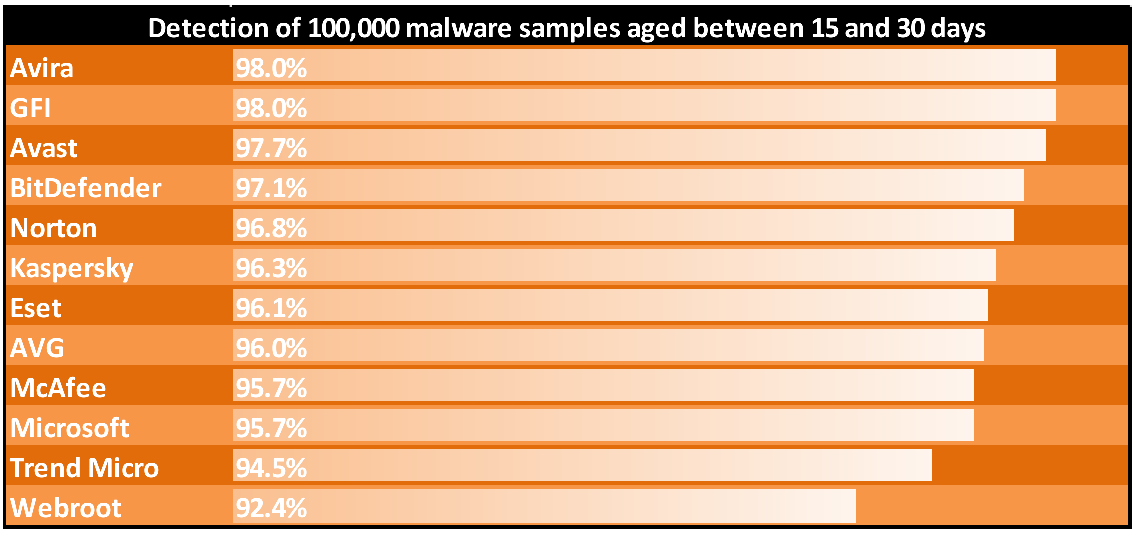
10. Testing is conducted with all systems having internet access.

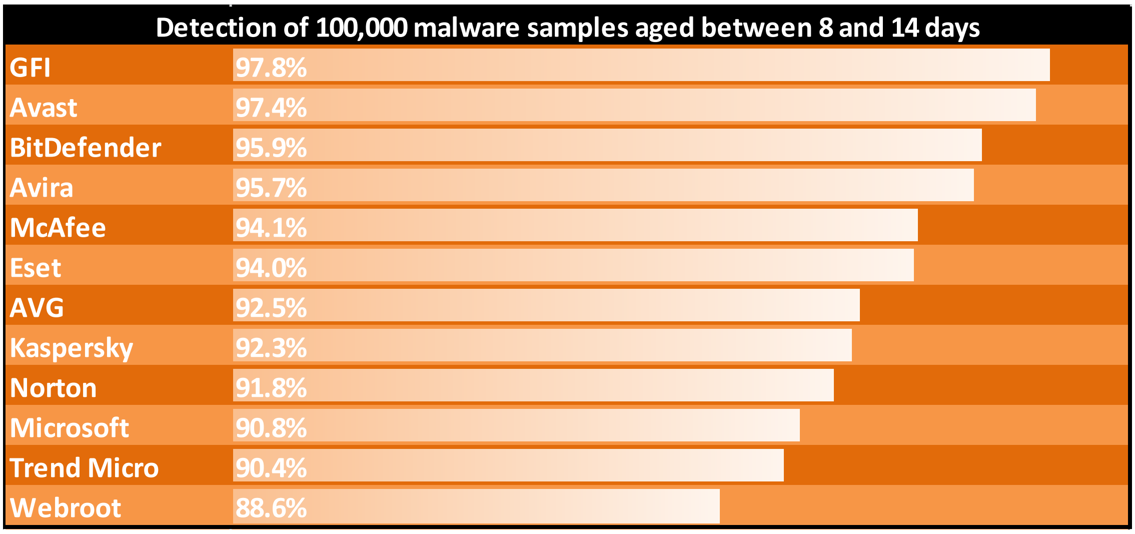
11. For dynamic testing, the IP address of the VM is changed for before downloading each sample.

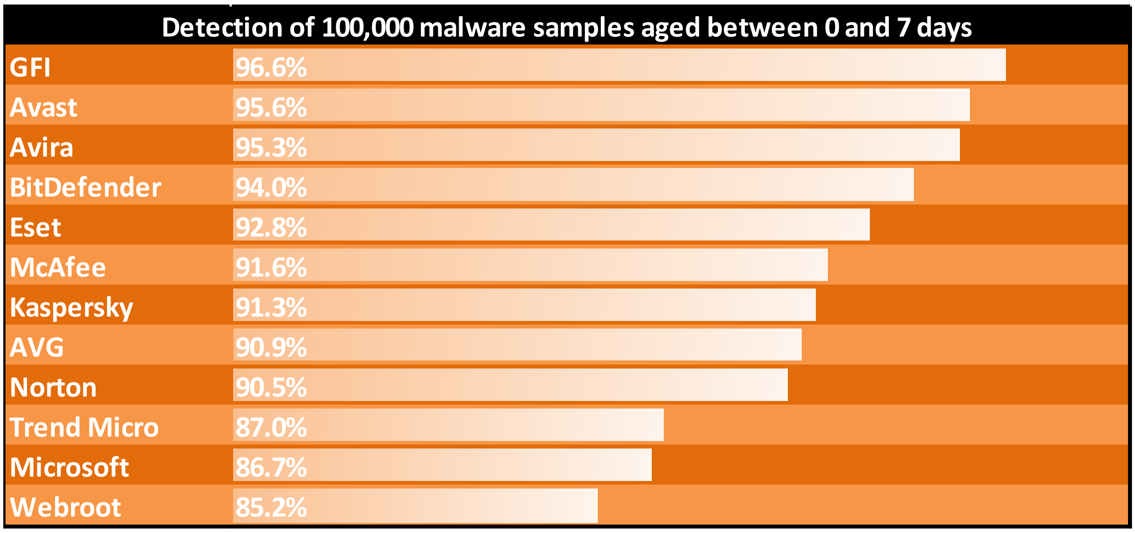
12. All security applications are fully functional unregistered versions or versions registered anonymously, with no connection to MRG Effitas.

Test Results:

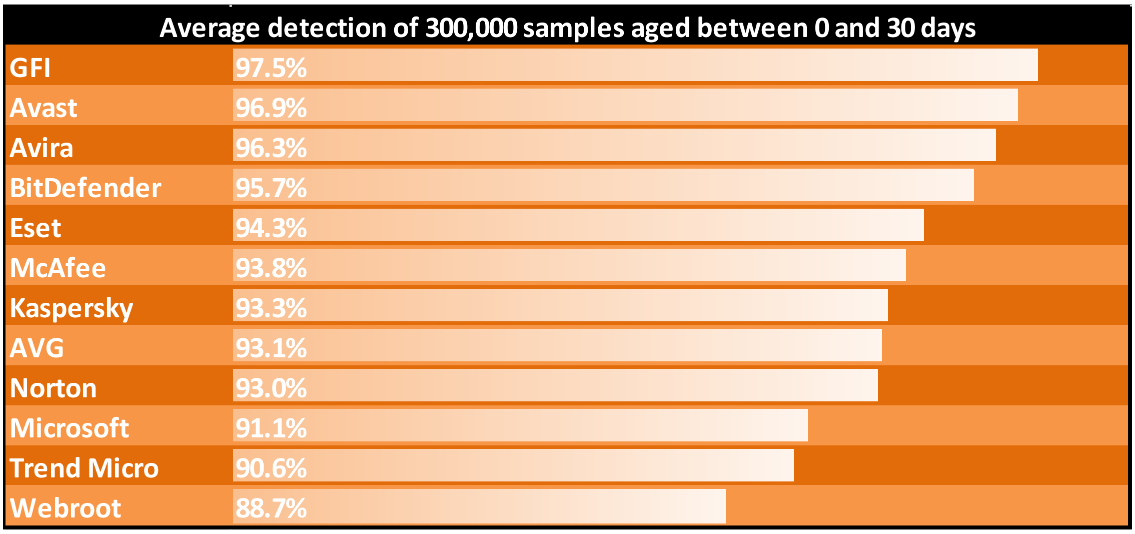
The tables below show the results of the static testing conducted on three age groups of samples. The samples were in groups of 100,000 and divided in to age groups of 0 – 7 days old, 8 – 14 days old and 15 – 30 days old and comprised of various malware types in their in the wild proportions.



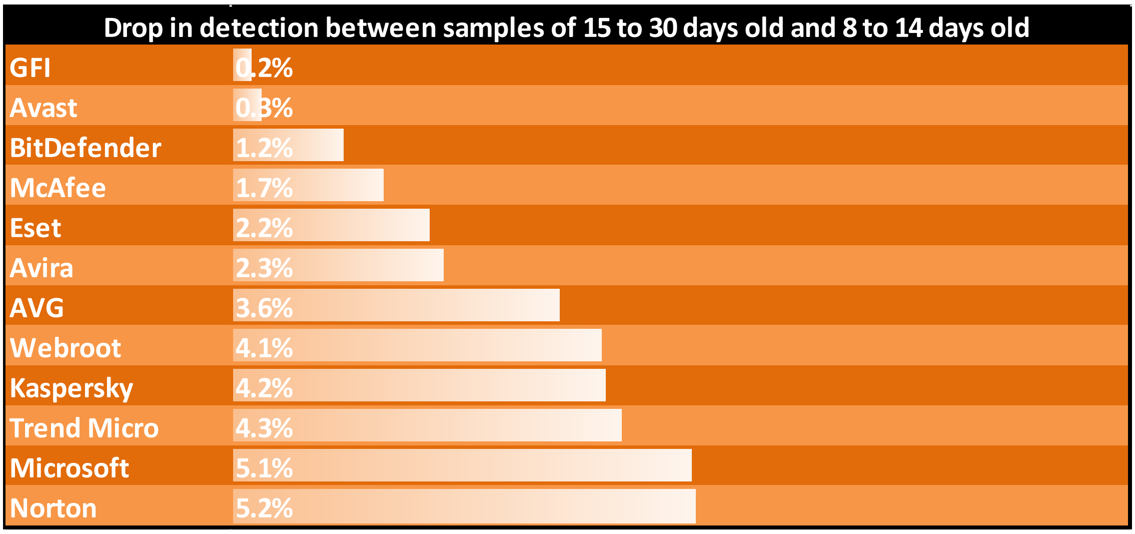



Detection of 100,000 malware samples aged between 0 and 7 days

The table below shows the average detection for all the samples used in the static test.


Average detection of 300,000 samples aged between 0 and 30 days

To clearly illustrate the drop in the applications ability to detect samples as their age decreases, the following two tables show the drop in detection between the age groups. (Lower % is better)

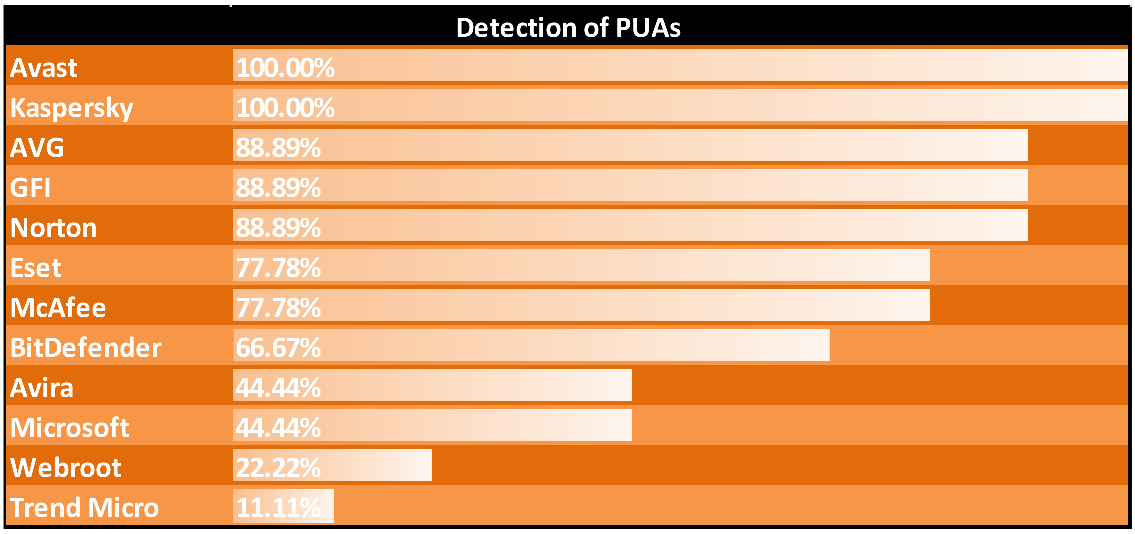

Drop in detection between samples of 15 to 30 days old and 8 to 14 days old

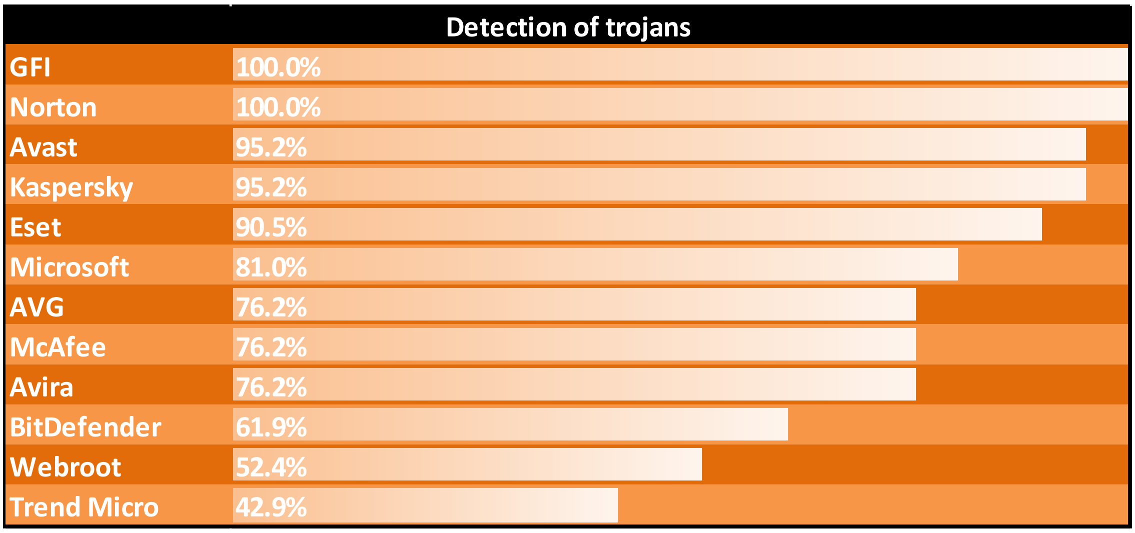
Drop in detection between samples of 15 to 30 days old and 0 to 7 days old	
GFI	1.4%
Avast	2.1%
Avira	2.8%
BitDefender	3.2%
Eset	3.4%
McAfee	4.3%
Kaspersky	5.2%
AVG	5.3%
Norton	6.5%
Webroot	7.8%
Trend Micro	7.9%
Microsoft	9.4%

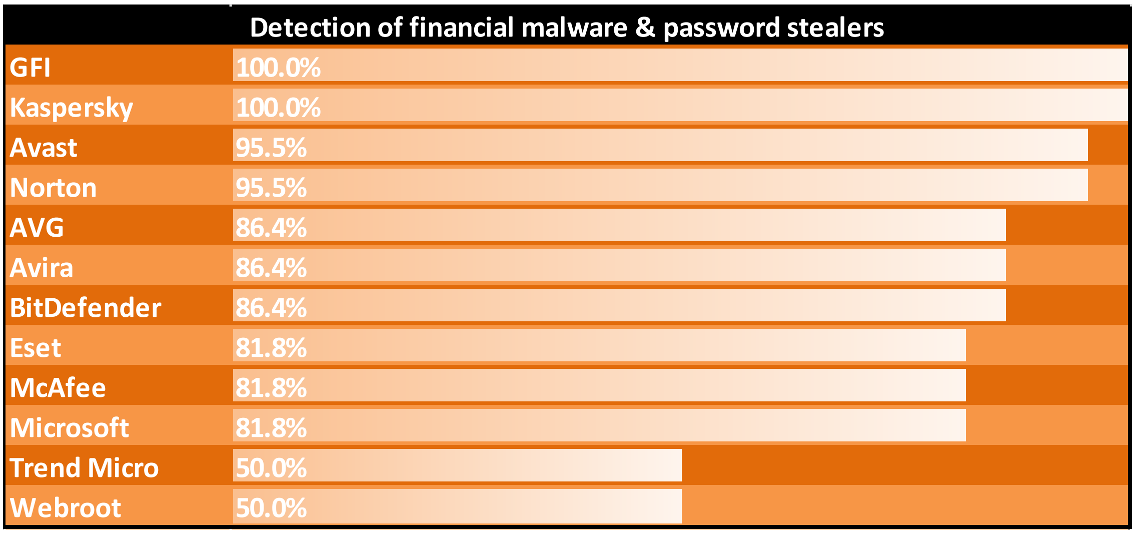
The following tables detail results from the dynamic testing using seven categories of malware. In total, 100 samples were used.

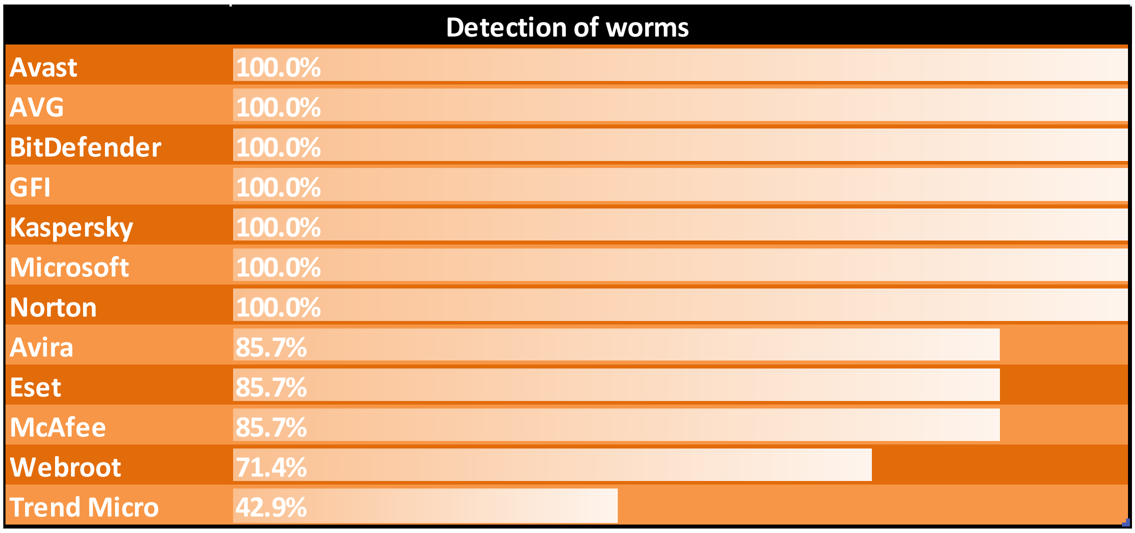
Detection of backdoors	
Avast	100.0%
GFI	100.0%
Microsoft	100.0%
Norton	100.0%
BitDefender	92.9%
Eset	92.9%
Kaspersky	92.9%
McAfee	92.9%
AVG	85.7%
Avira	85.7%
Trend Micro	64.3%
Webroot	57.1%

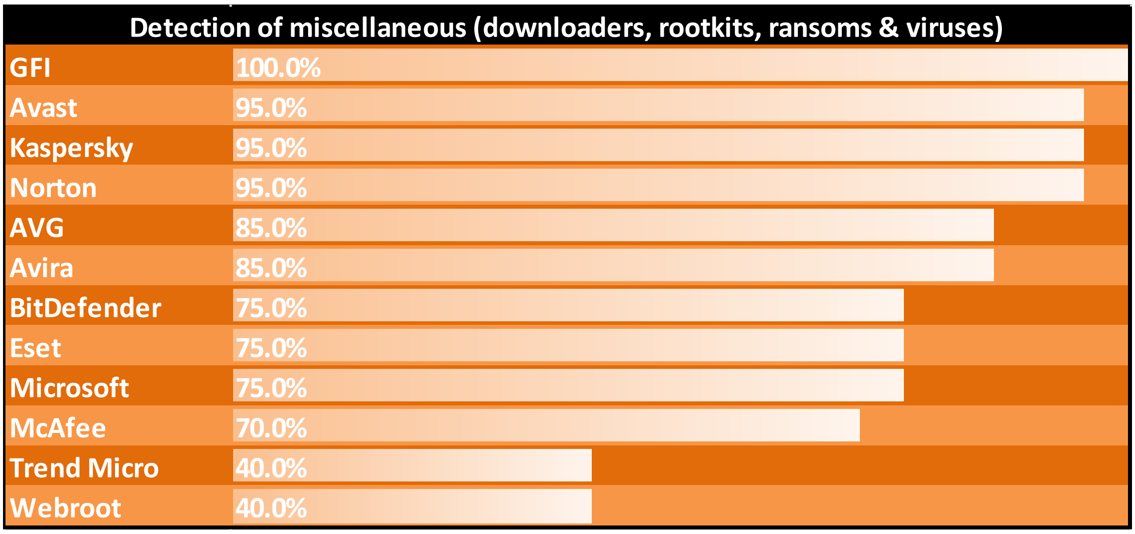
Detection of PDF exploits	
Avast	100.0%
Avira	100.0%
Eset	100.0%
Kaspersky	100.0%
Microsoft	100.0%
Webroot	100.0%
GFI	85.7%
BitDefender	42.9%
Norton	28.6%
AVG	0.0%
McAfee	0.0%
Trend Micro	0.0%


Detection of PUAs
Avast 100.00%
Kaspersky 100.00%
AVG 88.89%
GFI 88.89%
Norton 88.89%
Eset 77.78%
McAfee 77.78%
BitDefender 66.67%
Avira 44.44%
Microsoft 44.44%
Webroot 22.22%
Trend Micro 11.11%

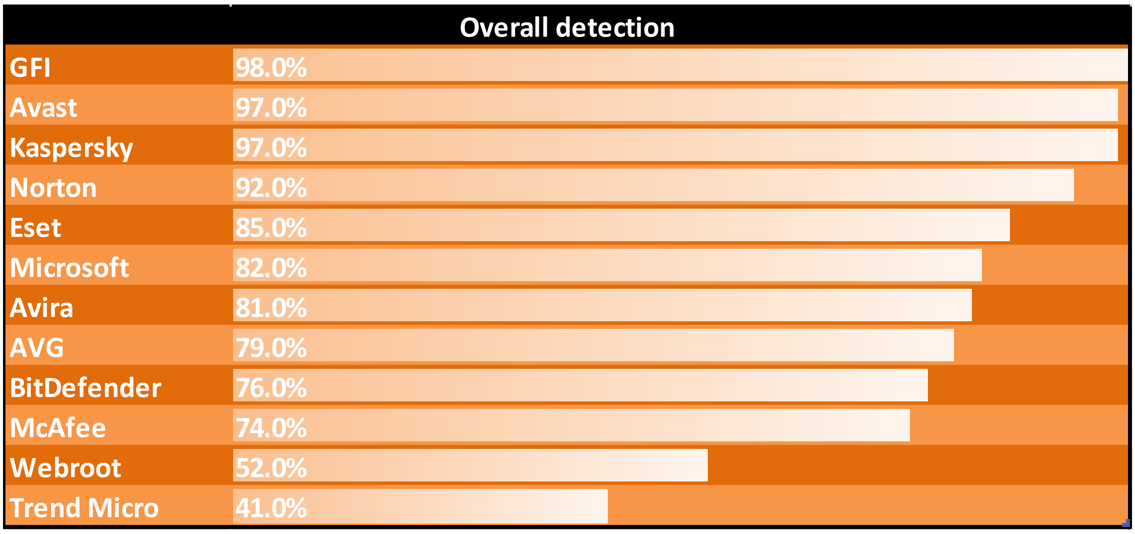

Detection of trojans
GFI 100.0%
Norton 100.0%
Avast 95.2%
Kaspersky 95.2%
Eset 90.5%
Microsoft 81.0%
AVG 76.2%
McAfee 76.2%
Avira 76.2%
BitDefender 61.9%
Webroot 52.4%
Trend Micro 42.9%


Detection of financial malware & password stealers
GFI 100.0%
Kaspersky 100.0%
Avast 95.5%
Norton 95.5%
AVG 86.4%
Avira 86.4%
BitDefender 86.4%
Eset 81.8%
McAfee 81.8%
Microsoft 81.8%
Trend Micro 50.0%
Webroot 50.0%





The table below shows the overall detection for all the samples used in the dynamic test.



Conclusions:

In the context of these tests, VIPRE Antivirus Premium demonstrated overall, superior detection capabilities in both static and dynamic testing.

Our overwhelming concern when assessing the efficacy of antimalware applications is their ability to protect users against current malware threats. It is important to understand that the greatest risk users face is from early life malware. Nearly all infections occur as a result of drive by attacks or users unintentionally executing malware on their systems, in either case, the malware is invariably early life and certainly younger than seven days old.

The ability to protect against early life malware is crucial and therefore assessment of efficacy against this age of threat is vastly more relevant than using older samples which in most cases only exist in research labs.

GFI are to be commended for VIPREs' excellent performance in threat scenarios which closely map to real world usage.

Appendix:

The tables below detail the full results from the dynamic testing.

	Backdoors														PDF Exploits							PUAs								
	Bifrose	Buterat	CycBot	DarkMoon	FlyAgent	Hupigon	IrcBot	Outbreak	Rbot	Ripinip	Ruskill	Torr	Wuca	Xyligen	Pdfka 1	Pdfka 2	Pdfka 3	Pdfka 4	Pdfka 5	Pdfka 6	Pdfka 7	FakeAlert 1	FakeAlert 2	FakeAlert 3	FakeAlert 4	FakeAV 1	FakeAV 2	FakeAV 3	FakeAV 4	FakeAV 5
Avast	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AVG	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓
Avira	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✗	✗	✓	✗
BitDefender	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓
Eset	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓
GFI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓
Kaspersky	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
McAfee	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓
Microsoft	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓	✗	✗	✓
Norton	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓
Trend Micro	✗	✓	✗	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗	✗	✗
Webroot	✗	✓	✓	✓	✓	✗	✗	✗	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✓	✗	✗	✗	✗	✓

	Trojans																					Other																			
	Buzus 1	Buzus 2	Cdur	FakeSysdef	Hamweq	Inject 1	Inject 2	IrcBrute	Jorik	Liac	Malat	Pakes	Pincav 1	Pincav 2	Qhost	Refroso	Rettesser	ServStart	StartPage	VBInject	Yakes	Banload	Delf 1	Delf 2	Injecter	Psyme	Cidox	Vedio	Coco	Zwangi	Themida	TDSS 1	TDSS 2	ZAccess	Ransom 1	Ransom 2	Ransom 3	Ransom 4	CeeInject	Dracur	VBkrypt
Avast	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AVG	✗	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓
Avira	✗	✗	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓
BitDefender	✗	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✗
Eset	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✗	✓	✓	✗
GFI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kaspersky	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
McAfee	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✓	✗	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✓
Microsoft	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✗	✓	✓	✗
Norton	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Trend Micro	✗	✗	✓	✗	✗	✓	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✓	✗	✓	✓	✗	✗	✗	✓	✗	✗	✓	✗	✗	✓	✗	✓	✗	✓	✓	✗	✗	✓	✗	✓
Webroot	✓	✓	✓	✗	✗	✓	✗	✓	✓	✗	✗	✓	✓	✗	✗	✗	✗	✓	✓	✗	✓	✗	✗	✓	✓	✗	✗	✓	✓	✗	✓	✗	✓	✓	✗	✗	✗	✗	✓	✗	✗

	Financial Malware & Password Stealers																						Worms						
	Bancos	Banker 1	Banker 2	Banker 3	Banker 4	Dybalom	Fignotok	Kykumber	Sinowal 1	Sinowal 2	Sinowal 3	Vkont	Carberp	PerfLoger	SpyEye 1	SpyEye 2	Webmoner	Zeus 1	Zeus 2	Zeus 3	Zeus 4	Zeus 5	Ainslot	Apher	AutoRun	Bybz	DarkBot	Kolab	Vobfus
Avast	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
AVG	✓	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Avira	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✗	✓	✓	✓	✓	✓	✓
BitDefender	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Eset	✓	✗	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓
GFI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Kaspersky	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
McAfee	✓	✗	✗	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓
Microsoft	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✗	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Norton	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Trend Micro	✗	✓	✗	✓	✗	✓	✗	✓	✓	✓	✓	✗	✗	✓	✗	✓	✗	✗	✓	✗	✓	✗	✗	✗	✗	✗	✓	✓	✓
Webroot	✗	✗	✗	✗	✗	✓	✓	✓	✗	✗	✗	✗	✓	✗	✓	✓	✓	✓	✓	✗	✓	✓	✗	✓	✓	✓	✗	✓	✓