360 Degree Assessment & Certification

Q3 2018

MRG Effitas
EFFICACY ASSESSMENT & ASSURANCE

MRG Effitas Ltd.
Efficacy Assessment & Assurance

Contents

Introduction 3
Executive Summary 4
Certification 5
Certified (level 1): 5
Certified (level 2): 5
The Purpose of this Report 6
Tests Employed 7
In the Wild 360 / Full Spectrum Test 7
PUA / Adware Test 7
Exploit / Fileless Test 8
False positive Test 9
Performance Test 9
Security Applications Tested 10
Malware sample types used to conduct the tests 10
Test Results 11
Q3 2018 In the Wild 360 / Full Spectrum Test Results 11
Understanding Grade of Pass 19
Appendix 1 20
Methodology used in the “In the Wild 360 / Full Spectrum”, PUA, False positive tests 20
Methodology used in the Exploit / Fileless test 21
Methodology of the Performance test 23
Non-default endpoint protection configurations 23

Effitas is a world-leading, independent IT security efficacy testing & assurance company. We are trusted by antimalware vendors across the world

TEL:
+44 (0)20 3239 9289

EMAIL:
contact@mrg-effitas.com

TWITTER:
@mrgeffitas

Introduction

MRG Effitas has a core focus on efficacy assessments both in the anti–financial fraud space and also in the traditional “Real World” detection tests.

The methodology employed in this test maps closely to Real World use.

This Programme is called a “360 Assessment” since it deals with the full spectrum of malware instead of just financial malware. In the 360 Assessments, trojans, backdoors, ransomware, PUAs, financial malware and “other” malware are used.

Besides the “Real world test”, we performed tests to check PUA/Adware protection, Exploit / Fileless protection, measured the False positive rates and measured the Performance impacts of the security products.

Executive Summary

This Certification Programme is designed to serve as a reflection of product efficacy based on what we have previously termed "metrics that matter".

In many of our previous tests, particularly those that have focused on financial malware, we started with the assumption that the endpoint has already been compromised. Being one of the world's largest supplier of early-life malicious binaries and malicious URLs, and from our own simulator development, we know that all endpoints can be infected, regardless of the security solution employed.

For us, a product's ability to block initial infection (although critical in most cases) is not the only metric that matters. One also needs to measure the time taken for the security product to detect malware on a system and remediate it.

When conducting these tests, we tried to simulate normal user behaviour. We are aware that a "Real World" test cannot be conducted by a team of professionals inside a lab because we understand how certain types of malware work, how malware attacks and how such attacks could be prevented. Simulating normal user behaviour means that we paid special attention to all alerts given by security applications. A pass was given only when alerts were straightforward and clearly suggested that malicious action should be blocked.

With these, it is very important to note that the best choice for an average user is to keep things very simple and for the product not to present many pop-up alerts or questions.

Out of eleven products we tested, eleven managed to meet the specification to attain our Q3 2018 360 certification award, these being:

- avast! Business Antivirus
- Avira Antivirus Pro - Business edition
- BitDefender Gravityzone Advanced Business Security
- ESET Endpoint Security
- F-secure Business, Computer Protection
- Kaspersky Small Office Security
- McAfee Endpoint Security
- Microsoft Windows Defender with SmartScreen
- Symantec Endpoint Protection Cloud
- Trend Micro Worry-Free™ Services with XGEN
- Webroot SecureAnywhere Business

In this quarter, no security application failed the test in that it was unable to detect the malware and/or remediate the system even after the end of a 24-hour period.

Certification

In order to attain a quarterly MRG Effitas 360 Degree certification award, a security application must either protect the system from initial infection (autoblock or behaviour protection - Level 1 pass) or detect at least 98% of all cases any malware and fully remediate the system before or on the first retest (Level 2 pass). Applications that meet this specification are given certification for that quarter. PUA/Adware, Exploit / Fileless, False positive and Performance tests are not part of the certification.

Under the MRG Effitas 360 Degree Assessment & Certification, the following products were certified for Q3 2018:

Certified (level 1):

- avast! Business Antivirus
- Avira Antivirus Pro - Business
- BitDefender Gravityzone Advanced Business Security
- F-secure Business - Computer Protection
- Kaspersky Small Office Security
- Symantec Endpoint Protection Cloud
- Trend Micro Worry-Free™ Services with XGEN

Certified (level 2):

- ESET Endpoint Security
- McAfee Endpoint Security
- Microsoft Windows Defender
- Webroot SecureAnywhere Business

The Purpose of this Report

Since its inception in 2009, MRG Effitas has strived to differentiate itself from traditional testing houses by having its primary focus on providing “efficacy assessments" and not just performing “tests”.

Traditionally, testing of security software has centred on measuring a product's ability to detect malware. Testing has evolved rapidly over the last two to three years as most labs, under the direction of AMTSO (of which MRG Effitas is a member) strived to conduct “Real World" testing following these guidelines. More information can be found on the AMTSO website:

https://www.amtso.org/compliance-summary-ls1-tp003-mrg-q3-2018/

Although there is no absolute definition of this kind of testing, loosely speaking, it involves the introduction of malware to an endpoint through a realistic vector, such as a browser or USB memory stick. Real World testing mostly involves “dynamic testing" (i.e. the malware is executed and then the ability of the security product to block the malware is measured).

Whilst these types of tests are useful and yield valid and meaningful data, MRG Effitas wanted to merge these tests and also go one step further by measuring the time security products take to detect infections and remediate the endpoint.

To make testing more akin to Real World scenarios, no manual scanning was conducted. Instead, the system was retested exactly 24 hours after the system was compromised, thereby giving security applications the opportunity to detect infections on restart.

As we have stated in our previous test reports, most malware has one primary objective, and that is to make money for the cybercriminals.

Measuring initial detection rates and the time taken to detect active malware is important, particularly in today's threat landscape with the mix of malware that is prevalent.

As we have repeated in our previous financial malware test reports, the longer a cybercriminal can have their malware on a system, the greater the opportunity for them to be able to capture private user information including banking passwords and social media credentials, etc.

There has been an increase in the prevalence of targeted ransomware, which once active on the system, holds the user at ransom to decrypt system data or unlock the system in some other.

For these types of malware, it is initial detection that is of the greatest importance, since the vast majority of security solutions will be unable to remediate an encrypted system.

In providing these quarterly certifications, the MRG Effitas 360 Assessment & Certification Programme is the de facto standard by which security vendors, financial institutions and other corporations can attain the most rigorous and accurate determination of a product's efficacy against the full spectrum of malware that is prevalent during the period.

Tests Employed

In this assessment (Q3 2018), we ran the following tests:

In the Wild 360 / Full Spectrum Test

Most of the malicious URLs used in this test were compromised legitimate websites which served malware. We believe that such URLs pose the greatest danger to users as this is the place where they least expect to get infected. Some URLs come from our regular honeypots or in case of ransomware and financial malware in particular, we used URLs from newly-discovered distribution sites.

Malware delivered by URLs used in this test can be considered as Zero Day in the true meaning of that phrase. This posed a challenge to the participant products.

Applications that didn't protect the system from file encrypting ransomware cannot be certified because they could not remediate the threat; as files usually cannot be decrypted.

~10% of the threats used in this test were introduced to the system via internal webmail sites. We have witnessed many SMBs being infected through internal webmails and lack of spam filtering. Downloading malware attachments from internal webmail sites bypass the URL blocking features of the products, and this happens in-the-wild.

During the In the Wild 360 / Full Spectrum test, 329 live ITW samples were used. The stimulus load comprised the following: 168 trojans, 46 backdoors, 79 financial malware samples, 2 ransomware samples, and 34 others.

PUA / Adware Test

The PUA samples used in this test are deceptors or potentially unwanted applications (PUA) that aren't malicious but are generally considered unsuitable for most home or business networks. It contains adware, installs toolbars or has other unclear objectives. It may also contribute to consuming computing resource. PUAs can be deceptive, harmful, HOAX, show aggressive popups and misleading or scaring the user. They may provide unconventional ways of uninstalling the application, maybe retain some of their components on the device without the user's consent. We use a filtered AppEsteem's feed as they developed deceptor requirements as part of a cross-industry effort between many of the world's leading security companies and represent a minimum bar that all apps and services must meet to avoid being titled deceptive.

AppEsteem as a member of the AMTSO group is dedicated to help protecting consumers from harassing and objectionable material, and to help to enable security companies to restrict access to such actions. MRG Effitas as part of the AMTSO group also dedicated to protecting these thoughts.

In the PUA / Adware section we tested the products against 9 PUAs, all coming from the AppEsteem feed.

Exploit / Fileless Test

The main purpose of this test is to see how security products protect against a specific exploitation technique. In order to measure this, we developed test cases that simulate the corresponding exploit and post-exploitation techniques only. By this method we were able to see which products protect against which techniques.

Drive-by download exploits are one of the biggest threats and concerns in an enterprise environment because no user interaction is needed to start the malware on the victim machine. Outdated browser and Office environments are very “popular” in enterprise environments because of compatibility issues, lack of proper patch-management, etc.

We were not looking to test the products’ ability to avoid exposure to adversaries, to interrupt malware delivery before it reaches the device or to identify malicious files. We wanted to focus explicitly on each product’s ability to mitigate each attack technique. The results are not intended to evaluate the complete efficacy of the products, but rather the products’ anti-exploit and anti-post-exploit features in isolation.

During this test we used three different exploitation techniques.

In the first scenario we created a .lnk file which contains a PowerShell-Command to get another PowerShell-Stager. Following this the second stage was a PowerShell Empire payload which started a new session with our CnC server.

If the security product was not blocking the attack, we were able to control the test machine via C2 server, download or upload files, or perform remote code execution.

References:
https://www.powershellempire.com

In the second setup we used Meterpreter (module: exploit/multi/browser/firefox_proxy_prototype on Firefox 31.0) to exploit a known vulnerably in this browser with a payload (windows/meterpreter/reverse_http) to connect back to our C2 server.

If the security product was not blocking the attack, we were able to control the test machine via C2 server, download or upload files, or perform remote code execution.

References:
https://www.rapid7.com/db/modules/exploit/multi/browser/firefox_proxy_prototype

As the last Exploit / Fileless test in this quarter, we used the same Firefox exploit than previously (firefox_proxy_prototype) with a PowerShell Empire payload. However, in this case we used the IronSquirrel framework that aims at delivering browser exploits to the victim browser in an encrypted fashion. Ellyptic-curve Diffie-Hellman (secp256k1) is used for key agreement and AES is used for encryption.

If the security product was not blocking the attack, we were able to control the test machine via C2 server, download or upload files, or perform remote code execution.

References:
https://github.com/MRGEffitas/Ironsquirrel
https://www.rapid7.com/db/modules/exploit/multi/browser/firefox_proxy_prototype

False positive Test

Malicious content blocking from a security product is not necessary achieved by 100% correct detection rate. In many cases all malware blocking is a result of a very aggressive filter which can block non-malicious legitim applications as well prohibiting everyday work by blocking legitim, perhaps newly developed in-house software.

In order to test this feature, we tested the security applications against completely clean, recently created applications.

False positive assessment consisted of 997 clean and legitimate application samples. The samples are focused on samples one can find in enterprise environments, like drivers, media editors, developer tools, etc.

Performance Test

A security product's usefulness does not depend on protection level solely, but the footprint and the effect of the operating system is also an important measure.

To assess the products' influence on the operating system we tested several performance factors on physical machine and combined the results based on a scoring approach. Detailed information can be found in the Appendix.

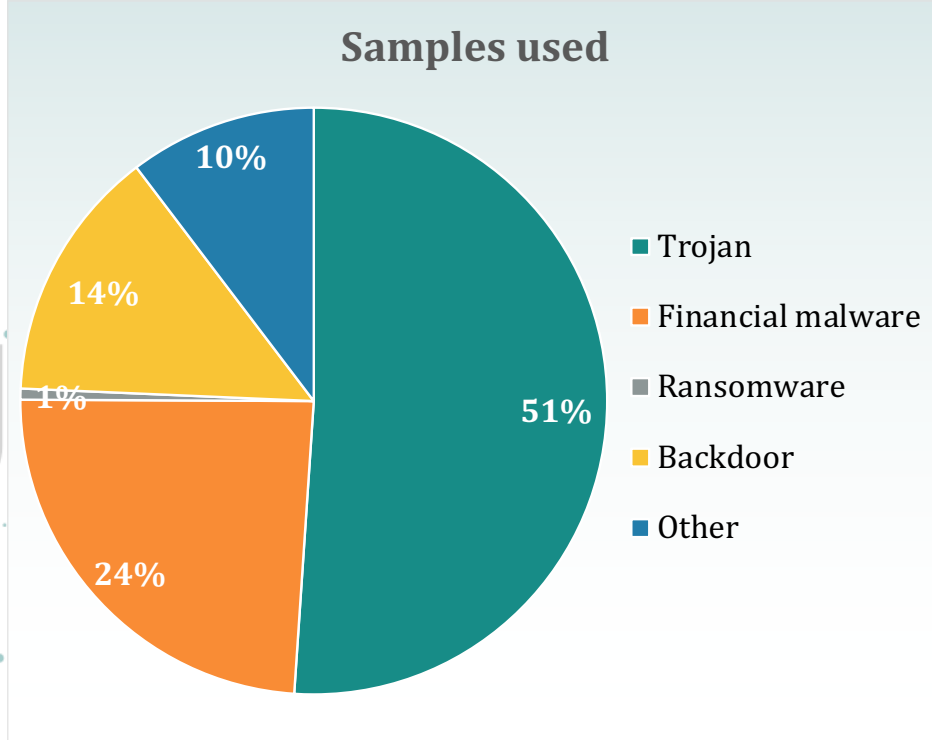
In every test case, (except for the performance test) our testing environment supports the use of VM aware malware, this is the reason why we were able to use more sophisticated threats which wouldn't run on Virtual Machines.

Please note that the measured size on the disk can significantly change, due to application logs, quarantine, new signatures downloaded, cache for rollback, etc.

Security Applications Tested

- avast! Business Antivirus 18.6.2540
- Avira Antivirus Pro - Business edition 15.0.40.12
- BitDefender Gravityzone Advanced Business Security 6.6.6.84
- ESET Endpoint Security 6.6.2086.1
- F-secure Business, Computer Protection 18.5
- Kaspersky Small Office Security 19.0.0.188(b)
- McAfee Endpoint Security 10.6.0.542
- Microsoft Windows Defender with SmartScreen 4.18.1809.2
- Symantec Endpoint Protection Cloud 22.15.1.8
- Trend Micro Worry-Free™ Services with XGEN 6.5.1265
- Webroot SecureAnywhere 9.0.21.18

Malware sample types used to conduct the tests

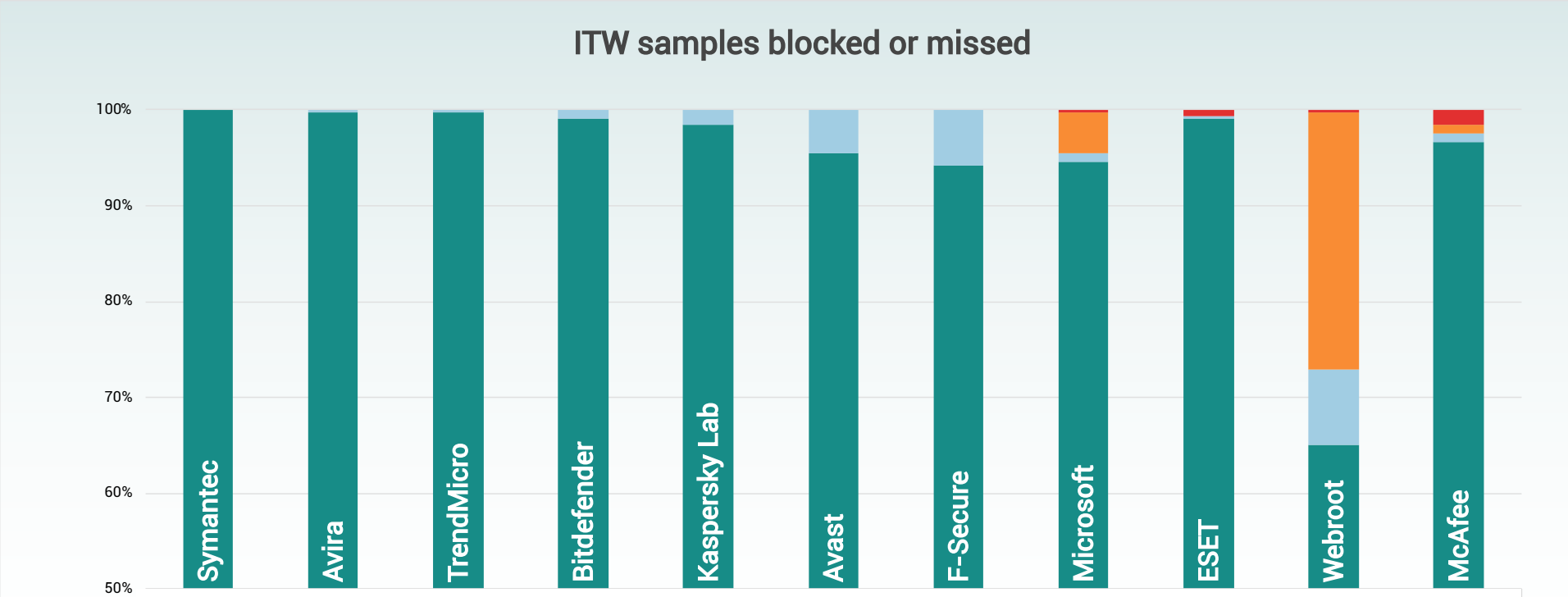


Test Results

The tables below show the results of testing under the MRG Effitas 360 Q3 Assessment Programme.

Q3 2018 In the Wild 360 / Full Spectrum Test Results

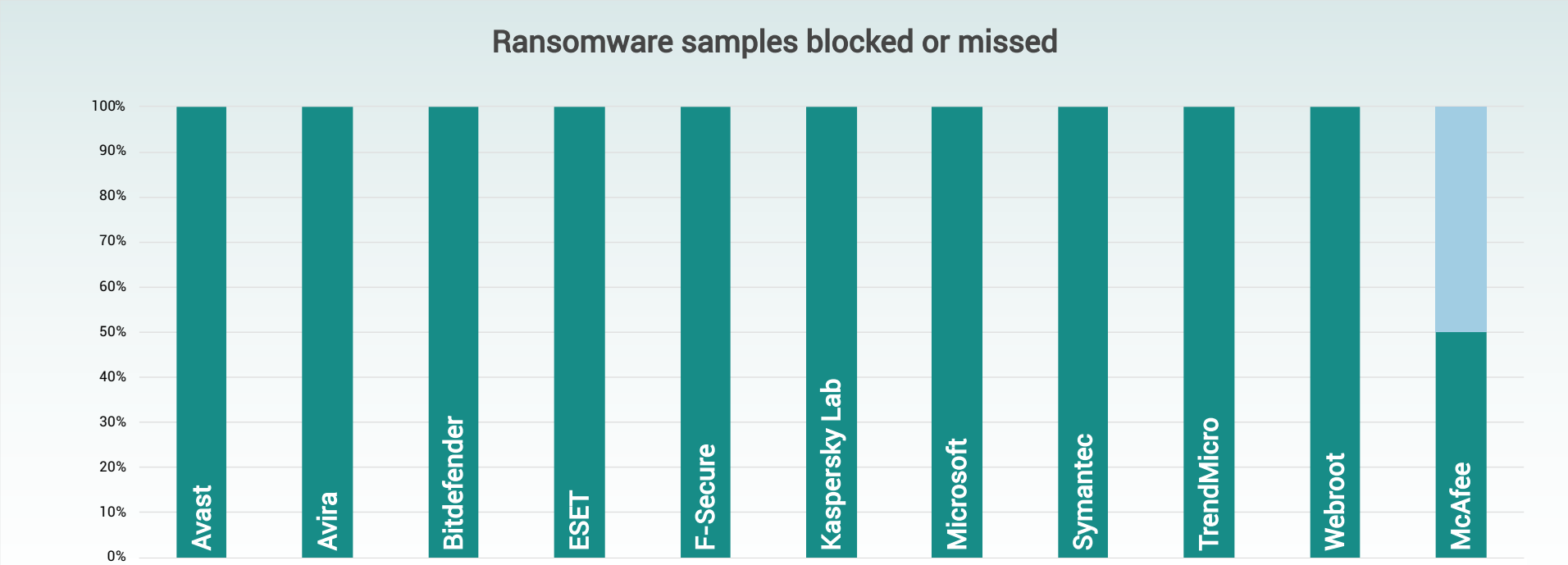
The table below shows the initial detection rates of the security products for 329 ITW samples. This table is sorted by smallest amount of failures.



	Symantec	Avira	TrendMicro	Bitdefender	Kaspersky Lab	Avast	F-Secure	Microsoft	ESET	Webroot	McAfee
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,30%	0,61%	0,30%	1,52%
Blocked in 24h	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	4,26%	0,00%	26,75%	0,91%
Behaviour block	0,00%	0,30%	0,30%	0,91%	1,52%	4,56%	5,78%	0,91%	0,30%	7,90%	0,91%
Auto block	100,00%	99,70%	99,70%	99,09%	98,48%	95,44%	94,22%	94,53%	99,09%	65,05%	96,66%

Ransomware samples assessment results

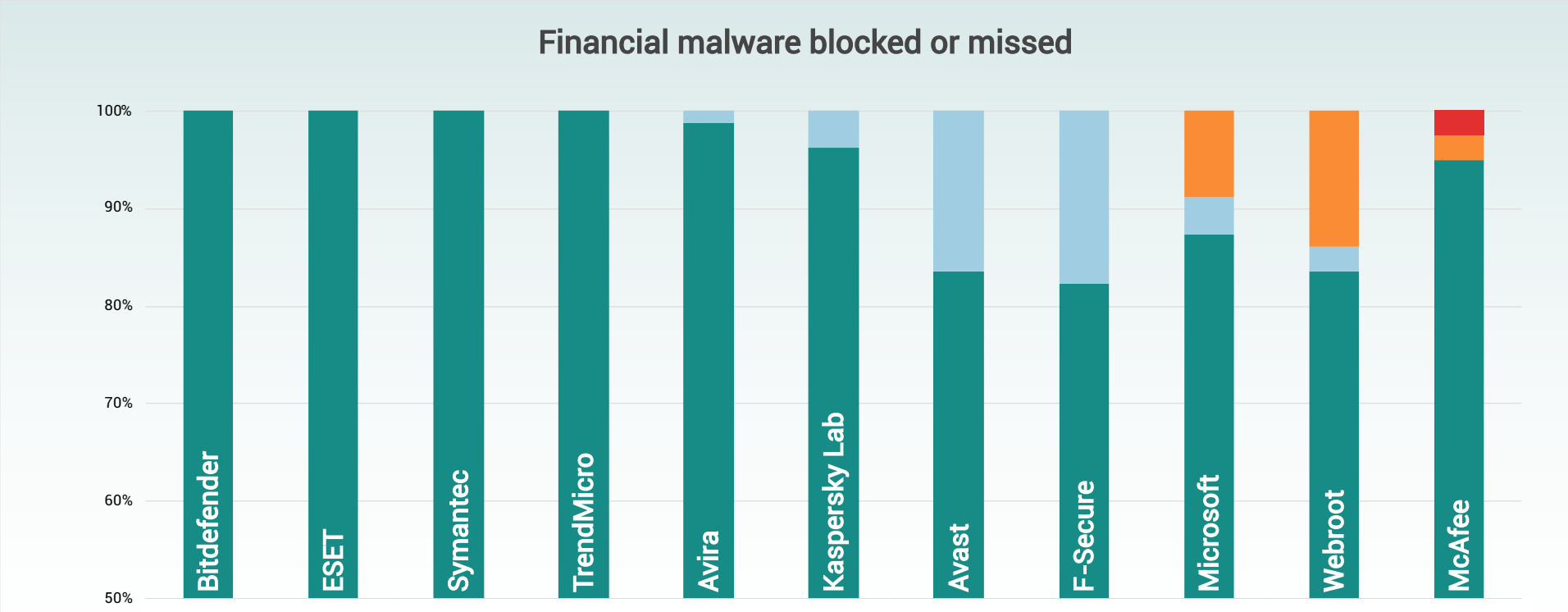
The table below shows the initial detection rates of the security products for 2 ransomware samples. This table is sorted by smallest amount of failures.



	Avast	Avira	Bitdefender	ESET	F-Secure	Kaspersky Lab	Microsoft	Symantec	TrendMicro	Webroot	McAfee
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
Blocked in 24h	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
Behaviour block	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	50,00%
Auto block	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	50,00%

Financial malware samples assessment results

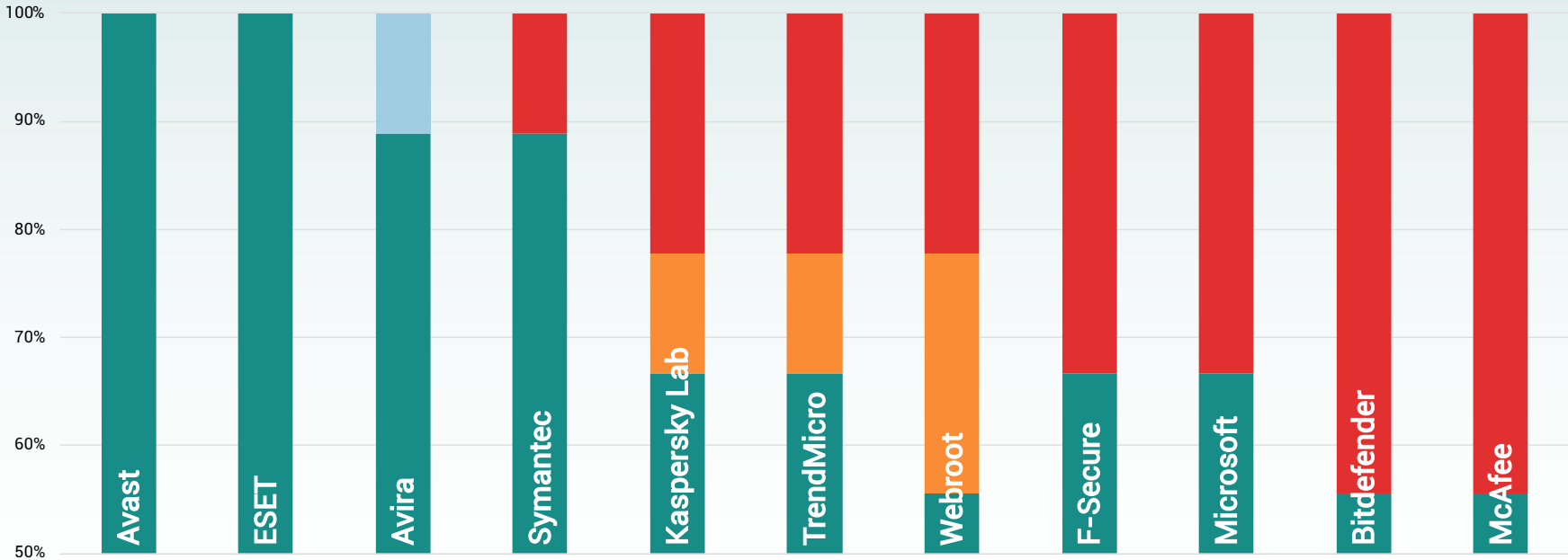
The table below shows the initial detection rates of the security products for 79 financial malware. This table is sorted by smallest amount of failures.



	Bitdefender	ESET	Symantec	TrendMicro	Avira	Kaspersky Lab	Avast	F-Secure	Microsoft	Webroot	McAfee
Miss	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	2,53%
Blocked in 24h	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	8,86%	13,92%	2,53%
Behaviour block	0,00%	0,00%	0,00%	0,00%	1,27%	3,80%	16,46%	17,72%	3,80%	2,53%	0,00%
Auto block	100,00%	100,00%	100,00%	100,00%	98,73%	96,20%	83,54%	82,28%	87,34%	83,54%	94,94%

PUA/Adware samples assessment results

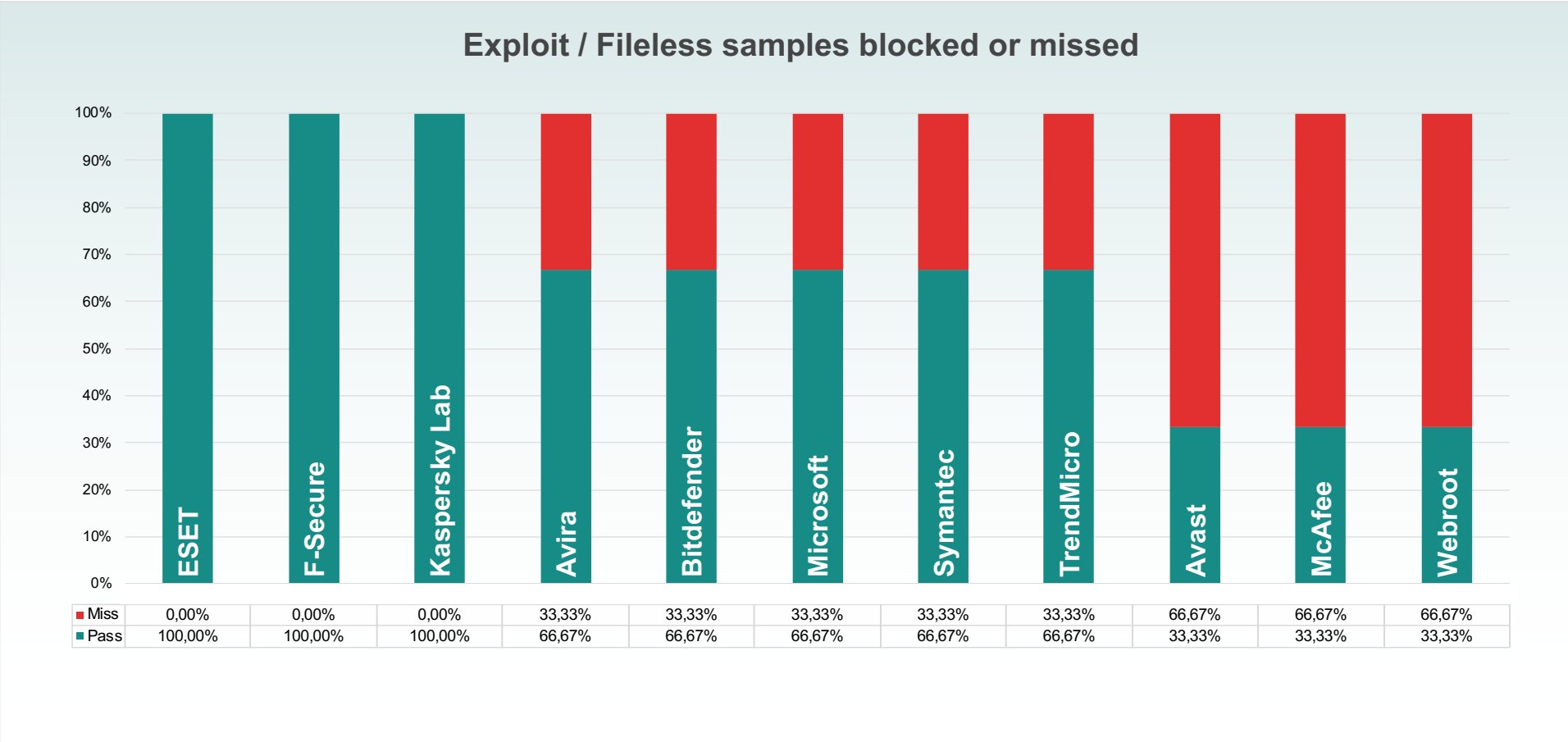
The table below shows the initial detection rates of the security products for 9 PUA/Adware applications. This table is sorted by smallest amount of failures.



	Avast	ESET	Avira	Symantec	Kaspersky Lab	TrendMicro	Webroot	F-Secure	Microsoft	Bitdefender	McAfee
Miss	0,00%	0,00%	0,00%	11,11%	22,22%	22,22%	22,22%	33,33%	33,33%	44,44%	44,44%
Blocked in 24h	0,00%	0,00%	0,00%	0,00%	11,11%	11,11%	22,22%	0,00%	0,00%	0,00%	0,00%
Behaviour block	0,00%	0,00%	11,11%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%
Auto block	100,00%	100,00%	88,89%	88,89%	66,67%	66,67%	55,56%	66,67%	66,67%	55,56%	55,56%

Exploit / Fileless samples assessment results

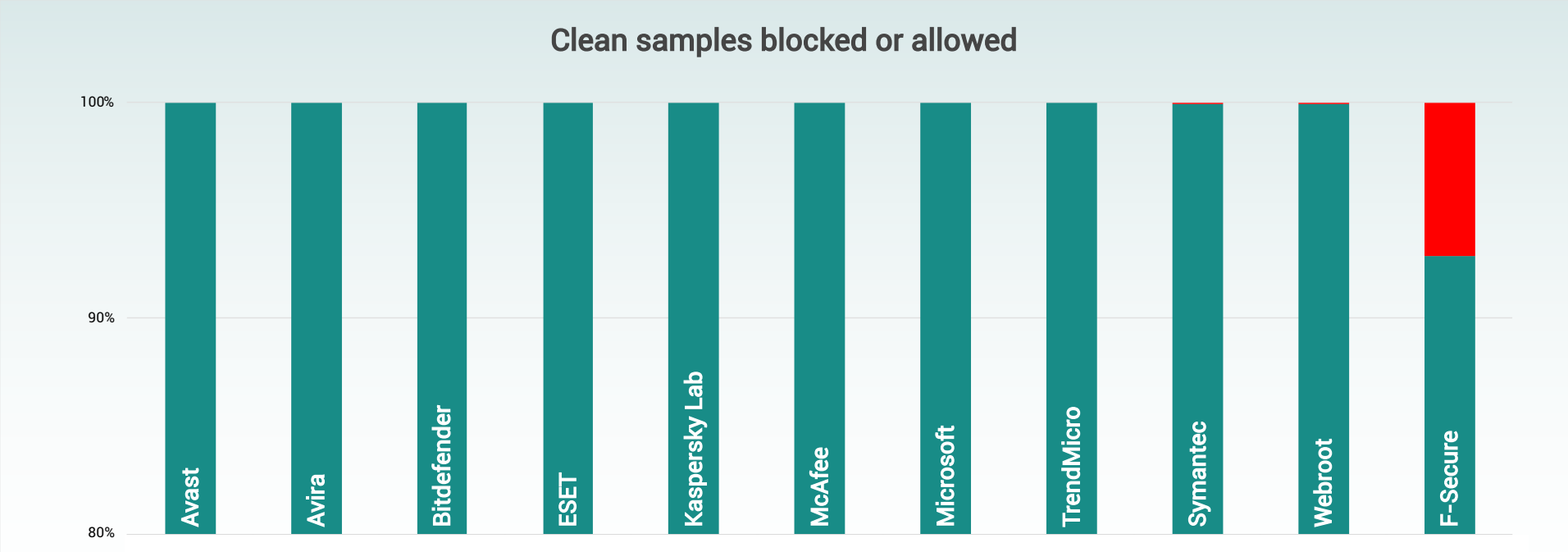
The table below shows the initial detection rates of the security products for 3 Exploit / Fileless test. This table is sorted by smallest amount of failures.



	ESET	F-Secure	Kaspersky Lab	Avira	Bitdefender	Microsoft	Symantec	TrendMicro	Avast	McAfee	Webroot
Miss	0,00%	0,00%	0,00%	33,33%	33,33%	33,33%	33,33%	33,33%	66,67%	66,67%	66,67%
Pass	100,00%	100,00%	100,00%	66,67%	66,67%	66,67%	66,67%	66,67%	33,33%	33,33%	33,33%

False positive samples assessment results

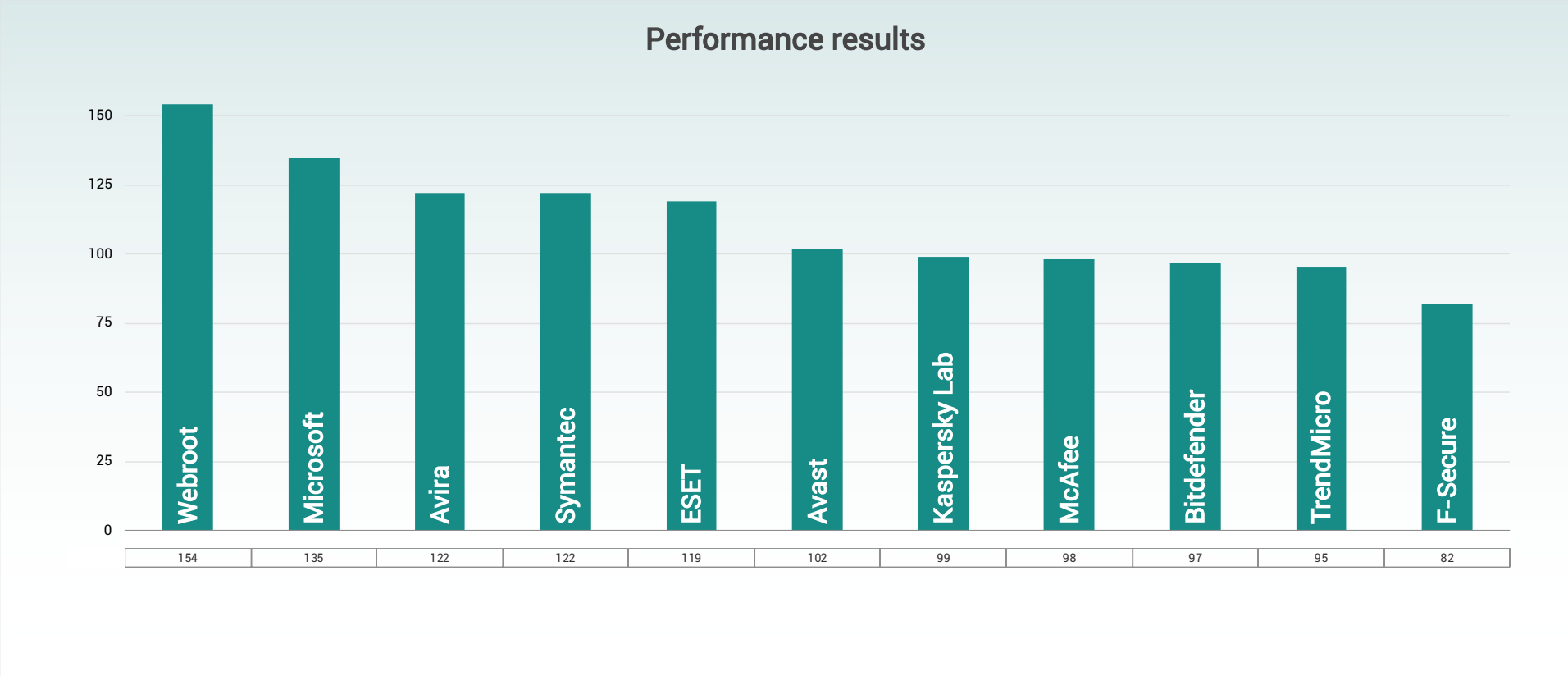
The table below shows the initial detection rates of the security products for 997 false positive samples. This table is sorted by smallest amount of failures.



	Avast	Avira	Bitdefender	ESET	Kaspersky Lab	McAfee	Microsoft	TrendMicro	Symantec	Webroot	F-Secure
False block	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,00%	0,10%	0,10%	7,12%
Allowed to run	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	100,00%	99,90%	99,90%	92,88%

Performance assessment results

The table below shows the summary of the performance results of the security products This table is sorted by the highest score.



Scoring details can be found in the Appendix.

Detailed results of the Performance assessment

The table below shows the detailed results of the performance test of the security products. This table is sorted alphabetically.

	Avast	Avira	Bitdefender	ESET	F-Secure	Kaspersky Lab	McAfee	Microsoft	Symantec	TrendMicro	Webroot
Bootup time (s)	26,2	25,8	27,0	23,2	29,0	23,7	29,2	22,3	23,1	29,6	23,0
Install time (s)	37,3	89,3	180,7	19,3	116,3	33,0	76,3	N/A	28,3	194,3	31,3
Firefox startup time (s)	1,3	1,1	1,1	1,2	1,5	1,5	1,2	1,5	1,6	1,9	1,5
10 minutes of idling											
CPU usage (%)	0,6	0,8	0,9	0,7	0,7	1,1	1,4	0,8	0,8	2,3	1,4
Used memory (Mb)	6530,8	6571,6	6244,7	6739,1	6295,2	6526,2	6389,9	6625,8	6560,5	6569,5	6634,7
Memory - % Commited Bytes In Use	12,8	13,1	16,8	10,5	15,8	12,6	16,3	11,9	12,7	13,4	11,9
Physical disk usage (%)	0,9	0,6	1,7	1,7	1,4	2,2	1,9	1,1	2,1	2,9	0,4
Security software update											
Time (s)	14,0	53,3	111,0	17,0	77,0	28,0	38,3	30,0	15,7	18,3	N/A
CPU usage (%)	27,6	34,3	24,3	19,7	33,5	31,5	35,2	19,6	26,4	14,8	N/A
Memory - Available Mbytes	6312,6	6254,8	6218,7	6623,0	5982,5	6347,6	6099,7	6498,0	6372,7	6403,0	N/A
Memory - % Commited Bytes In Use	14,7	15,2	17,4	11,7	19,4	14,1	23,8	13,3	13,9	14,1	N/A
Physical disk usage (%)	24,8	18,4	11,8	50,6	42,5	11,0	12,2	21,4	10,2	6,5	N/A
Security software scanning - C:\											
Time (s)	324,0	424,0	20,0	65,3	97,3	151,0	1107,7	1396,3	156,3	762,0	393,3
CPU usage (%)	26,7	24,4	31,4	25,3	93,1	79,2	96,4	23,7	58,2	28,7	46,8
Memory - Available Mbytes	5958,3	6200,4	6172,7	6574,2	5175,3	6237,7	5741,9	6038,3	6508,3	6108,0	6358,8
Memory - % Commited Bytes In Use	18,6	16,0	17,1	11,6	20,8	14,1	23,7	16,0	13,2	17,4	13,9
Physical disk usage (%)	62,5	25,8	51,4	51,6	110,8	95,2	8,5	20,9	51,6	25,9	34,1
Size On Disk In Bytes											
Just after install (Mb)	1272,3	368,6	826,6	925,6	316,7	545,1	230,9	142,7	37,9	481,9	10,6
After first scan (Mb)	945,7	417,2	877,1	828,5	1387,0	856,3	378,6	671,1	501,6	464,6	16,7
After update (Mb)	1094,1	408,6	877,0	822,1	1364,7	873,5	377,8	528,8	665,8	476,7	N/A
1 hour after install (Mb)	979,5	372,2	924,7	928,9	1362,9	677,2	859,4	534,7	730,5	525,8	10,8

Understanding Grade of Pass

Level 1

All threats detected on first exposure or via behaviour protection.

- avast! Business Antivirus
- Avira Antivirus Pro - Business
- BitDefender Gravityzone Advanced Business Security
- F-secure Business - Computer Protection
- Kaspersky Small Office Security
- Symantec Endpoint Protection Cloud
- Trend Micro Worry-Free™ Services with XGEN

Level 2

At least 98% of the threats detected and neutralised / system remediated before or on the first rescan.

- ESET Endpoint Security
- McAfee Endpoint Security
- Microsoft Windows Defender
- Webroot SecureAnywhere Business

Failed

Security product failed to detect all infections or at least 98% of them and remediate the system during the test procedure

Appendix 1

Methodology used in the “In the Wild 360 / Full Spectrum", PUA, False positive tests

1. Windows 10 64-bit operating system was installed on a hardened virtual machine, all updates are applied and third-party applications installed and updated.
2. An image of the operating system was be created.
3. A clone of the imaged systems was made for each of the security applications used in the test.
4. An individual security application was installed using default settings on each of the systems created in (3) and then, where applicable, updated. If the vendor provided a non-default setting, this setting was checked whether it was realistic. If yes, the changes were documented, applied, and added in the report in an appendix (if any).
5. A clone of the system as at the end of (4) was created.
6. Each live URL test was conducted by the following procedure.
    a. Downloading a single binary executable (or document, script, etc.) from its native URL using Microsoft Edge to the Downloads folder and then executing the binary.
    b. Either the security application blocked the URL where the malicious binary was located.
        i. Or the security application detected and blocked the malicious binary whilst it was being downloaded to the desktop.
        ii. Or the security application detected the malicious binary when it was executed according to the following criteria: It identified the binary as being malicious and either automatically blocked it or postponed its execution and warned the user that the file was malicious and awaited user input.
7. The system under test was deemed to have been infected if the security application failed to detect or block the binary at any stage in (6) and allowed it to be executed.
8. The test case was retested 24 hours after the initial test if the security application failed to detect or block the malicious binary.
9. Tests are conducted with all systems having internet access.
10. As no user-initiated scans was involved in this test, applications rely on various technologies to detect, block and remediate threats. Some of these technologies were: URL blacklist, reputation, signature, machine learning, heuristics, behavior etc.

Methodology used in the Exploit / Fileless test

1. One default install Windows 10 hardened virtual machine endpoint is created. The default HTTP/HTTPS proxy is configured to point to a proxy running on a different machine. SSL/TLS traffic is not intercepted on the proxy, and optionally AV's have been configured to skip the proxy totally.
2. The security of the OS is weakened by the following actions:
   a. Microsoft Defender is disabled
   b. Internet Explorer SmartScreen is disabled
3. The following vulnerable software is installed:
   a. Java 1.7.0.17
   b. Adobe Reader 9.3.0
   c. Flash Player 15.0.0.152 or Flash Player 16.0.0.287 in a small number of cases
   d. Silverlight 5.1.10411.0
   e. Internet Explorer 11
   f. Firefox 31.0
   g. Chrome 38.0.2125.101

   These version numbers were specified with the following two requirements:
   - The highest number of in-the-wild exploits should be able to exploit this specific version, thus increasing the coverage of the tests.
   - The version must currently be popular among users.
   - Windows Update is disabled.
4. From this point, a number of different snapshots are created from the virtual machine, each with different endpoint protection products and one with none. This procedure ensures that the base system is exactly the same in all test systems. The following endpoint security suites, with the following configuration, are defined for this test:
   a. No additional protection, this snapshot is used to infect the OS and to verify the exploit replay.
   b. Vendor A
   c. Vendor B
   d. …

   The endpoint systems are installed with default configuration, potentially unwanted software removal is enabled, and if it was an option during install, cloud/community participation is enabled. The management servers (if needed) are installed onto a different server. The purpose of management servers is to centrally administer, update and analyse logs in an enterprise environment. Installing the management server on a different server is highly recommended by vendors, so it does not interfere with the testing, machine resources are not used by the management server, etc.

5. Two sources of exploits are used during the test. One in-the-wild exploit kits, and one from publicly available open-source exploit frameworks (e.g. Metasploit). In spite of other “real world protection tests”, no binary downloads (e.g. exe) were tested. ActiveX, VBscript based downloaders are out of scope in the exploit test section.
6. The virtual machine is reverted to a clean state and traffic was replayed by the proxy server. The replay meant that the browser is used as before, but instead of the original webservers, the proxy server answers the requests based on the recorded traffic. In this replay, other traffic is allowed, which means that unmatched requests (previously not recorded) are answered as without the proxy. When the “replayed exploit” is able to infect the OS, the exploit traffic is marked as a source for the tests. This method guarantees that exactly the same traffic will be seen by the endpoint protection systems, even if the original exploit kit goes down during the tests. Although this might be axiomatic, it is important to note that no exploit traffic test case was deleted after this step of the test. All tests are included in the final results. In the case of HTTPS traffic, the original site is contacted, without replaying.
7. After new exploit traffic is approved, the endpoint protection systems are tested, in a random order. Before the exploit site is tested, it is verified that the endpoint protection had been updated to the latest version with the latest signatures and that every cloud connection is working. If there is a need to restart the system, it is restarted. In the proxy setup, unmatched requests are allowed to pass through. No VPN is used during the test. When user interaction is needed from the endpoint protection (e.g. site visit not recommended, etc.), the block/deny action is chosen. When user interaction is needed from Windows, we chose the run/allow options, except for UAC. No other processes are running on the system, except the Process Monitor from Sysinternals and Wireshark (both installed to non-default directories and modified not to be detected by default tools).
8. After navigating to the exploit site, the system is monitored to check for new processes, loaded DLLs or C&C traffic.
9. After an endpoint protection suite is tested, a new endpoint protection is randomly selected for the test until all endpoint protection products had been tested.
10. The process goes back to step 7. until all exploit site test cases are reached.

Methodology of the Performance test

1. Windows 10 64-bit operating system was installed on a physical machine, all updates are applied and third-party applications installed and updated.
2. A backup image of the operating system was created.
3. A security application was installed into the OS. Same configuration is used as in the other tests.
4. The following performance metrics were measured:
    a. Install time, starting from downloading the installer binary, finished when the security application is installed, started, and the GUI is working.
    b. Size of the files installed and created by the security application. The size is measured both after the installation, and after some time passed with normal computer usage.
    c. CPU overhead of the processes and services belonging to the security applications are summed.
    d. Memory footprint (private and shared working set) of the processes and services belonging to the security applications are summed.
    e. Performance impact on the browser load time is measured. The browser should fully load a complex website, from a local network URL or replay proxy.

Every performance result is the average of three times measurement except for the Firefox start-up time as it was measured twenty times for each vendor.

Performance chart was calculated based on:

- The security product reaching the best result in the category was rewarded with 10 points, the second received 9 points and so on. Once every performance category was measured, the points were added, the final result was summed and the calculation is shown according to these scores. Test cases indicated by N/A were rewarded with 10 points as there was basically 0 resource usage.

Physical machine specification:

- OS: Windows 10 x64
- CPU: Intel Core i5
- Memory: 8GB
- Storage: 100GB SSD

Non-default endpoint protection configurations

During this quarter, all endpoint protection software was running on default configuration.

[1] VM hardware specification is 100GB SSD, 4GB RAM & 2 core processor.

[1] AES includes Adobe Flash, Reader, Java, Microsoft Office 2010, Edge & VLC Player. All Microsoft components were fully updated; all third-party components were out of date by three months.[1]