MRG Effitas 360 Degree Assessment & Certification

Q2 2018

Contents

Introduction

MRG Effitas has a core focus on efficacy assessments in the anti–financial fraud space, but we also publish more traditional "Real World" detection tests.

For this assessment, time-to-detect will employ a methodology based on the infected endpoint being re-scanned once during a 24-hour period.

The methodology employed in this test maps more closely to Real World use, and although it may not be a 100% accurate model of how an "average" system is used, it gives a more realistic assessment of a security product's ability to detect and remediate an infected endpoint.

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.

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 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 Q2 2018 360 certification award, these being: **avast! Internet Security, Avira Internet Security, BitDefender Internet Security, ESET Internet Security, F-secure Business - Computer Protection, Kaspersky Internet Security, McAfee Total Protection, Microsoft Windows Defender, Symantec Norton Security, Trend Micro Maximum Security, Webroot SecureAnywhere**

The other 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 user initiated rescan (Level 2 pass). Applications that meet this specification are given certification for that quarter. PUA/Adware test is not part of the certification.

Under the MRG Effitas 360 Degree Assessment & Certification, the following products were certified for Q2 2018:

Certified (level 1): **avast! Internet Security, Avira Internet Security, ESET Internet Security, F-secure Business - Computer Protection, Kaspersky Internet Security, Symantec Norton Security**

Certified (level 2): **BitDefender Internet Security, McAfee Total Protection, Microsoft Windows Defender, Trend Micro Maximum Security, Webroot SecureAnywhere**

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-tp001-mrg-q2-2018/

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 re-scanned once a day (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, all 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 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 rescue an encrypted or locked 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 (Q2 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 of the URLs pose as fake porn websites serving visitors with various types of malware. The remaining 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 great challenge to all participants.

It is our opinion that Ransomware currently poses the greatest threat to users, for this reason we choose to use more URLs serving this threat than before.

Because of the wide spectrum of malware used in this project and the freshness of the samples, we used a smaller set than usual.

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.

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.

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.

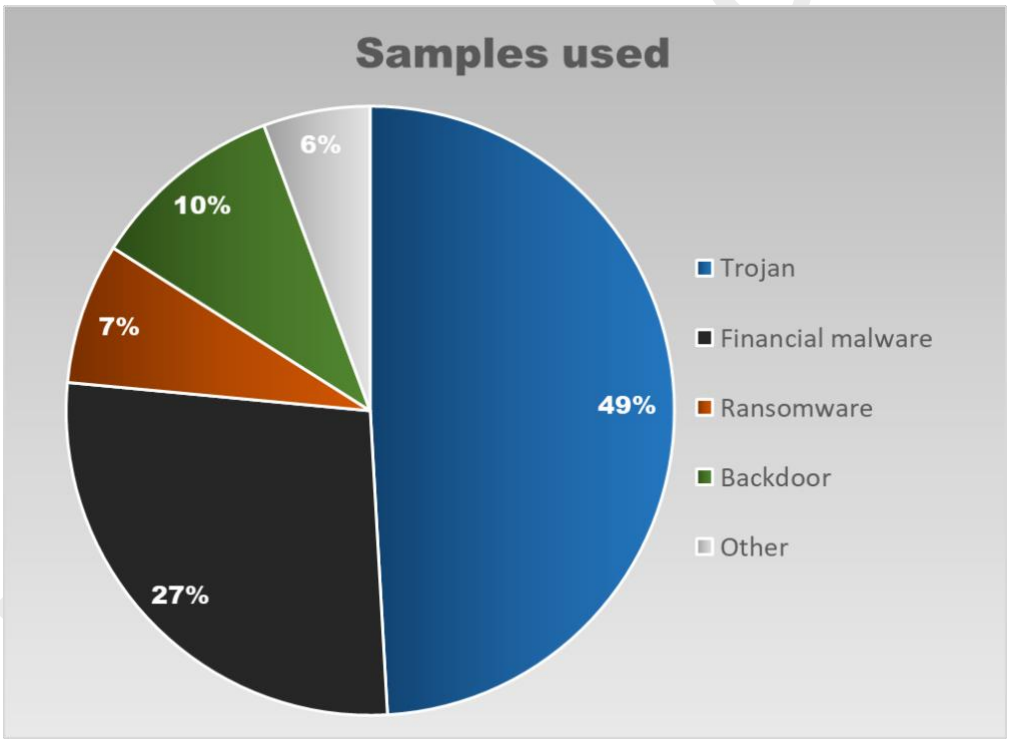
~10% of the threats used in this test were introduced to the system via internal webmail sites.

Testing was conducted as per the methodology detailed in Appendix 1. In total, 387 live ITW samples were used. The stimulus load comprised the following: 190 trojans, 40 backdoors, 106 financial malware samples, 29 ransomware samples, and 22 others. Additionally, to the ITW assessment we tested the products against 20 PUAs as well.

Security Applications Tested

- avast! Internet Security 18.5.2342
- Avira Internet Security 15.0.34.27
- BitDefender Internet Security 2018 22.0.21.297
- ESET Internet Security 11.1.54.0
- F-secure Business, Computer Protection 18.5
- Kaspersky Internet Security 2018 18.0.0.405 (h)
- McAfee Total Protection 16.0 R13
- Microsoft Windows Defender with SmartScreen 4.12.16299.15
- Symantec Norton Security 22.14.2.13
- Trend Micro Maximum Security 12.0.1226
- Webroot SecureAnywhere 9.0.20.31

Malware sample types used to conduct the tests

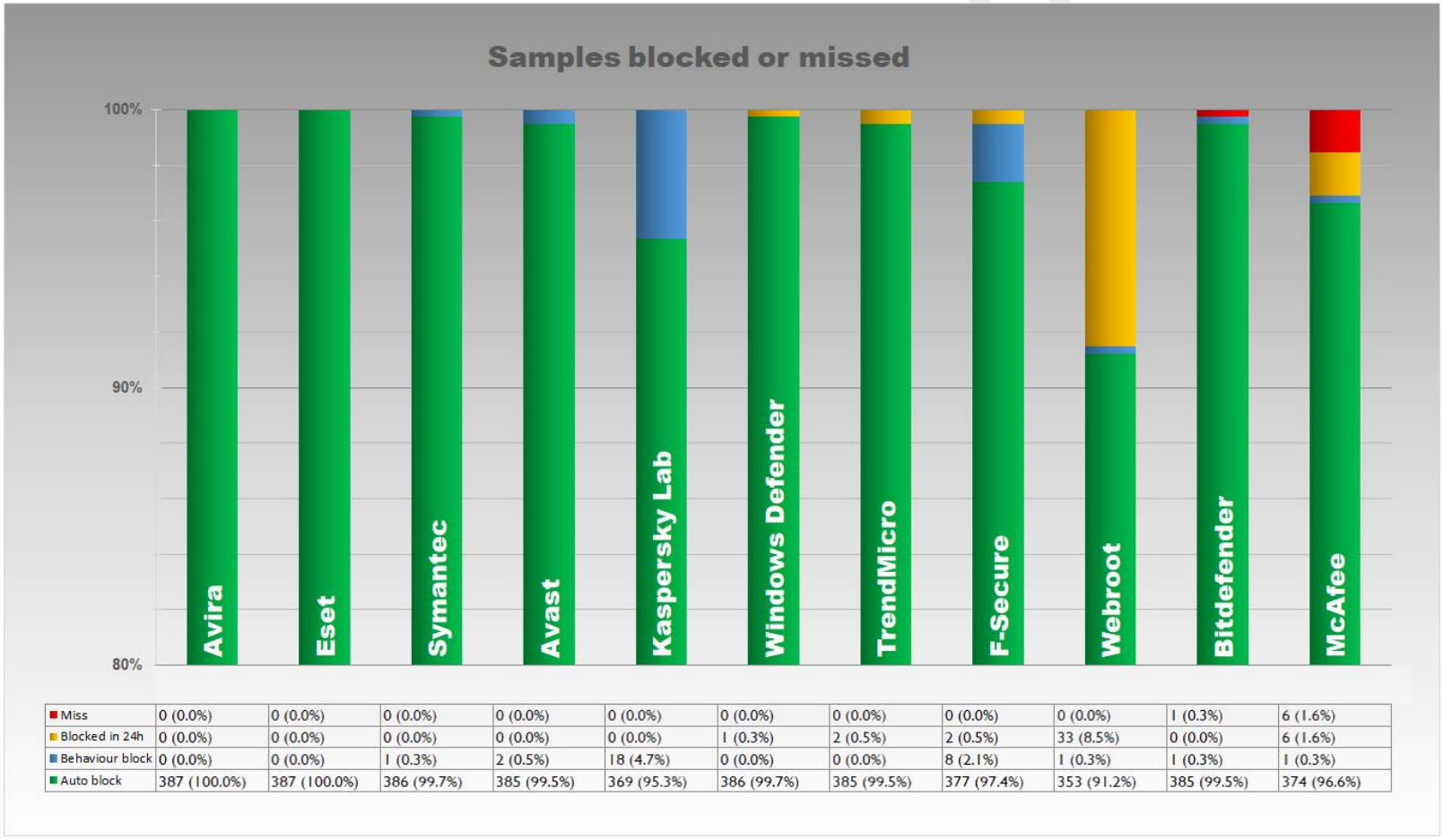


Test Results

The tables below show the results of testing under the MRG Effitas 360 Q2 Assessment Programme.

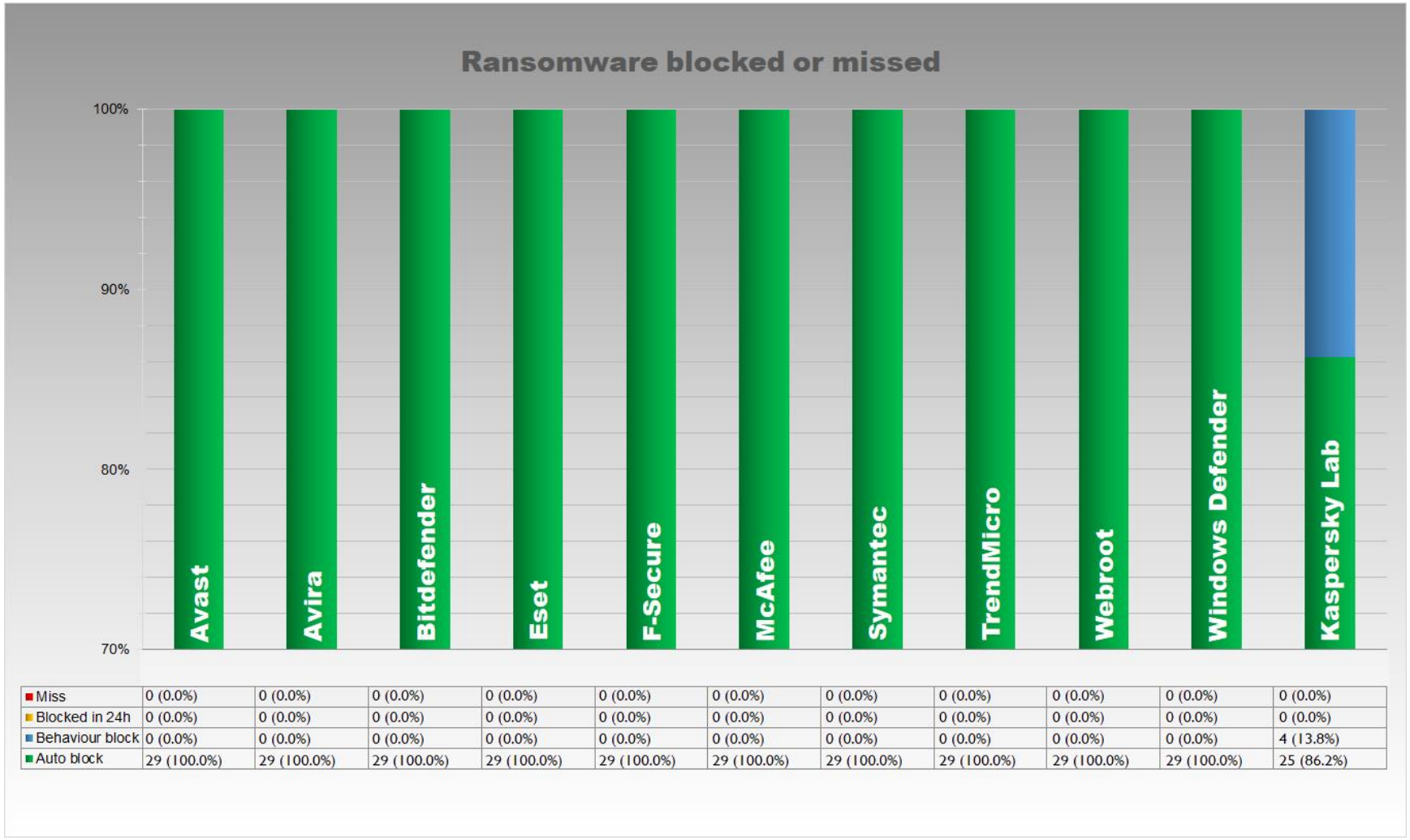
Q2 2018 In the Wild 360 / Full Spectrum Test Results

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



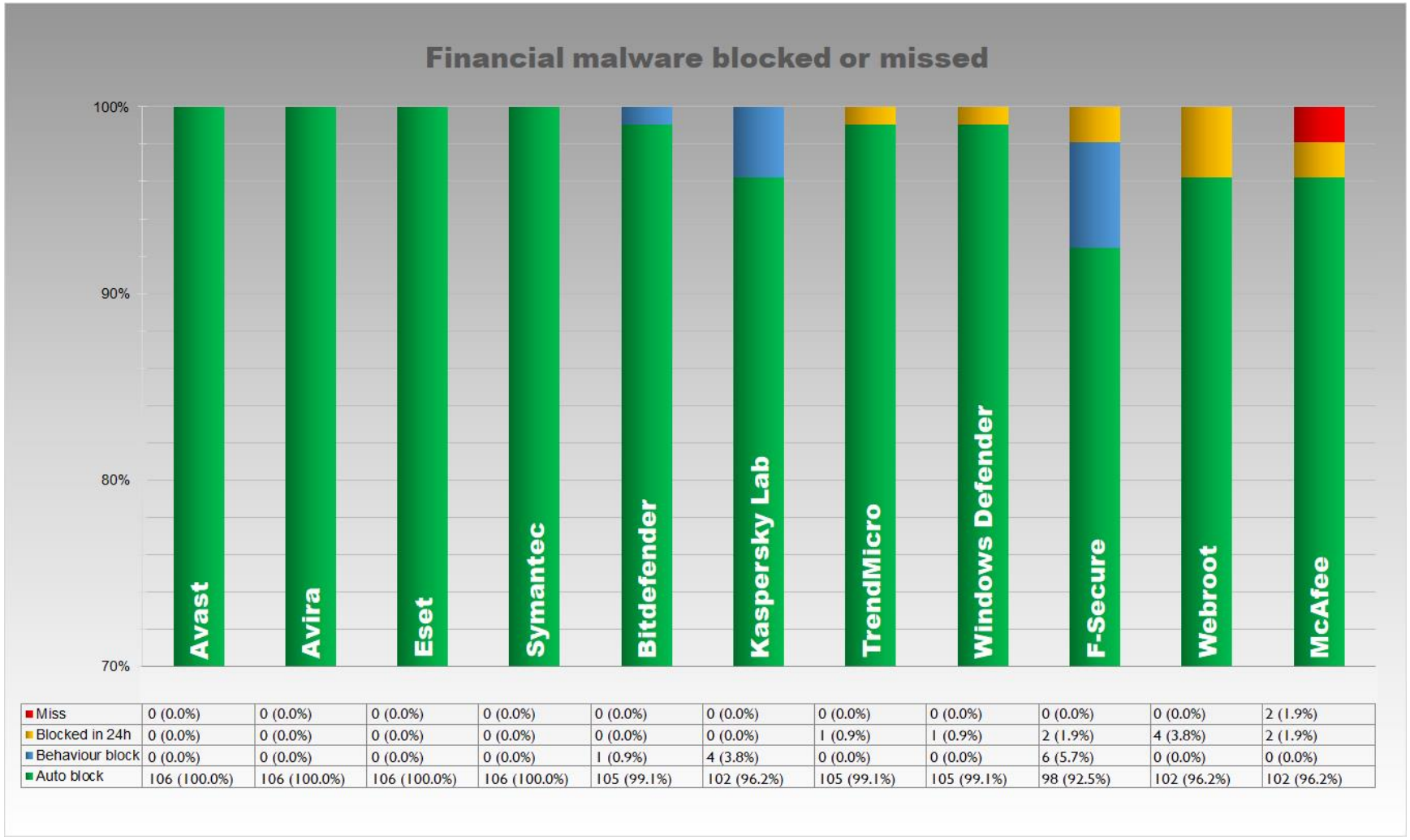
	Avira	Eset	Symantec	Avast	Kaspersky Lab	Windows Defender	TrendMicro	F-Secure	Webroot	Bitdefender	McAfee
Miss	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (0.3%)	6 (1.6%)
Blocked in 24h	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (0.3%)	2 (0.5%)	2 (0.5%)	33 (8.5%)	0 (0.0%)	6 (1.6%)
Behaviour block	0 (0.0%)	0 (0.0%)	1 (0.3%)	2 (0.5%)	18 (4.7%)	0 (0.0%)	0 (0.0%)	8 (2.1%)	1 (0.3%)	1 (0.3%)	1 (0.3%)
Auto block	387 (100.0%)	387 (100.0%)	386 (99.7%)	385 (99.5%)	369 (95.3%)	386 (99.7%)	385 (99.5%)	377 (97.4%)	353 (91.2%)	385 (99.5%)	374 (96.6%)

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



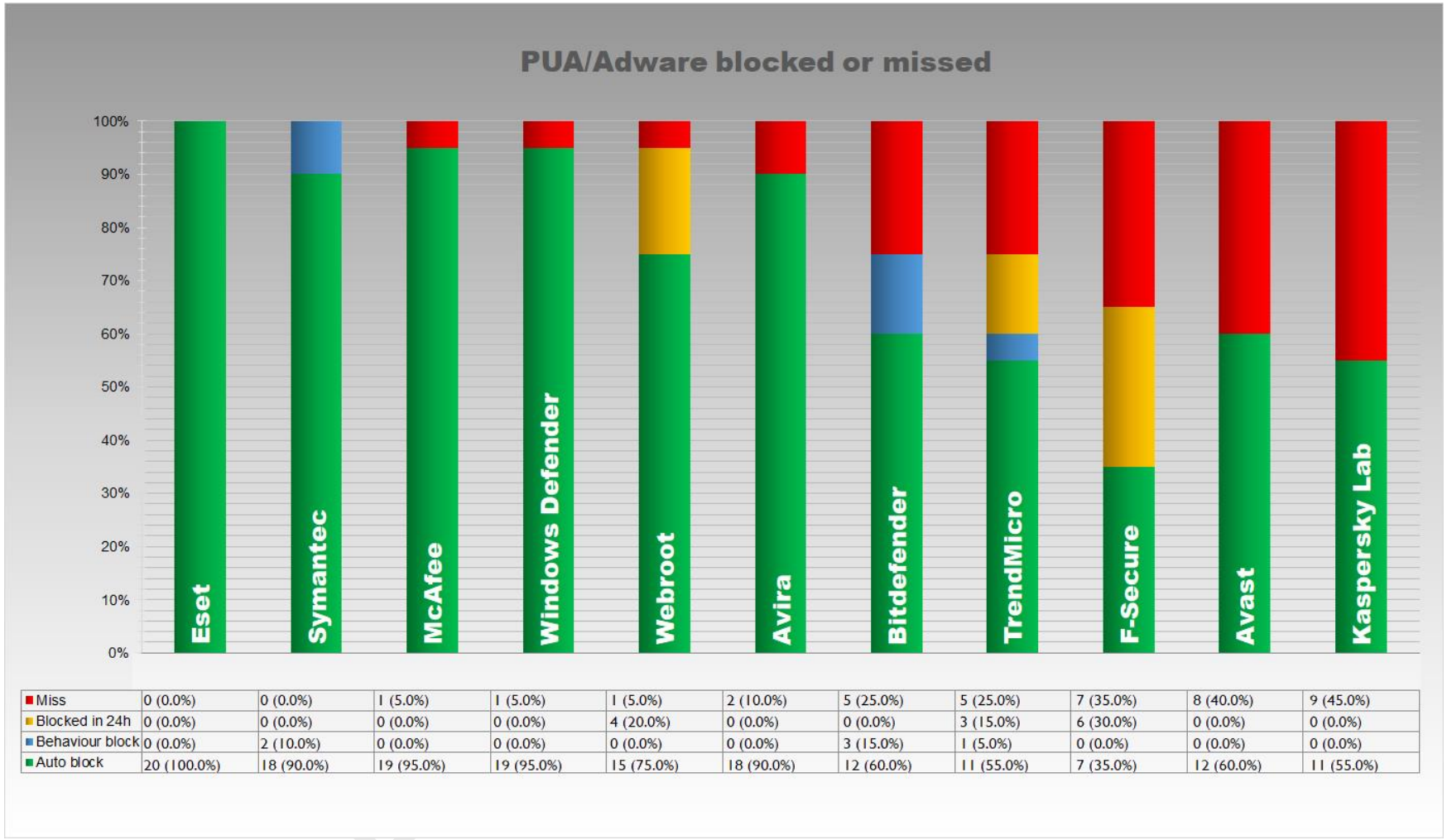
	Avast	Avira	Bitdefender	Eset	F-Secure	McAfee	Symantec	TrendMicro	Webroot	Windows Defender	Kaspersky Lab
Miss	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Blocked in 24h	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Behaviour block	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (13.8%)
Auto block	29 (100.0%)	29 (100.0%)	29 (100.0%)	29 (100.0%)	29 (100.0%)	29 (100.0%)	29 (100.0%)	29 (100.0%)	29 (100.0%)	29 (100.0%)	25 (86.2%)

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



Miss	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (1.9%)
Blocked in 24h	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (0.9%)	1 (0.9%)	2 (1.9%)	4 (3.8%)	2 (1.9%)
Behaviour block	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (0.9%)	4 (3.8%)	0 (0.0%)	0 (0.0%)	6 (5.7%)	0 (0.0%)	0 (0.0%)
Auto block	106 (100.0%)	106 (100.0%)	106 (100.0%)	106 (100.0%)	105 (99.1%)	102 (96.2%)	105 (99.1%)	105 (99.1%)	98 (92.5%)	102 (96.2%)	102 (96.2%)

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



	Eset	Symantec	McAfee	Windows Defender	Webroot	Avira	Bitdefender	TrendMicro	F-Secure	Avast	Kaspersky Lab
Miss	0 (0.0%)	0 (0.0%)	1 (5.0%)	1 (5.0%)	1 (5.0%)	2 (10.0%)	5 (25.0%)	5 (25.0%)	7 (35.0%)	8 (40.0%)	9 (45.0%)
Blocked in 24h	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	4 (20.0%)	0 (0.0%)	0 (0.0%)	3 (15.0%)	6 (30.0%)	0 (0.0%)	0 (0.0%)
Behaviour block	0 (0.0%)	2 (10.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	3 (15.0%)	1 (5.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)
Auto block	20 (100.0%)	18 (90.0%)	19 (95.0%)	19 (95.0%)	15 (75.0%)	18 (90.0%)	12 (60.0%)	11 (55.0%)	7 (35.0%)	12 (60.0%)	11 (55.0%)

Understanding Grade of Pass

- **Level 1** = All threats detected on first exposure or via behaviour protection.

  avast! Internet Security

  Avira Internet Security

  ESET Internet Security

  F-secure Business, Computer Protection

  Kaspersky Internet Security

  Symantec Norton Security

- **Level 2** = At least 98% of the threats detected and neutralised / system remediated before or on the first rescan.

  BitDefender Internet Security

  McAfee Total Protection

  Microsoft Windows Defender with SmartScreen

  Trend Micro Maximum Security

  Webroot SecureAnywhere

- **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 360 Assessment & Certification Programme Q2 2018

1. Windows 10 64 bit operating system was installed on a virtual machine[i], all updates were applied and third party applications installed and updated according to our "Average Endpoint Specification"[ii]
2. An image of the operating system was 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[iii] on each of the systems created in 3. and then, where applicable, updated.
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 malicious binary from its native URL using Microsoft Edge to the desktop and then executing the binary.
    b. The security application blocked the URL where the malicious binary was located.
    c. The security application detected and blocked the malicious binary whilst it was being downloaded to the desktop.
    d. 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. Testing on infected systems continued for 24 hours. The system was rescanned once, 24 hours after the system was compromised.
9. Remediation performance of an application was determined by manual inspection of the system in contrast to its pre-infected state and not by the logs and reports of the security application itself.[iv]
10. Testing was conducted with all systems having internet access.
11. Each individual test for each security application was conducted from a unique IP address.
12. All security applications were fully-functional unregistered or registered versions with no connection to MRG Effitas.
13. All testing was conducted during Q2 2018.
14. As no user initiated scans were involved in this test, applications relied on various technologies to detect, block and remediate threats. Some of these technologies were: background scanning, startup scanning, scheduled scanning, system monitors, etc. A scheduled scan was used only if enabled by default.

[i] VM hardware spec is 4GB RAM & 2 core processor.
[ii] 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.
[iii] During installation of the security application, if an option to detect PUAs was given, it was selected.
[iv] This is because in some instances, an application will claim to have removed an infection, but actually failed to do so and was still active on the system.