MRG Effitas Android AV review

Contents

Introduction

MRG Effitas is an independent IT security research company, with a heavy focus on applied malware analysis. Besides conventional AV efficacy testing and providing samples to other players in the AV field, we regularly test APT appliances and enterprise grade IT security products, simulating realistic attack scenarios. In this regard, testing methods have evolved rapidly over the last couple of years as most labs, under the guidance of AMTSO (of which MRG Effitas is a member) strived to conduct "Real World" testing.

Tests Applied

MRG Effitas performed an in-depth test of several Android AVs. Our efforts were focused on two aspects of the products:

1. Efficacy of the AV application, the level of protection in real-life scenarios with in-the-wild pieces of malware. This report summarises the results of efficacy tests. Our test scenario focused on an early stage of detection, when the sample has been copied on the sdcard drive of the test device.
2. We tested the AV application itself, in order to identify any weakness that might even increase the attack surface of the device. Efforts were focused on self defence and the potential leak of private user data. Reports of this stage are shared exclusively with the vendors.

During the assessment, we ran the following test suite to simulate the early stage of malware infection. In the tested scenario, the device has not yet been infected with the samples, the malicious .apk files are only downloaded to the sdcard, ready to be installed.

Testing took place on an Android 5.1.1 Genymotion emulator image. In cases where ARM native libraries have been used and could not install the application on an x86 emulator, we opted for a stock Nexus 5x device with the then-latest Android 7.1.1.

1. Having initialised the device, we installed the AV application and initialised it (accepted EULA, downloaded the latest definition file etc.) When asked, we enabled all features that can be enabled for free.
2. We set up the application to include the sdcard in the scan scope.
3. We downloaded the sample set to the sdcard and started the scan.
4. We instructed the application to remove all suspicious files.
5. We ran the scan again, until we saw no warning or suspicious files on the device.
6. We collected the remaining samples.

Testing focused on an early stage detection, which means that the samples have not been installed but downloaded to the internal storage of the device. In our opinion, a properly designed AV suite should detect threats as early as possible and should not allow users to install potentially dangerous applications on their devices.

Test Samples

Testing used an initial 200-sample malware set, with a 20-sample set of legitimate applications from the Play Store.

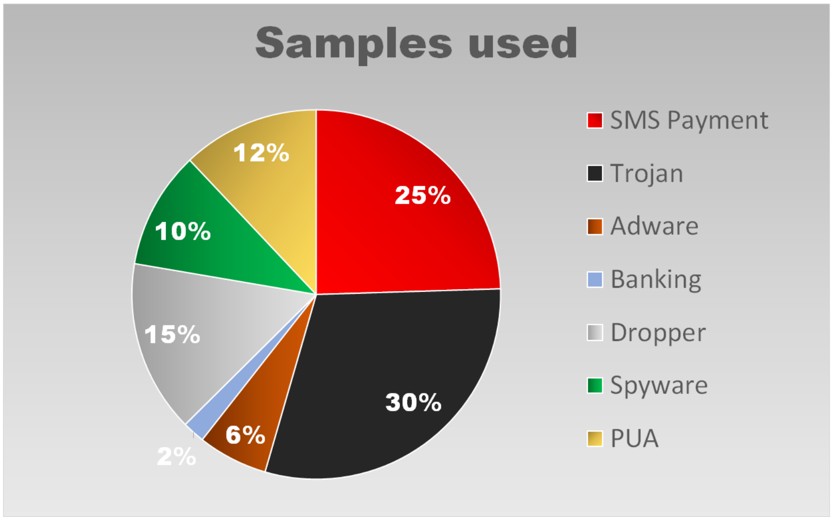


Figure 1 – Malware sample set distribution

The samples have been collected in the wild.

- **SMS Payment.** The application provides features to send SMS messages to premium rate numbers. Most of the selected samples were able to 'auto-send' messages, as they opted for the SEND_SMS permission, resulting in a direct financial loss for the victim.
- **Trojan.** Trojans are applications, which display a certain set of features within their description. However, the implemented modules require a wide range of permissions which do not belong to the advertised functionality. A typical example is a flashlight app, which can read the contact list, the GPS position and send them to the Internet.
- **Adware.** The downloaded application implements little or no functionality besides displaying ads on the screen, which, besides legitimate apps, might lure the user into downloading more malware (e.g. with a fake 'the device is infected! Download this AV now!' screen). Typical traits of such applications are that they require permissions to draw over other apps for no obvious reason (SYSTEM_ALERT_WINDOW permission).
- **Spyware.** We classified a sample Spyware if it leaks information, which can be used to track the user (as most security-conscious users do not wish to be tracked). Ironically, most ad propelled applications qualify as spyware, as they leak IMEI, phone number etc. to the ad provider network.
- **Banking.** This type of malware detects if the user is logged in to a mobile banking session using either a browser or mobile banking application and, for instance, might attempt to display a matching phishing site or to draw an overlay window to fool the user into thinking that the session has ended and that they need to re-authenticate. Typically, such samples use permissions to get the task list, combined with the SYSTEM_ALERT_WINDOW permission.

- **Dropper.** Droppers are used to download the actual malware to the device. Usually, a dropper is very hard to distinguish from a 'normal' app, as ad modules portray a similar kind of operation.
- **PUA.** The term 'Potentially Unwanted Applications' denotes applications, containing modules, which perform actions that are not in alignment with the security-conscious user's intentions. For instance, applications provided with aggressive advertisement modules usually make it possible for ad campaigners to track individual users, even to assign the device with the user's demographic properties through social network ad services. Effitas claims that security-conscious users are sensitive regarding their privacy and possibly no application feature can make it up for the users' private data and browsing habits to be sold over the Internet and a decent AV should let the user know if such an application is about to be installed.

Note that most samples implement several kinds of operation, therefore most samples fall into several categories (For instance, consider a typical piece of malware, which serves malicious ads and if possible, it attempts to obtain the SEND_SMS permission to send premium rate messages).

Security Applications Tested

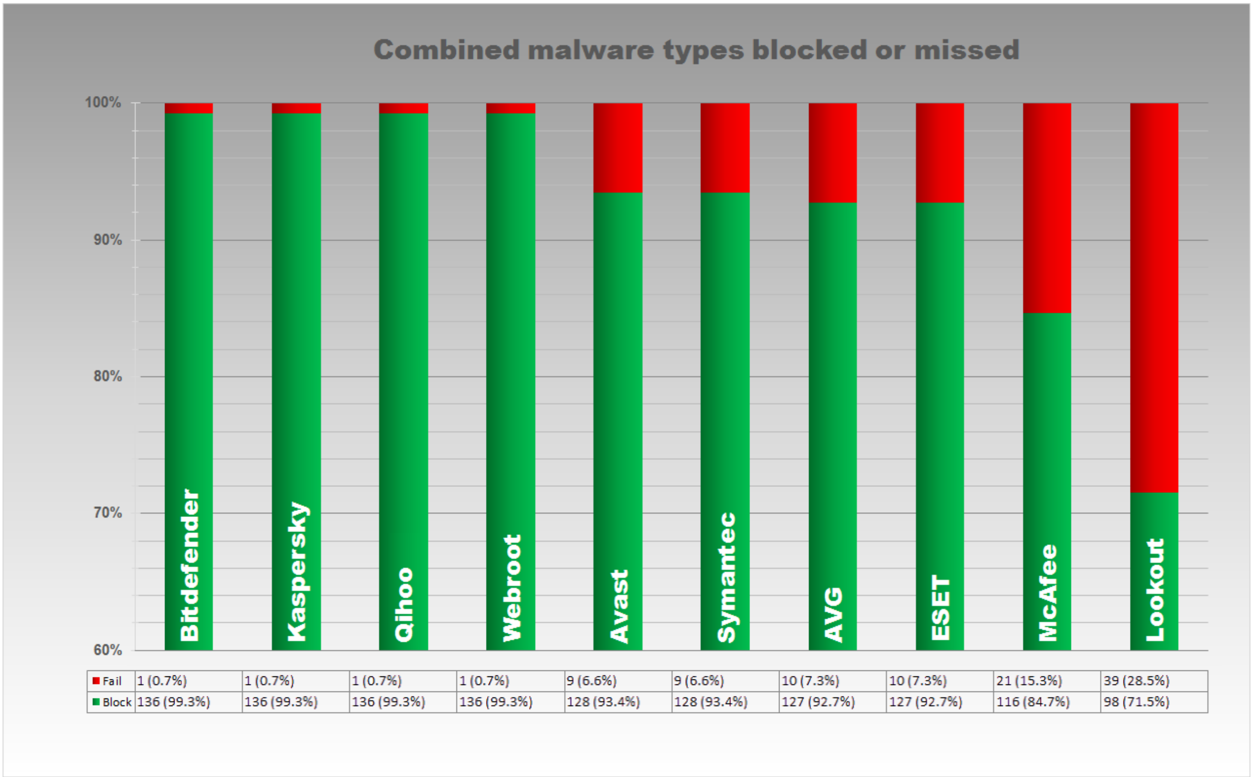
The following security suites have been selected for testing:

- Kaspersky Internet Security 11.13.4.803
- Webroot SecureAnywhere 4.1.0.832
- ESET Mobile Security 3.5.100.0
- Lookout 10.6.2-188fb64[1]
- McAfee Security 4.9.0.336
- Norton Mobile Security 3.18.0.3226
- Qihoo 360 Security 3.8.9.4821
- AVG AntiVirus 5.9.4.1
- Avast Mobile Security 6.0.1
- BitDefender Antivirus Free 3.2.188

Test Results

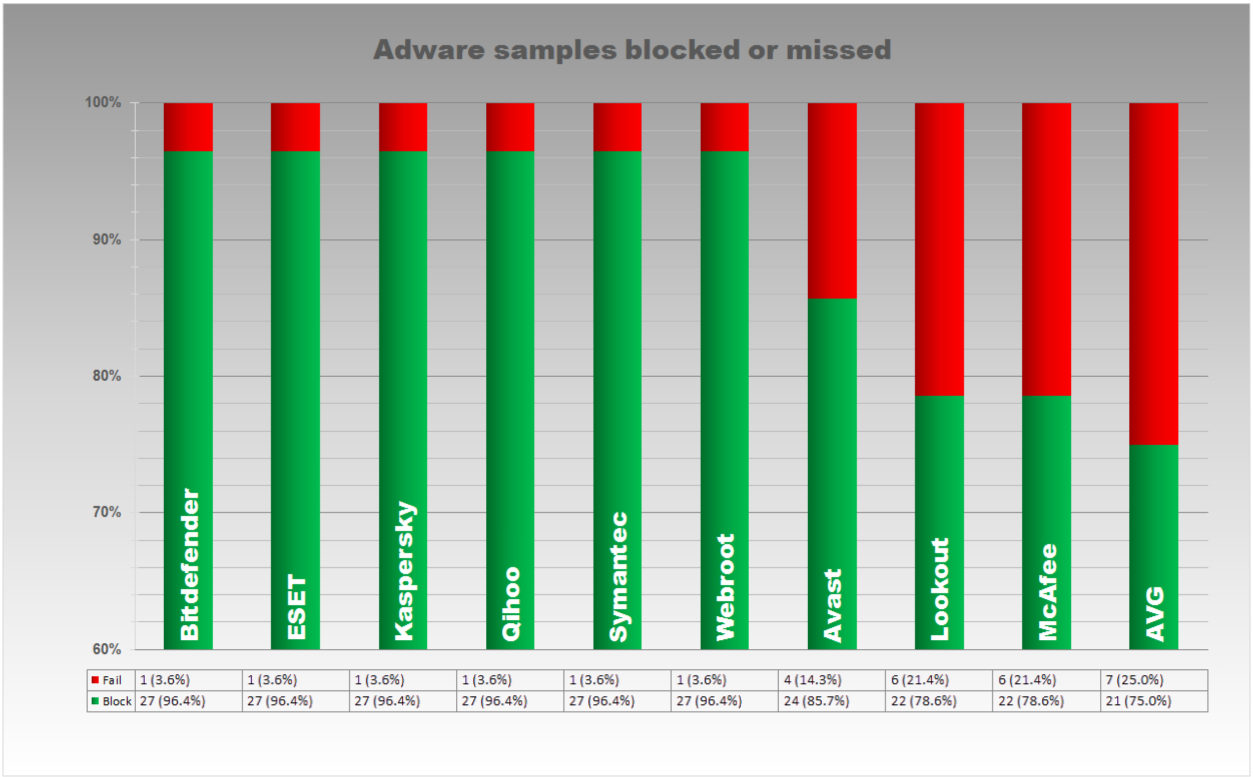
The tables below show the results of testing under the MRG Effitas Android AV Testing Program.

[1] During testing, the installed Lookout instance had issues when removing some samples from the device sdcard storage. Namely, even though the sample had been detected, the AV was unable to actually remove the sample. Since actual detection had taken place, we counted such samples as passed test cases.



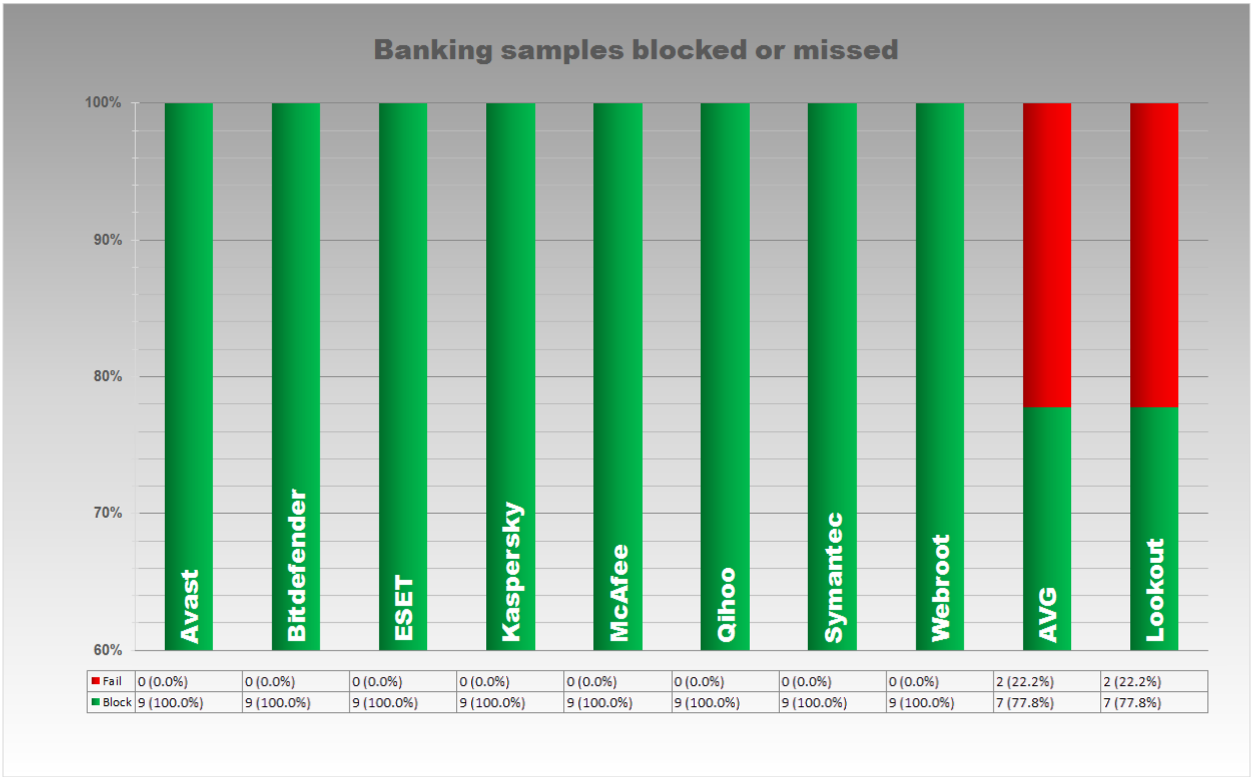
	Bitdefender	Kaspersky	Qihoo	Webroot	Avast	Symantec	AVG	ESET	McAfee	Lookout
🟥 Fail	1 (0.7%)	1 (0.7%)	1 (0.7%)	1 (0.7%)	9 (6.6%)	9 (6.6%)	10 (7.3%)	10 (7.3%)	21 (15.3%)	39 (28.5%)
🟩 Block	136 (99.3%)	136 (99.3%)	136 (99.3%)	136 (99.3%)	128 (93.4%)	128 (93.4%)	127 (92.7%)	127 (92.7%)	116 (84.7%)	98 (71.5%)

Figure 2 Combined malware type detection rates (excluding PUA samples)



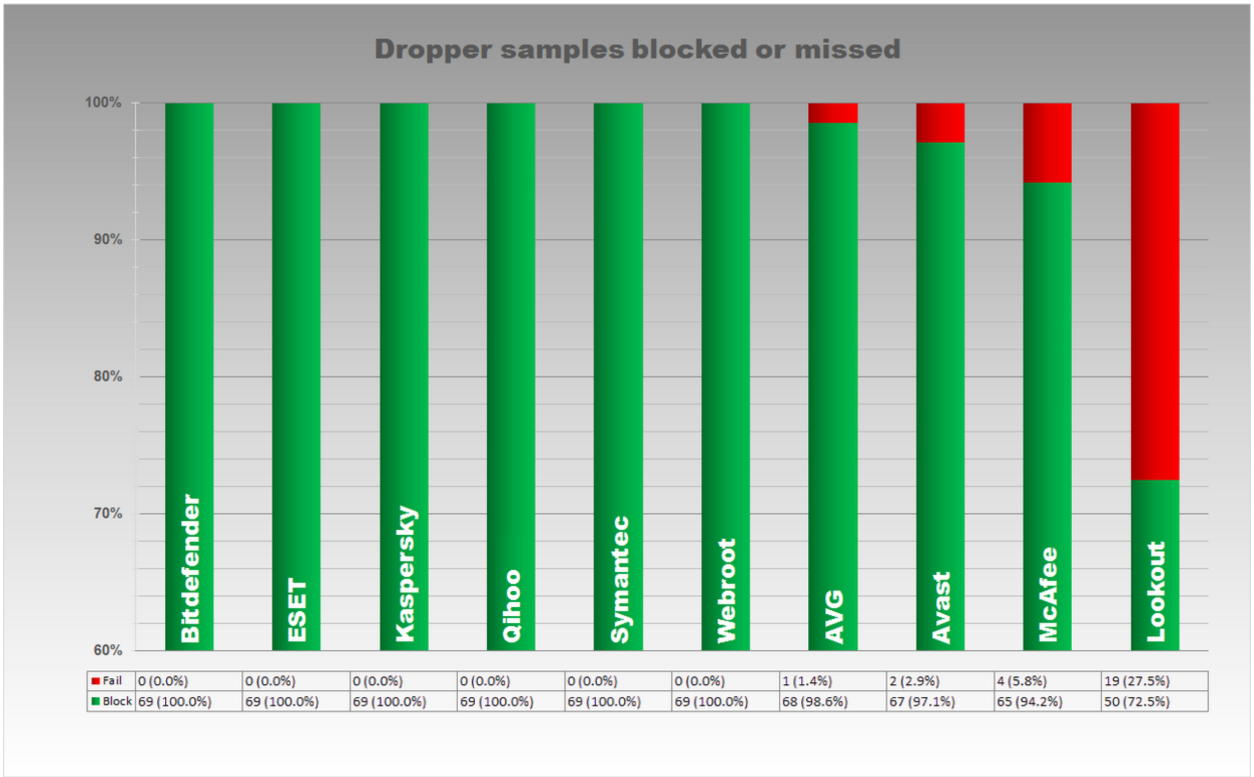
	Bitdefender	ESET	Kaspersky	Qihoo	Symantec	Webroot	Avast	Lookout	McAfee	AVG
🟥 Fail	1 (3.6%)	1 (3.6%)	1 (3.6%)	1 (3.6%)	1 (3.6%)	1 (3.6%)	4 (14.3%)	6 (21.4%)	6 (21.4%)	7 (25.0%)
🟩 Block	27 (96.4%)	27 (96.4%)	27 (96.4%)	27 (96.4%)	27 (96.4%)	27 (96.4%)	24 (85.7%)	22 (78.6%)	22 (78.6%)	21 (75.0%)

Figure 3 Early detection of adware



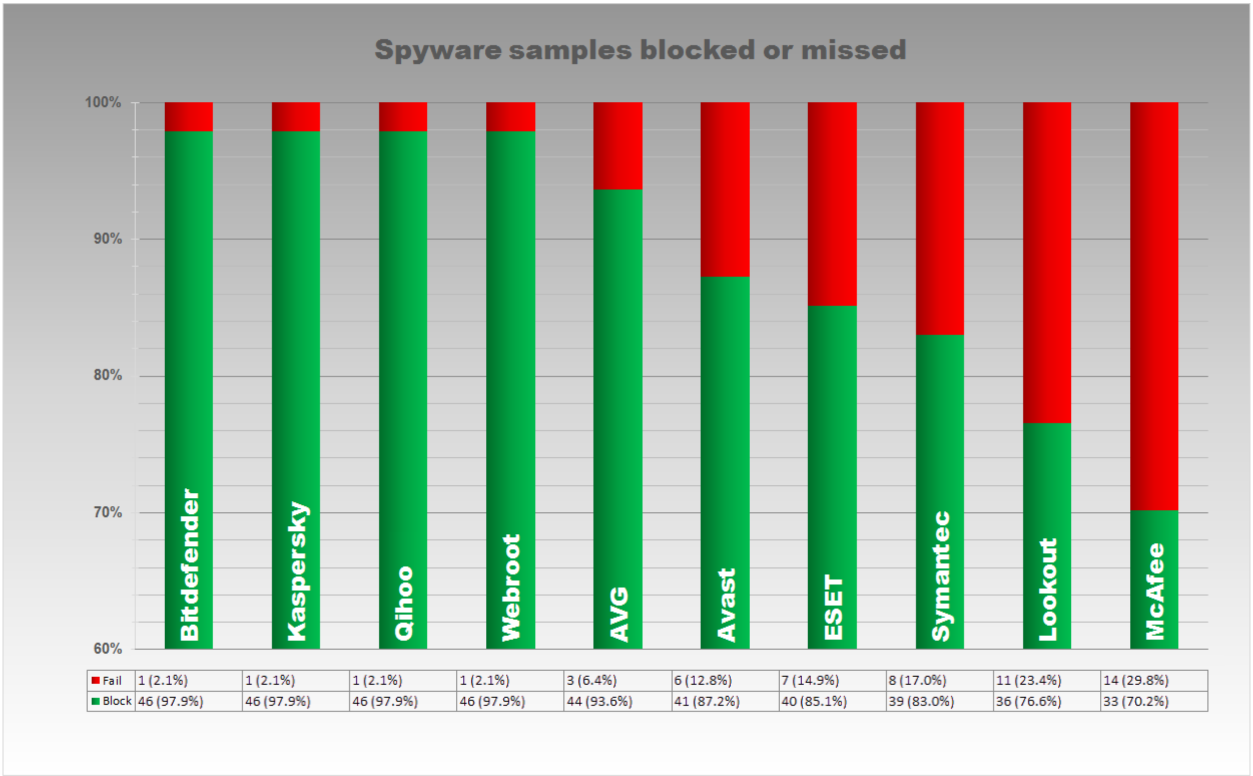
	Avast	Bitdefender	ESET	Kaspersky	McAfee	Qihoo	Symantec	Webroot	AVG	Lookout
🟥 Fail	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	2 (22.2%)	2 (22.2%)
🟩 Block	9 (100.0%)	9 (100.0%)	9 (100.0%)	9 (100.0%)	9 (100.0%)	9 (100.0%)	9 (100.0%)	9 (100.0%)	7 (77.8%)	7 (77.8%)

Figure 4 Early detection of banking malware



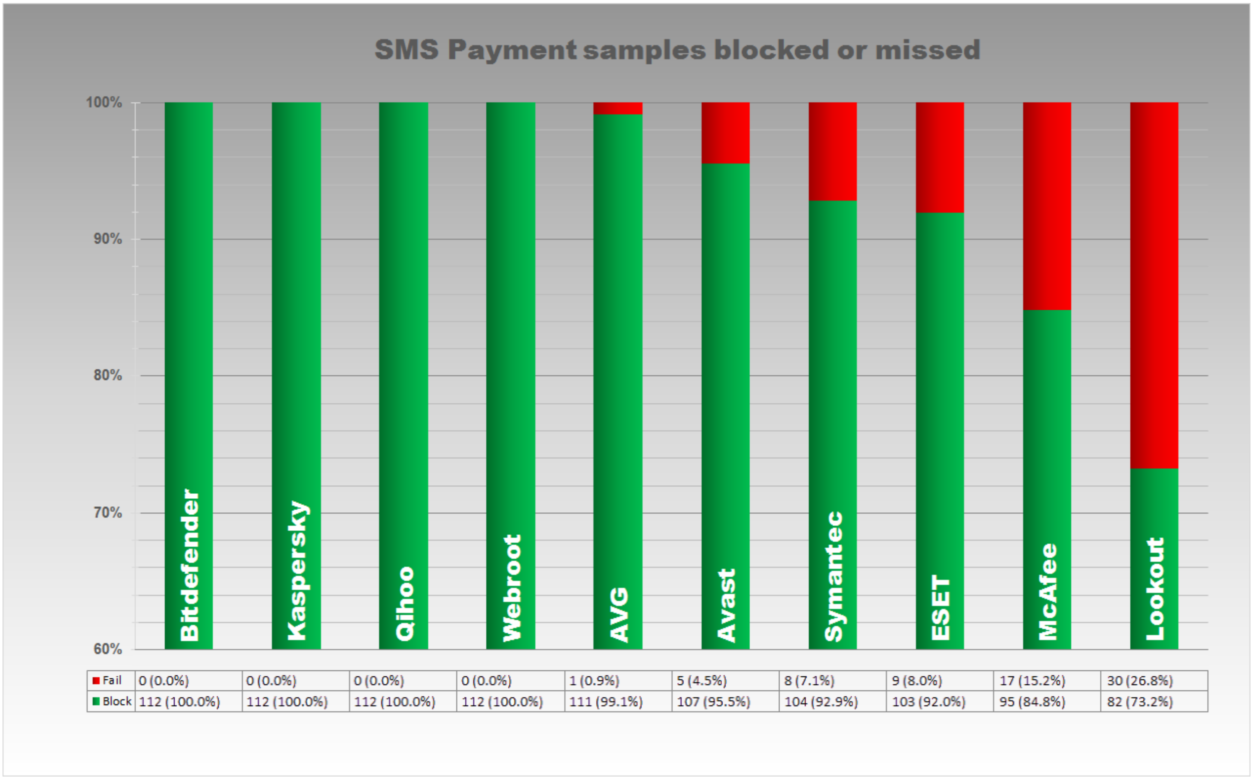
	Bitdefender	ESET	Kaspersky	Qihoo	Symantec	Webroot	AVG	Avast	McAfee	Lookout
🟥 Fail	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (1.4%)	2 (2.9%)	4 (5.8%)	19 (27.5%)
🟩 Block	69 (100.0%)	69 (100.0%)	69 (100.0%)	69 (100.0%)	69 (100.0%)	69 (100.0%)	68 (98.6%)	67 (97.1%)	65 (94.2%)	50 (72.5%)

Figure 5 Early detection of dropper samples



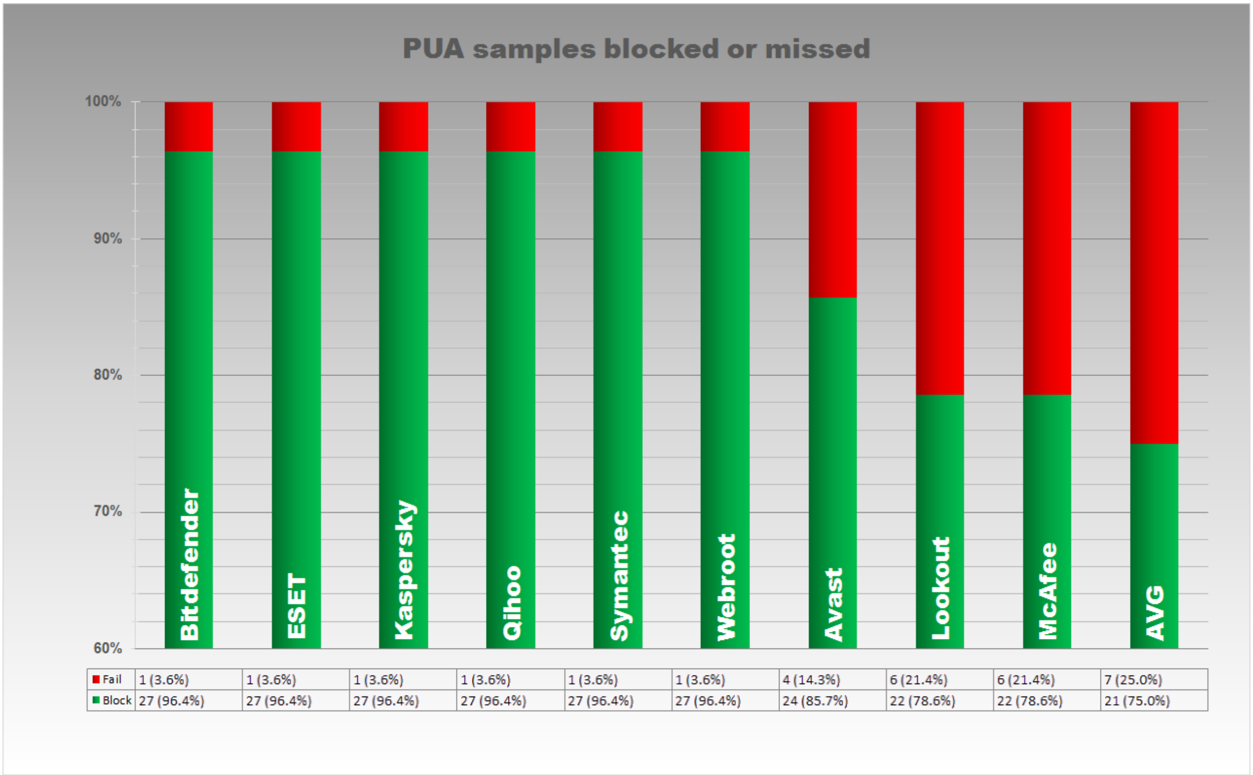
	Bitdefender	Kaspersky	Qihoo	Webroot	AVG	Avast	ESET	Symantec	Lookout	McAfee
🟥 Fail	1 (2.1%)	1 (2.1%)	1 (2.1%)	1 (2.1%)	3 (6.4%)	6 (12.8%)	7 (14.9%)	8 (17.0%)	11 (23.4%)	14 (29.8%)
🟩 Block	46 (97.9%)	46 (97.9%)	46 (97.9%)	46 (97.9%)	44 (93.6%)	41 (87.2%)	40 (85.1%)	39 (83.0%)	36 (76.6%)	33 (70.2%)

Figure 6 Early detection of spyware samples



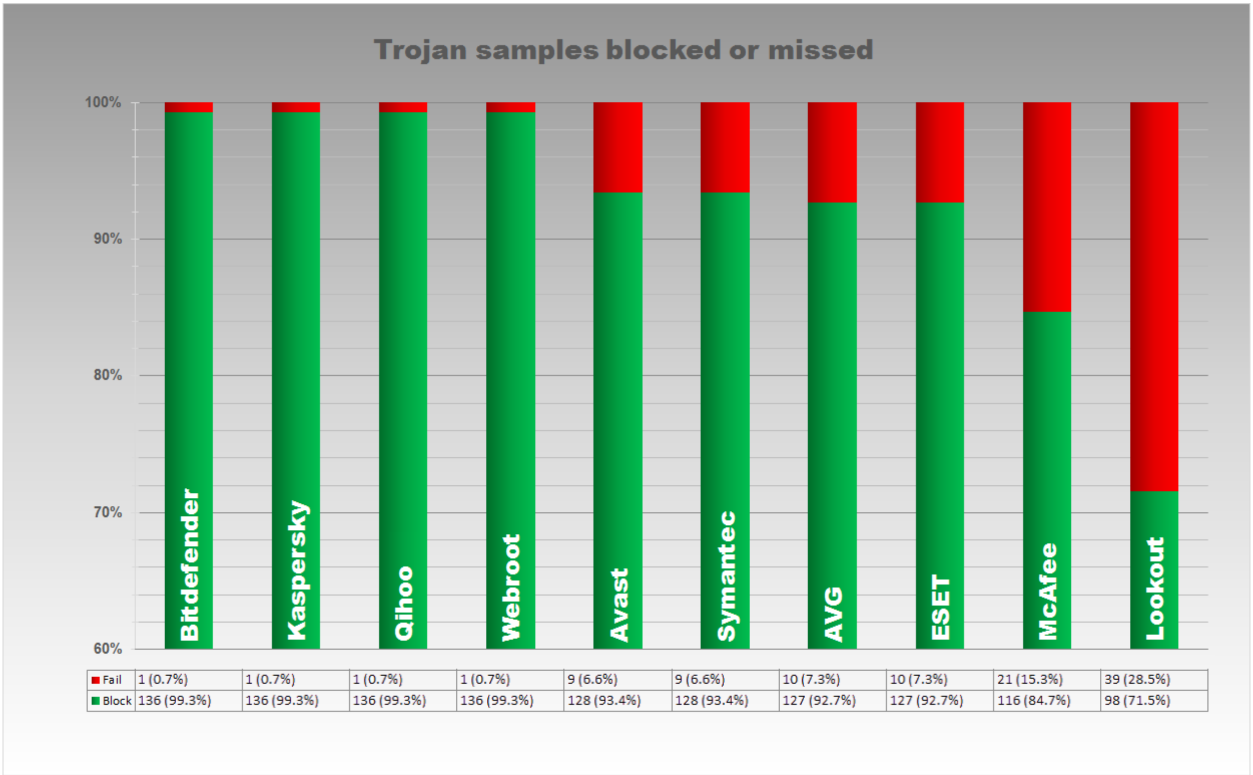
	Bitdefender	Kaspersky	Qihoo	Webroot	AVG	Avast	Symantec	ESET	McAfee	Lookout
🟥 Fail	0 (0.0%)	0 (0.0%)	0 (0.0%)	0 (0.0%)	1 (0.9%)	5 (4.5%)	8 (7.1%)	9 (8.0%)	17 (15.2%)	30 (26.8%)
🟩 Block	112 (100.0%)	112 (100.0%)	112 (100.0%)	112 (100.0%)	111 (99.1%)	107 (95.5%)	104 (92.9%)	103 (92.0%)	95 (84.8%)	82 (73.2%)

Figure 7 Detection of malicious SMS payment samples



	Bitdefender	ESET	Kaspersky	Qihoo	Symantec	Webroot	Avast	Lookout	McAfee	AVG
🟥 Fail	1 (3.6%)	1 (3.6%)	1 (3.6%)	1 (3.6%)	1 (3.6%)	1 (3.6%)	4 (14.3%)	6 (21.4%)	6 (21.4%)	7 (25.0%)
🟩 Block	27 (96.4%)	27 (96.4%)	27 (96.4%)	27 (96.4%)	27 (96.4%)	27 (96.4%)	24 (85.7%)	22 (78.6%)	22 (78.6%)	21 (75.0%)

Figure 8 Detection of PUA samples



	Bitdefender	Kaspersky	Qihoo	Webroot	Avast	Symantec	AVG	ESET	McAfee	Lookout
🟥 Fail	1 (0.7%)	1 (0.7%)	1 (0.7%)	1 (0.7%)	9 (6.6%)	9 (6.6%)	10 (7.3%)	10 (7.3%)	21 (15.3%)	39 (28.5%)
🟩 Block	136 (99.3%)	136 (99.3%)	136 (99.3%)	136 (99.3%)	128 (93.4%)	128 (93.4%)	127 (92.7%)	127 (92.7%)	116 (84.7%)	98 (71.5%)

Figure 9 Detection of trojan samples

Conclusions

Testing revealed that AV vendors are in an interesting situation when it comes to the Android OS. The overall security design of the operating system makes it challenging to develop and maintain an effective on-demand protection, while the effects on battery lifetime and overall device performance are not affected noticeably.

Some sample types are particularly difficult to detect (such as adware or dropper-type malware), due to the fact that with these samples, the actual malicious payload either needs some kind of user interaction to be deployed (consider a fake AV screen), or at the time of testing, the ad network serves benign content and therefore, the sample is considered non-malicious.

One of the Vendors requested to express their views regarding PUA type samples.

> “We consider these samples as clean ones; they do nothing malicious and contain non-aggressive advertising modules, which do not make these apps PUA, from our point of view; an advertising model is the one of basic business models for Android, and it is not correct to accuse applications with ads of being bad until advertising modules behave aggressively”

Avast expressed that many of their detection routines kick in after installation, therefore the detection rate might be different in an installation scenario.

We hope that other testing houses and AV vendors will follow our example and make a step towards ad modules, which do not utilise hardware based (e.g. IMEI) or other identifiers to distribute targeted advertisements breaching user privacy. Furthermore, since most ads are HTML content downloaded from a 3rd party site, ad networks provide an additional attack surface and security-conscious users should be warned when installing such applications.

For example, consider a piece of malware which, provided with READ_PHONE_STATE and INTERNET permissions, reads out identifiers of the device and leaks it to malvertisers – this hypothetical application is clearly malicious and this is not altered by any added ‘useful’ functionality.

We understand that in order for ad providers to ensure their content reflects the user's interests it is necessary to have some kind of tracking - therefore the whole question of focused ads respecting user privacy should be reconsidered by end users. This subject is beyond the scope of this report.