Keywords: anti-malware; compliance; assessment; testing; test plan; MRG Effitas; 360 Degree Android Assessment

July 29 2022

Version 1.1

MRG Effitas Test Plan for Q3 2022 360 Android Assessment and Certification

Sponsored and Authored by: MRG Effitas (Lorand Lajsz)

AMTSO Standard Compliance Statement

This Test has been designed to comply with the Anti-Malware Testing Standards Organization, Inc. ("AMTSO") Testing Protocol Standard for the Testing of Anti-Malware Solutions, Version [1.3] (the "Standard"). This Test Plan has been prepared using the AMTSO Test Plan Template and Usage Directions, Version [2.3]. Effitas Ltd. is solely responsible for the content of this Test Plan.

Table of Contents

MRG Effitas 360 Android Assessment and Certification Test Plan – Q3'2022

1. Introduction

A first-of-its-kind test that covers all angles, our pioneering 360 Android Assessment and Certification Test targets the key threats faced by internet users. In each test case we employ the full spectrum of Early Life Malware.

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. Our Android test suite provides a comprehensive yet realistic test set for any Android AV on the market to make sure that its protection capabilities are sufficient for security conscious real-life users.

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

2. Scope

This Certification Programme is designed to serve as a reflection of product efficacy based on what we have previously termed "metrics that matter". 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. When conducting these tests, we try 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 attack and how such attacks could be prevented. Simulating normal user behaviour means that special attention is paid 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. Since on Android, AV apps, for the most part are considered 'just another app', meaning that their capabilities end on the point when they inform the user about any potential threat and point her to the uninstallation activity. We tested a group of internet security suites and complementary security applications. 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, keep user interaction focused and streamlined.

In our next execution of this Test Plan, 8 Test Subjects were considered. Specific Test Subject Vendors and Participants will be determined after the Public Test Notification has been issued.

Product name	Play Store URL
AVG Security & Virus Cleaner	https://play.google.com/store/apps/details?id=com.antivirus

Avira Security Antivirus & VPN	https://play.google.com/store/apps/details?id=com.avira.android
Bitdefender Mobile Security	https://play.google.com/store/apps/details?id=com.bitdefender.security
Comodo Mobile Security	https://play.google.com/store/apps/details?id=com.comodo.cisme.antivirus
ESET Mobile Security & Antivirus	https://play.google.com/store/apps/details?id=com.eset.ems2.gp
Norton 360: Mobile Security	https://play.google.com/store/apps/details?id=com.symantec.mobilesecurity
Malwarebytes Mobile Security	https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware
Zoner AntiVirus	https://play.google.com/store/apps/details?id=com.zoner.android.antivirus

3. Methodology and Strategy

Performing AV testing on Android platform has its own characteristics, with regards to the general Android platform philosophy.

AV capabilities

Note that on Android, a mere installation of a piece of malware does not necessarily mean unwanted consequences for the user, as it is the first launch that kicks in actual malicious code. Having started the sample, however, can have detrimental consequences from a security perspective. For instance, after the first launch, a piece of malware requesting SYSTEM_ALERT_WINDOW permission can continuously display a request screen to the user. In such cases, the user is unable to get rid of the application as they have no access to the launcher, the application drawer, or the Settings application to perform an uninstall. Therefore, a timely detection of a sample, displayed before the first launch, is critical from a user standpoint.

User Notification

When it comes to AV activity, vendors need to make a lot of engineering decisions, including how the user should be notified, should a successful threat detection occur. Basically, two basic methods are in use on the market.

1. The AV engine displays a 'threat detected' type of screen, meaning that any potential user activity is interrupted, and the user has to manually dismiss the screen. As for threat clear-up, the detected sample needs to be uninstalled manually, therefore the user is usually taken to the system GUI where the installed applications can be manually removed. Advantages of this approach include a prompt notification and action from a user's perspective, as it is impossible not to notice the threat.

2. The AV engine initiates a user notification sequence, resulting in a change in the OS

notification bar. This is a more subtle approach, providing a streamlined Android experience, however it also has a couple of drawbacks. For instance, on Android it is possible to re-prioritize app notifications, therefore it is possible for the user to manually snooze notification in advance. Furthermore, it is possible for the user to overlook any notification from the AV, which is especially critical in the first couple of seconds after an installation.

3.1. Test methodology

The second scenario involves actual installation of each sample, aiming to check the installation time protection of the AV products.

Detailed steps are as follows.

The scenario involves three phase: Downloading, Saving to storage, Installing

Preparations:

0. Disable Play Protect.
1. Install the AV trough play store and set it up as the application recommends enabling all features / protections.
2. If any, Fine tune the settings according to the AV recommendation such as enabling extra features like PUA detection or switching to deep scans.
3. Allow the default browser as a source for install unknown application.
4. Upgrade all application including AV applications to ensure the entirety of the device is up to date.
5. Update the virus definition.

APK file testing methodology:

1. Having the test device initialized an instance of a web browser is launched using an explicit intent to a browser application, visiting an URL with the malicious APK.
a. After 30 seconds wait time for detection to occur, if the download hasn't began the download button is touched.
b. After another 30 seconds wait time an open command initiated for the downloaded file.
2. An automated sequence is initiated to install the downloaded package.
a. Having the sample installed a 30 seconds detection time is given for AV to notify the user.
3. If detection occurs we use the AV UI to uninstall the sample, otherwise we use ADB to remove the application.

Evaluation from the Testing steps:

1. In the download phase (1a), the test is counted as DETECTED DURING DOWNLOAD
2. After the download has finished but the application install has not yet started (1b), counted as DETECTED BEFORE INSTALL
3. After the application install has finished (2a) counted as DETECTED AFTER INSTALL
4. No detection from the AV results in MISSED.
5. If the AV unable the remove te threat or unable navigate the user how to remove the threat resulted as a FAIL.

Monitoring / Evidences / Log:

1. Video recording is made from Preparation step 4. until the end of Testing step 3.
3. Main device log is saved from Testing step 1. until the end of Testing step 3.
2. Screen shot is made from:

a. Application up to dateness (Preparation step 4).
b. Definition up to dateness (Preparation step 5).
c. AV Detection, if non occure then after Testing step 2a.

3.2. False positive test methodology

The false positive scenario involves actual installation of each sample, aiming to check the installation time protection of the AV products.

Detailed steps are as follows.

1. Having initialised the test device, we install the AV application and initialise it (accept EULA, download the latest definition files etc.)
2. Using adb, we perform the following steps.
    a. An instance of a web browser is launched, visiting an URL with the APK.
    b. The package is downloaded, and an automated sequence is initiated to install the downloaded package. All warnings are dismissed, and all appearing dialogs are accepted.
    c. Following the installation, the AV is informed about the newly installed application, kicking in detection routines.
3. We give 30 seconds for the AV to finish all scanning activities.
4. We create a screen shot of the resulting screen. Should the AV display a warning or an alert, the test is counted as a MISS, no warning results in a PASS.
5. Using adb, we uninstall the sample and move on to test the next one.

4. Participation

AMTSO's goal with having Participants is that in exchange for cooperating (engaging with Testers and following disclosure requirements), Participants have additional rights to audit their configuration and provide commentary on Test results. There must be no additional cost to a Test Subject Vendor to be a Participant. If a Tester charges to participate in a Public Test or any related services, and a Test Subject Vendor chooses to not pay the fee, that Vendor must be able to choose to be a Participant and follow this AMTSO standard.
Opt-Out Policy : Vendors can opt out if Vendor can prove that the test system or the Product was misconfigured in a way which greatly changes the test results. E.g. important modules were unnecessarily turned off compared to default configuration, or during the test the system could never reach the cloud.

Conflict of Interest Disclosure : There is no known conflict of interest.

Funding : Funding of this project is achieved by vendors subscribing to participate in this project, this gives them more in-depth information on how their product(s) performed, and, if there are any issues discovered in the product during testing, our technical team provides all the data

necessary to help improve the product.

Part of the funding comes from directly licensing reports so they can be used for marketing purposes.

Vendors often silently enter testing, sometimes of their newly developed product or a product in BETA or Pre-Release phase.

Finally, part of our funding comes from third parties, they commission us to include certain product into testing, both public and private.

5. Environment

Test hardware and configuration details follow.

Physical Configuration : Testing takes place on Genymotion virtualized images, and in cases where the AV utilizes ARM native binaries, on physical Nexus devices.

Sample Relevance : For ITW tests, majority of the malicious URLs used in this test were compromised legitimate websites which served malware. The remaining samples come from our regular honeypots or, in case of ransomware and financial malware in particular, we used URLs from newly-discovered distribution sites.

Geographic Limitations : There are no geographic limitations in terms of samples.

Curation Process : Voluntary Participants are given equal opportunities to participate in such Curation and feedback processes for all their respective Test Subjects.

Malware delivered by URLs used in this test can be considered as Zero Day in the true meaning of that phrase. Testing was conducted as per the methodology detailed in Appendix 1.

Distribution of Test Data : We send all failed samples to all participants, along with detailed test logs.

6. Schedule

Start Date Range: The test commencement date is August 01, 2022.

Test Duration and Calculated End Date: The test is expected to require approximately fourteen weeks (without installation of products) and is forecast to conclude on November 07, 2022.

Milestones: Delivery milestones appear in the following chart.

MRG-Effitas 360 Degree Assessment and Certification Test Project Schedule Milestones

Index	Test Activity	Start Date Range	Dependencies
1	*Test Commencement*	*August 01, 2022*	
2	*Confirm Vendor Configuration Feedback*	*August 08, 2022*	
3	*Milestone 1 – Preliminary Results*	*October 17, 2022*	*(1), (2)*
4	*Milestone 2 – Test Report First Edition – End of Testing Period*	*October 24, 2022*	*(3)*
5	*Feedback and Dispute Resolution Time – Retests as Needed*	*November 01, 2022 - November 07, 2022*	*(4)*
6	*Milestone 3 – Issue Final Report – End Date for Test*	*November 15, 2022*	*(5)*

Communications: Whenever there are significant deviations from this schedule (more than 5 workdays), we will notify all affected vendors within 3 business days.

Risks and Risk Management : We could not identify any risks with the test.

7. Control Procedures

Connectivity Validation : Tests are conducted with all systems having internet access. All security applications are fully functional unregistered versions or versions registered anonymously with no connection to MRG Effitas. Each vendor can supply a utility or another in-product feature to validate proper cloud-connectivity functionality.

Logging : In the first initial email to the vendors, we will ask if they require any special logging during the test. We expect these methods and tools to be working, otherwise we cannot guarantee the result of these logs. For the most part, we rely on standard Android logging capabilities, i.e. logcat.

Updates : Each individual security application will be installed using default settings on each of the test systems defined in the Environment section of this Test Plans and then, where applicable, updated.

8. Dependencies

Participant Actions : As this test scope are consumer Test Subjects, we do not require any Vendor specific actions.

9. Scoring Process

In order to attain a quarterly MRG Effitas Android 360 Degree certification award, a security application must either protect the system with a combined score of 99% in the in-the-wild category.

10. Dispute Process

After the vendors receive the test results and the logs, Vendors can dispute individual test cases if they can prove that they do not agree with the result.

11. Attestations

I understand and agree that I am submitting this Test Plan, and the following Attestations, on behalf of the entity listed below, and I represent and warrant that I have authority to bind such entity to these Attestations. All references to “I” or “me” or similar language refer to such entity. I represent and warrant that the following Attestations are true, to the best of my knowledge and belief, and each of the following commitments will be upheld to the best of my ability.

1. I will provide public notification on the AMTSO website covering my obligation for notification of a Public Test, regardless of whether a potential Participant is in actual receipt of such notification prior to the Commencement Date of a Test. (Section 1, Section 4, Section 6)

2. All products included in this Test will be analysed fairly and equally. (Section 2, Section 3, Section 5)

3. I will disclose any anticipated or known imbalance or inequity in the Test design to all Participants in the Test. (Section 2, Section 3)

4. Although I may charge for participation in a Test, I will not charge any additional fees for a vendor to be a test subject under the Standards. (Section 4)

5. I will disclose any material conflicts of interest or other information that could materially impact the reliability of the Test. (Section 4)

6. I will disclose how the Test was funded. (Section 4)

I hereby affirm, to the best of my knowledge and belief that this Test Plan complies with the AMTSO Testing Standards, as of the date hereof.

Signature: /s/ Lorand Lajsz

Name: Lorand Lajsz

Test Lab: MRG Effitas

AMTSO Test ID: [AMTSO-LS1-TP056]