TESTING GROUND LABS

Android Malware Detection Test

Enterprise Product

2023 Apr

• • • Celebrating Technology Innovation

Table of Contents

Report version 1.0, published on 2023.05.25, initial version

Report version 1.1, published on 2023.06.09, second version

Chap.1 Background

Android is a mobile operating system developed by Google. It is based on a modified version of the Linux kernel and other open-source software, and is designed primarily for touchscreen mobile devices such as smartphones and tablets. In addition, Google has further developed Android TV for televisions, Android Auto for cars, and Wear OS for wrist watches, each with a specialized user interface. Variants of Android are also used on game consoles, digital cameras, PCs and other electronics. Android's smartphone share will hover with around 85% throughout the forecast. Volumes are expected to grow at a five-year compound annual growth rate (CAGR) of 1.7% with shipments approaching 1.36 billion in 2022. Android maintained its position as the leading mobile operating system worldwide in January 2022, controlling the mobile OS market with a close to 70 percent share. Google's Android and Apple's iOS jointly possess over 99 percent of the global market share. Overall this is a positive sign that consumers are seeing the benefits of moving to a slightly more premium device than they likely previously owned.

Aside from the clear advantages to build mobile devices on Android, the platform also introduces numerous security risks to the platform users. Among them the following malicious activities:

1. Send messages to "premium service" SMS numbers that cost extra money.
2. Send your personal information to unknown parties.
3. Turn your phone into a part of a botnet so others can execute commands remotely for nefarious purposes, such as spam, DDOS attack, and more.
4. Non-authorized persons may monitor your phone calls and text messages.
5. Open you to blackmail, if something embarrassing can be found and sent elsewhere.
6. Trick you into entering financial information, such as account number, birth date, and more.
7. Even stuff on your PC if you connect your PC to your smartphone.

Clearly, to protect user's system and the data from the listed threats and the others, Android-based security applications exist and their efficiency is to be evaluated regularly against the permanently evolving threats.

This test is designed to independently assess the efficiency of consumer security solutions for Android OS on detecting currently spread malicious mobile apps.

Chap.2 Test Process & Test Software

Detailed process is as follows:

1. Several Android based mobile devices are prepared and backup images are created then. Platform: Android 12 on XiaoMi 8.
2. 864 malware samples and 415 different clean android applications installers are collected, and delivered in a mixed set to the internal storage of mobile devices. The malware is collected from multiple sources (including China region-based ones), clean apps are taken from Google AppStore and other legitimate app stores.
3. Install selected security applications on the physical mobile devices in default configuration.
4. Update the security applications and their antivirus bases.
5. Run full scan of the collection by the security application. Malware detection and false positive rates are recorded.
6. Install each missed malicious sample and then run each application, detection (if happened) is recorded.
7. Installation process against clean apps is not executed.
8. Test date: April, 2023.

Vendor	*Software*	*Version*
Dr.Web	*Dr.Web Mobile Security Suite*	*12.9.0(2)*
ESET	*ESET Endpoint Security*	*3.5.8.0*
Kaspersky	*Kaspersky Endpoint Security*	*10.48.1.31*
Total Defense	*Total Defense Mobile Security*	*3.3.9*

- *Dr.Web Mobile Security Suite is included in Dr.Web Enterprise Security Suite*

Chap.3 Tested Result (The test results are shown on the following tab)

Vendor	Total Samples	Missed Samples	Detected Samples	Detection Rate	False Positive Counts	Total Score
ESET	864	0	864	100.00%	0	100.00
Kaspersky	864	0	864	100.00%	0	100.00
Total Defense	864	17	847	98.03%	0	98.03
Dr.Web	864	307	557	64.47%	0	64.47

- For each security solution, a Final Score is calculated once the full test is performed:
  Final Score = (Detection %) *100 - 0.2*FP
- Basing on the Final Score, the correspondent rating is grated to each participating security solution, in accordance with the tab below:

final score	monthly award
98.00 - 100.00	5-star rating
95.00 - 97.99	4-star rating
90.00 - 94.99	3-star rating

Chap.4 Test Summary & Monthly Award

- Monthly Award:

2023 April	Android Malware Detection Test from Testing Ground Labs
ESET Kaspersky Total Defense	**5 Star Monthly Award 2023 April** **Enterprise Product**

Chap.5 Compliance

This test was made in accordance with the requirements of the AMTSO Testing Protocol Standard v.1.3 https://www.amtso.org/standards/, and is confirmed by AMTSO as the compliant with the Standard.

Details about the test compliance are available on page: https://www.amtso.org/tests/testing-ground-labs-android-malware-detection-test-april-2023-enterprise/ .

Chap.6 Rights Statement

Unless otherwise stated, Testing Ground Labs (hereinafter referred to as "TG Labs"), owns the copyright of this report. Without prior written consent of TG Labs, no other unit or individual shall have the right to alter the contents of this report and use it for commercial purposes by any means (including but not limited to transmission, dissemination, reproduction, excerpt, etc.).

Unless otherwise stated, TG Labs shall be the rightful owner of the trademarks and service marks used in the report. Any action of infringing upon the legal rights of TG Labs is prohibited. TG Labs shall have the right to pursue the legal liability of the infringer in accordance with the law.

Chap.7 Disclaimer

Note that before using the report issued by Testing Ground Labs (hereinafter referred to as "TG Labs"), please carefully read and fully understand the terms and conditions of this disclaimer (hereinafter referred to as "Disclaimer"), including the clauses of exclusion or restriction of the liabilities of TG Labs and the limitations of the rights of users. If you have any objection to the terms and conditions of this Disclaimer, you have the right not to use this report, the act of using this report will be regarded as acceptance and the recognition of the terms and conditions of this Disclaimer, so by using this report, you agree to the following terms and conditions:

1. The report is provided by TG Labs, all the contents contained herein are for reference purposes only, and will not be regarded as the suggestion, invitation, or warranty for readers to choose, purchase or use the products mentioned herein. TG Labs will not guarantee the absolute accuracy and completeness of the contents of the report; you should not rely solely on this report, or substitute the viewpoints of the report for your independent judgment. If you have any queries, please consult the relevant departments of the State, and then choose, purchase or use products by your independent judgment.
2. The contents contained herein is the judgment made by TG Labs to the product characteristics as of the date the report was published. In the future, TG Labs will have the right to issue new reports which contain different contents or draw different conclusions, but TG Labs has no obligation or responsibility to update the original report or inform readers of the update of it. In this case, TG Labs will bear no responsibility for readers' loss for using the original report.

3. The report may contain links to other websites, which are provided solely for the readers' convenience. The contents of the linked websites are not any part of this report. Readers shall assume the risks and losses or bear the costs when visiting such websites. TG Labs will not guarantee the authenticity, completeness, accuracy, and legitimacy of the contents of such websites (including but not limited to advertising, products or other information). TG Labs does not accept any liability (direct or indirect) for readers' damages or losses arising from their clicking on or viewing such websites to obtain some information, products, or service.
4. TG Labs may have or will have a business relationship with the companies which produce the products mentioned in this report, but have no obligation to notify readers about it, it doesn't matter if there has already been, or there will be such business relationship in the future.
5. The act of readers' receiving this report is not regarded as the establishment of the business relationship between readers and TG Labs, so there is no customer relationship existing. TG Labs does not accept any legal liability as the readers' customer.
6. The products which are used to be tested as samples by TG Labs are bought through the official channels and legal means, so the report is proper for products bought through the same, not for products bought through unofficial channels and/or illegal means. Therefore, it's the users buying such products that will be responsible for any risk or loss arising there from. TG Labs will not have or accept any liability whatsoever for any such risk or loss.
7. Some trademarks, photos or patterns owned by units or individuals will probably be used in this report, if you think your legal right and interests are infringed, please contact TG Labs promptly, TG Labs will handle the matter as quickly as possible.

TG Labs reserves the rights to interpret, modify, and update the Disclaimer.

Attorney: Zhejiang CongDian Law Firm