PCSL

IT CONSULTING INSTITUTE

Android Malware Detection Test

手机安全软件病毒检测率测试

2016 Jun

• • • Celebrating Technology Innovation

报告目录

TABLE OF CONTENTS

Chap.1 Background

Android is an open-source platform founded in October 2003 by Andy Rubin and backed by Google, along with major hardware and software developers (such as Intel, HTC, ARM, Motorola and Samsung) that form the Open Handset Alliance. In October 2008, HTC released the HTC Dream, the first phone to use Android. The software suite included on the phone consists of integration with Google's proprietary applications, such as Maps, Calendar, and Gmail, and a full HTML web browser.

Android and iOS-powered devices have long dominated the smartphone market, and it's still clear that the two mobile operating systems show no sign of stopping anytime soon. New data has been released by Gartner, suggesting that Android holds 84.7 percent market share as of the third quarter of 2015, which is a 1.4-percent increase year over year. The research firm says Android's growth is thanks in part to strong global smartphone sales from Samsung and Huawei. These manufacturers make up 23.7 and 7.7 percent of all smartphones sold in Q3 2015, respectively.

Android security software can protect you from the following malware activities (all are actual cases):

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.

Chap.2 Test Process

Several android mobility devices will be prepared and backup images are created then.
Detailed process is as follows:

1. 2316 malware samples and bulks of clean android applications are prepared and delivered to the extended SD card.
2. Install a security product on the device.
3. Update the security product and perform a full scan against the malware set and clean applications. Malware detection rate and false positive status will be recorded. If full scan function is not provided, then perform one by one installation.
4. Restore the backup image and repeat the three steps above.

Vendor	Software	Version
AegisLab	AegisLab Antivirus Free	3.0.4 build r32444
AhnLab	AhnLab V3 Mobile Security	3.0.5.3(Build 1451)
Alibaba	Ali Money Shield	3.2.1
Antiy	AVL Pro	2.1.9
Ariasecure	Bornaria Mobile Security	1.5.79
Avast	Avast Mobile Security Free	5.2.0-9813-fc7c4dc
AVG	AVG Antivirus FREE for Android	5.3.0.2
Avira	Avira Antivirus Security Pro	4.5 build No.3926
Baidu	Baidu Mobile Security	8.2.0
Bitdefender	Bitdefender Antivirus Free	3.0.135
Bullguard	Bullguard Mobile Security	14.0.9.92
Cheetah	CM Security	2.10.4.3050
Dr.Web	Dr.Web anti-virus Light	9.01.2(0)
ESET	ESET Mobile Security & Antivirus Free	3.2.60.0-15
G DATA	G DATA Internet Security for Android	25.10.11.947bcb3c
IKARUS	IKARUS mobile.security Free	1.7.51
Kaspersky Lab	Kaspersky Internet Security for Android	11.10.4.1821
Lookout	Lookout FREE	9.42.3-33dce32
Malwarebytes	Malwarebytes Anti-Malware Mobile	2.0.5.3
McAfee	McAfee Mobile Security	V4.6.1.915
Panda	Panda Mobile Security	3.0.2
Qihoo	Qihoo Antivirus	V2.2.0.1001
Quick Heal	Quick Heal Mobile Security	2.01.057
Sophos	Sophos Mobile Security	6.1.1962(15)
Symantec	Norton Mobile Security Free	3.14.0.3072
Tencent	Tencent Mobile Manager	6.3.0 Build 3490
Trend Micro	Trend Micro Mobile Security	7.0.0.1443
Zemana	Zemana Mobile Security	1.1.4
Zoner	Zoner AntiVirus Free	1.11.1

Chap.3 Tested Software

Vendor	Total Samples	Missed Samples	Detected Samples	Detection Rate	False Positive Counts	Total Score
IKARUS	2316	0	2316	100.000%	0	100.000
Kaspersky Lab	2316	0	2316	100.000%	0	100.000
Quick Heal	2316	0	2316	100.000%	0	100.000
Symantec	2316	0	2316	100.000%	0	100.000
Tencent	2316	0	2316	100.000%	0	100.000
ESET	2316	1	2315	99.957%	0	99.957
AhnLab	2316	1	2315	99.957%	1	99.857
Bullguard	2316	0	2316	100.000%	2	99.800
Baidu	2316	5	2311	99.784%	0	99.784
Qihoo	2316	5	2311	99.784%	0	99.784
Sophos	2316	5	2311	99.784%	0	99.784
AVG	2316	3	2313	99.870%	1	99.770
Avira	2316	7	2309	99.698%	0	99.698
Alibaba	2316	10	2306	99.568%	0	99.568
Trend Micro	2316	7	2309	99.698%	3	99.398
Avast	2316	12	2304	99.482%	1	99.382
Antiy	2316	15	2301	99.352%	0	99.352
Bitdefender	2316	17	2299	99.266%	1	99.166
Malwarebytes	2316	21	2295	99.093%	0	99.093
Dr.Web	2316	46	2270	98.014%	0	98.014
Cheetah	2316	62	2254	97.323%	0	97.323
G DATA	2316	59	2257	97.453%	8	96.653
McAfee	2316	161	2155	93.048%	0	93.048
AegisLab	2316	148	2168	93.610%	6	93.010
Ariasecure	2316	149	2167	93.566%	6	92.966
Panda	2316	171	2145	92.617%	0	92.617
Zemana	2316	416	1900	82.038%	0	82.038
Zoner	2316	585	1731	74.741%	0	74.741

Chap.4 Test Result

Remarks: Final Score= (Detection %)*100-0.1*FP
6 different mobile security products from six renowned security vendors crashed during the original test, we have already delivered the crash log and related information to them.

Monthly Award

2016.06

IKARUS Kaspersky Quick Heal Symantec Tencent ESET AhnLab Bullguard Baidu Qihoo Sophos AVG Avira Alibaba Trend Micro Avast Antiy Bitdefender Malwarebytes Dr.Web	5 Star Monthly Award 2016 June
Cheetah G DATA	4 Star Monthly Award 2016 June
McAfee AegisLab Ariasecure Panda	3 Star Monthly Award 2016 June

Chap.5 Information

Jiaxing Chenxiang Information Technology Co., Ltd. (PCSL IT Consulting Institute) is an IT product test and consulting company located in Jiaxing, Zhejiang, P. R. China. As a professional tester of desktop security products and mobile security solutions, we are willing to provide references to the endpoint users for choosing security solutions and provide security vendors product improvement solutions and consulting services. Not only do we test security solutions for different environment, but we also provide test and consulting reports for other IT products, e.g. battery, mobile devices, computer power, etc.

In early 2015, we launched a brand new service named BOOM Feeds Data Collection and Analysis Service, which provided a variety of different digital threat data like, android applications collection, PE malware collection, phishing Urls, malicious Urls, Linux threat binaries, iOS binaries, attack records, and white binaries collections.

Chap.6 Rights Statement

Chap.7 Disclaimer

Note that before using the report issued by Jiaxing Chenxiang Information Technology Co. Ltd. (hereinafter referred to as "Chenxiang Information Technology"), 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 Chenxiang Information Technology 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 Chenxiang Information Technology, 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. Chenxiang Information Technology 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 Chenxiang Information Technology to the product characteristics as of the date the report was published. In the future, Chenxiang Information Technology will have the right to issue new reports which contain different contents or draw different conclusions, but Chenxiang Information Technology has no obligation or responsibility to update the original report or inform readers of the update of it. In this case, Chenxiang Information Technology 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. Chenxiang Information Technology 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). Chenxiang Information Technology 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. Chenxiang Information Technology 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 Chenxiang Information Technology, so there is no customer relationship existing. Chenxiang Information Technology does not accept any legal liability as the readers' customer.

6. The products which are used to be tested as samples by Chenxiang Information Technology 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. Chenxiang Information Technology 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 Chenxiang Information Technology promptly, Chenxiang Information Technology will handle the matter as quickly as possible.

Chenxiang Information Technology reserves the rights to interpret, modify, and update the Disclaimer.

Attorney: Zhejiang Nanhu Law Firm

📞 +86 573 8280 9089
🖨 +86 573 8280 8561
✉ info@pitci.com
🌐 www.pitci.com
🏠 Room 3304-3306, Building 3, NO.3339 Linggongtang Road, Jiaxing, Zhejiang, China, 314000

© 2008-2016 PCSL IT Consulting Institute