AV-Comparatives

移动安全软件测试

语言：简体中文

2015 年 2 月
最后修订：2015 年 3 月 30 日

www.av - comparatives.org

简介

本次测试的是运行谷歌安卓操作系统的智能手机和平板电脑使用的移动安全软件。报告中的产品全部来自那些领先的安全软件生产商，他们都同意参与本次测试。测试于 2015 年 2 月执行，使用的是运行安卓 4.4.4 版本的 LG Nexus 5 智能手机。

需要注意的是，今年夏天我们仍将继续执行公开的重要测试，届时将会对移动安全软件进行全面的评估和测试。本报告只提供恶意软件防护测试，以便于各厂商可以先行对自己的新产品进行检验，然后可以决定是否参加今年晚些时候执行的重要公开测试和评测。在测试开始前，各个参与测试的厂商都被要求决定是否要公布本次测试结果。因此，您在报告中看到的都是对自己产品的检测能力非常自信的厂商的检测结果；另外还有几个厂商未出现在报告中，因为已经决定测试结果仅自己内部使用。

说明

本报告仅提供各产品的恶意软件检测率。如果用户要看移动安全软件的综合评测结果，如产品的特色、提供的各种功能及用户界面等内容，可以参考我们 2014 年 9 月份的评测报告(http://www.av-comparatives.org/mobile-security)，要么只能等待新的评测报告发表了（大约今年 9 月份）。

目前还没有完美的移动安全产品。如同 Windows 产品一样，我们建议您读完报告后，将报告中的每款产品的优缺点列个简表。然后可以安装并试用几天每款产品的免费试用版，这样可以更轻松的决定最后用哪款产品。尤其是安卓安全软件，不断的有已经改善并增加功能的新版本发布。

移动安全软件的防恶意软件功能组件，能扫描移动设备上的可疑软件，并会删除或隔离这些可疑文件。要想让该功能正常发挥，就必须保持软件处于最新状态；还有一些产品扫描时要使用云扫描。当出国旅行时，用户需要谨慎使用自动更新和云扫描，避免产生来自移动服务提供商的高额的漫游费。安卓恶意软件防护测试的结果请见第 6 页。

测试的产品

参加今年二月份公开测试的产品如下。各厂商提供的产品都是可以从他们自己官网或几个第三方商店中下载的最新可用的版本，或者已确定在测试的时候（2015 年 2 月），谷歌商店中也已可用。

除了安管佳是从他们的官网[1]下载的以外，大部分被测的产品要么可以从谷歌商店下载，要么可以从几个大的中国第三方应用商店[2]下载。所测试的 Qihoo 360 的版本只能从他们的官网[3]下载。

- AhnLab V3 Mobile 2.1.2.17
- 安管佳 安全管家 5.0.0
- Antiy AVL for Android 2.3.10
- Avast Mobile Security 4.0.7875
- Avira Antivirus Security 3.9
- Bitdefender Mobile Security 2.36.716
- ESET Mobile Security 3.0.1249.0-0
- G Data Internet Security 25.7.1.3a605e88
- Kaspersky Internet Security 11.7.4.822
- Qihoo 360 AntiVirus 1.3.3.1025
- Quick Heal Total Security 2.01.020
- Trend Micro Mobile Security 6.0

[1] http://www.anguanjia.com/?c=Downsoft&id=6
[2] http://shouji.baidu.com/soft/item?docid=7514506
[3] http://edl.cloud.360safe.com/360Antivirus_1.3.3.1025_EN.apk

安卓智能手机感染病毒的风险究竟有多大?

这是个很难回答的问题，因为这也要取决于许多不同的因素。在西方国家，如果只使用开发厂商的官方商店，如Google Play，风险就要比许多亚洲国家低许多，特别是中国。有许多智能手机被ROOTED且使用的是非官方商店提供的应用程序，从而增加了安装危险应用的几率。在许多亚洲国家，智能手机被当做PC的替代品使用，且经常使用手机登陆网上银行。在欧洲和美国，银行应用也越来越普遍。使用同一部用于汇款的手机接收TAN码会有很高的风险。在西方国家，如果您坚持使用官方应用商店，并且未经过ROOT，那么相对来说风险就会较低。但是，我们必须指出的是，“低风险”并不意味“无风险”。此外，威胁的情况可能发生迅速和显著的变化。最好为此做好准备，并在智能手机上安装安全软件。而目前我们会说，如果手机丢失或被窃，防止失窃手机中的信息丢失比预防恶意软件更重要。

一些安全软件厂商可能会声称有几百万的安卓恶意样本；事实上，这些程序大多数近似于“可能不受欢迎”的应用，而不能称得上是恶意应用。此外，大多数真正的恶意软件含有以前用过的恶意代码，只是被新的或不同的应用重新进行了包装；此类应用可能只选择热门的应用商店，因此，短短的时间内就会给用户带来较高的威胁。

怎样做才能保护我的移动设备?

对移动设备攻击的方法越来越复杂。欺诈性应用程序试图窃取用户的信息或钱财。为了减少发生这种情况的风险，我们在此建议用户。只下载谷歌商店中的应用程序，或可信任的应用制造商自己的网上商店。避免使用第三方商店和sideloading[4]。不可信任的应用程序的另一种表现是需要无关的访问权限。例如，测量速度的一个应用程序，当您旅游时，已不再能访问您的电话簿或者通话记录。当然，即使某个应用程序做到了，它也没有明显的迹象表明，它就是恶意程序，但如果仔细的考虑一下这个程序是否是真正或应使用的程序，也不无道理。看看App Store中的评论也是一种帮助，尽量避免使用带有不良或可疑评论的应用。如果您ROOT您的智能手机，将实现手机的更多功能，但同样也为恶意程序的侵入提供了机会。还有一点要考虑的是保修条件。没有明确的法律条文规定，对于ROOTED的智能手机的保修是否仍然有效。在许多情况下，保修将被视为无效。

AV-Ccomparatives 安卓分析系统

基于这种情况，我们向您介绍一种新的恶意软件分析工具-AV-Comparatives 安卓分析系统，用户可以免费使用。它是一个静态的分析系统，用于检测可疑的安卓恶意软件、广告软件并提供统计信息。用户可以上传 apk 文件，然后用各种分析机制看到分析结果。

我们诚挚的邀请读者进行体验：http://www.av-comparatives.org/avc-analyzer/

[4] http://en.wikipedia.org/wiki/Sideloading

基本保护标准以谷歌安卓为基础

现成的谷歌安卓操作系统已含有基本的恶意软件防护功能。如果用户在手机中安装新软件，手机会要求 Google Safebrowsing API 来检查应用是否是恶意应用。我们的目的就是要通过测试来识别该项服务对所有恶意样本的检测率。几场测试过后，我们发现，即使我们总是用同样的恶意样本进行测试，但是测试结果仍然是多种多样。仔细研究后发现，Google Safebrowsing API[5]对请求数量是有限制的。谷歌并不提供绝对的请求数。API 使用文档显示“*为了确保 API 较高的可用性，谷歌限制客户端请求的频率。根据请求的类型而进行不同的处理。*”

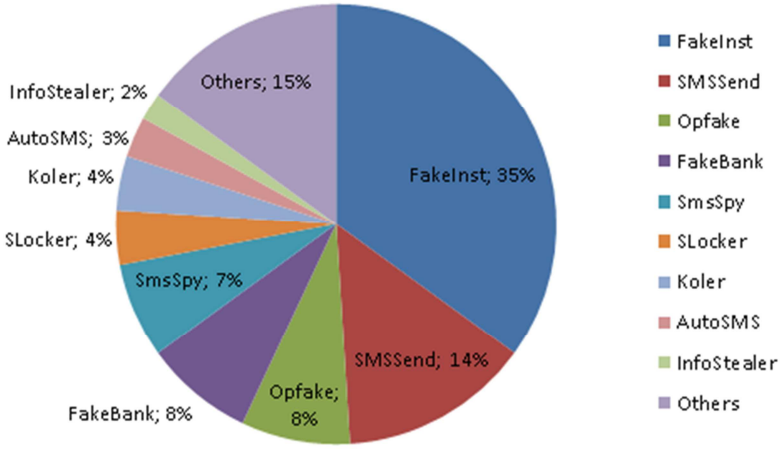
为了仔细验证我们的研究结果，我们建立了一个中间人（man-in-the-middle）攻击，然后分析在安装新的应用时的网络流量。用这个方法，我们可以确认之前测试的结果，因为谷歌 safebrowsing API 的响应是不同的，虽然我们总是安装相同的应用程序。如果在检测到的情况下，API 在屏幕上显示字符串内容，如“已被修改为包括可能有害的代码”和其他数据。如果漏掉了，屏幕上只会出现一个两个字节的回应（十六进制“08 00”）。

由于样本集比较大，我们不可能取得谷歌 safebrowsing 服务的任何一致的检测率。当请求谷歌安全团队将我们的设备加入限制的白名单时，我们收到的答复太晚了。

[5] https://developers.google.com/safe-browsing/developers_guide_v3#RequestFrequency

测试集

我们在测试开始前的几个月开始收集测试用的恶意样本。为了使测试集更具代表性，使用了 4,523 个恶意程序。测试集中删除了所谓的“可能不受欢迎的应用”。测试集中涵盖 125 个主要恶意软件家族（类型）。



2015 年 2 月 23 日对所有测试的安全产品进行了更新和测试。测试是在有有效互联网连接的真实的安卓智能手机（没有使用虚拟机）上进行的。测试集由专门的 APK 文件组成。首先进行的是按需扫描（on-demand）。之后，手工重新安装未检测到的应用。之所以这样做，是为了允许各安全软件使用实时保护功能来检测恶意应用。

检测率结果

	厂商名称	检测率[6]	产品
1.	Antiy	100.0%	Antiy AVL for Android 2.3
	Qihoo 360		Qihoo 360 AntiVirus 1.3
2.	AVIRA	99.9%	Avira Antivirus Security 3.9
	ESET		ESET Mobile Security 3.0
3.	Avast	99.8%	Avast Mobile Security 4.0
4.	AhnLab	99.7%	AhnLab V3 Mobile 2.1
5.	Bitdefender	99.6%	Bitdefender Mobile Security 2.36
	Kaspersky Lab		Kaspersky Internet Security 11.7
6.	Trend Micro	99.3%	Trend Micro Mobile Security 6.0
7.	Quick Heal	98.6%	Quick Heal Total Security 2.0
8.	G Data	96.1%	G Data Internet Security 25.7
9.	安管家	94.7%	安管家 安全管家 5.0

此外，我们还使用来自多个流行应用商店的前 200 个免费广告程序执行了误报测试。只有 Avast 在安装这些应用时，产生了一个误报，所有其他的程序都未产生误报。然而我们也注意到，所有的产品都容易产生误报和误认，尤其是对中国的应用和/或从知名的商店以外取得的应用。在亚洲，对于不受欢迎的应用的看法可能与欧洲或北美会有所不同。我们已经从测试样本集中删除了这类有争议的或可能引起争议的样本。

[6] 有的厂商同时提供几个不同版本的产品。本次测试结果不适用于其任何使用不同版本号，不同产品名称或不同语言的任何其他产品。

版权及免责声明

更多关于 AV - Comparatives 及测试方法，请访问我们的网站。

AV-Comparatives (2015 年 3 月)