



运营商恶意软件防护体系与关键技术研究^{*}

陈 涛¹, 高 鹏¹, 杜雪涛¹, 薛 珊¹, 杨满智²

(1. 中国移动通信集团设计院有限公司 北京 100080;

2. 恒安嘉新(北京)科技有限公司 北京 100191)

摘 要:近年来,运营商网络中恶意软件的数量急剧增加,严重威胁到移动互联网的安全。在综述现有恶意软件研判和防护技术的基础上,从运营商的角度,提出了网络侧与客户端联动的恶意软件防护体系,并研究了关键实施技术,为安全工程人员提供参考。

关键词:移动互联网安全;恶意软件;动态检测;静态检测

doi: 10.3969/j.issn.1000-0801.2014.01.013

Research on Operators Mobile Malware Protection Architecture and Key Technologies

Chen Tao¹, Gao Peng¹, Du Xuetao¹, Xue Shan¹, Yang Manzhi²

(1. China Mobile Group Design Institute Co., Ltd., Beijing 100080, China;

2. Eversec (Beijing) Technology Co., Ltd., Beijing 100191, China)

Abstract: In recent years, there is a rapid growth of malware on operators network. It severely threatens security of mobile internet. Based on reviewing of existing malware protection technologies, mobile malware protection architecture including both network side and terminal side technology and their interaction mechanism was proposed. Some key implementation technologies for engineer's reference were also studied.

Key words: mobile internet security, malware, dynamic detection, static detection

1 引言

截至 2012 年 12 月底,我国手机网民规模为 4.2 亿人。利用手机或 Pad 等移动终端作为上网设备,通过移动互联网下载游戏、获取天气或新闻服务、阅读电子书籍、参与社交活动逐渐成为人们的日常生活方式。移动互联网在给人们带来便捷生活的同时,安全问题也随之而来。据统计,移动互联网恶意程序由 2005 年的 52 个猛增到 2012 年的 162 981 个。移动恶意软件采用不知情订购方式消耗用户资费、窃取个人隐私(通讯录或位置信息)、实施远程监

控和钓鱼欺诈行为,极大地侵害了用户的切身利益。目前,90%以上的用户对手机缺乏安全感。移动互联网的安全状况不容乐观。

目前学术界与厂商的主要研究工作集中在恶意软件的识别与研判技术,希望借助手机安全软件检测并阻止智能终端上的恶意软件行为。但我国终端安全软件的普及率只有 54.6%,80%以上的用户表示对移动安全问题并没有特殊的关注。大量没有安全软件防护的用户暴露在恶意软件的直接威胁之下。

运营商在控制恶意软件的网络转播、样本采集、研判

^{*} 国家科技重大专项课题“LTE 覆盖增强组网技术”基金资助项目(No.2012ZX03001028)



和封堵方面具有强大的优势,研究运营商适用的恶意软件防治体系和关键技术对保障移动互联网安全具有重要意义。通过监控移动应用的下载源、下载渠道和终端运行环境,运营商能为用户提供更为安全的移动互联网通信环境。

2 相关研究工作

2007年,随着移动恶意软件的爆发式增长,国内外学者对新出现的移动恶意软件进行了跟踪研究,对恶意软件的行为特征、发展趋势、研判方法和识别系统进行了大量研究。

参考文献[1]指出,恶意软件多通过重新打包流行软件、升级恶意行为模块、恶意诱导用户下载等方式进行传播。恶意软件感染用户手机后,通常会进一步利用平台漏洞获取 root 权限,通过用户不知情的业务订购或上传用户隐私(通讯录、用户 IMEI 号码)等手段实施侵害,也可能与远程控制服务器联系获取进一步侵害指令。最近的研究表明,恶意软件越来越多地考虑经济因素,通过强行植入广告直接获取经济利益^[2]。

通常,移动恶意软件的检测研判方法可以按照静态检测和动态检测、人工检测和自动检测、基于特征规则的检测和基于统计数值的检测等方式进行分类。

静态检测主要包括两种方式:一种是基于签名的检测^[3,4],检测者事先需要建立黑白名单,包含安全程序和恶意程序的签名,比对需要检测的程序,就可以判定程序是否是恶意的,局限性是只能判断已知的恶意程序或识别出已知恶意程序的变体^[5];另一种是指利用逆向工程技术反编译移动程序,通过检测高危 Java API 调用、操作系统 API 调用、Java 原生代码或可装载模块的调用特征识别移动恶意代码^[6,7]。这种方法需要事先搜集恶意代码的识别特征,如程序是否调用 android.provider.telephony.sms.received 等短信发送 API,程序是否与 http://nkyt.net/bo 等已知的恶意 URL 有数据交互,是否截获来自“10086”客户号码的通知短信等,分析程序也可利用控制流或数据流等静态代码分析技术,检测是否存在没有用户输入的业务订购短信发送行为等,通过对上述代码特征的识别判定是否是移动恶意程序。因为反编译技术并不能完全恢复程序的所有原始信息,如数据类型信息、加密后的通信信息等,从而妨碍了恶意程序特征的提取,参考文献[8]试图利用数据类型推断等技术尽可能恢复源程序信息,但还是有一些恶意程序可

以通过高强度的加密措施逃避检测。此外,这种检测方法依赖于完善的恶意程序特征代码库。恶意行为识别特征目前主要来自研判人员的经验总结,人们将已知恶意行为归纳为研判规则,编码后对移动程序进行检测。参考文献[9~12]尝试利用机器学习、模式分类、人工免疫等方法自动提取恶意程序的研判特征,目前还处于研究阶段,区分恶意程序的模型和准确率还有待改进。

动态检测指将移动程序加载到模拟器或真机环境下,通过观察程序与 Android 平台、网络环境的交互行为判定是否是恶意程序^[13~15]。通常在移动程序运行时,利用这种检测技术对其系统调用和网络通信进行监控,一般利用日志记录技术和沙箱技术实现。但由于某些恶意程序可以主动探测运行环境、延迟激发恶意行为或通过加密方式传输数据,自动检测程序短时间内不能发现这类程序的异常行为,还需要采用代码注入等方式提高检测效率。代码注入指向目标程序文件中动态写入检测和提取敏感权限执行的代码逻辑,在不影响原程序执行的前提下动态监测程序运行过程中的敏感行为,从而提升研判效率。参考文献[16]介绍了人工检测常用工具,对于运营商来说,自动化的恶意代码检测系统更具有实际意义。参考文献[17,18]介绍了两个结合静态和动态检测技术的自动检测系统,但尚未在运营商网络中进行规模测试。

综上所述,目前学术界的大量研究工作集中在移动恶意程序的研判方法方面,还没有从运营商角度,对恶意软件防护体系结构进行系统研究,而运营商在恶意程序的发现、研判和封堵方面具有独特的优势。结合深度分组检测、日志留存、网络侧封堵和客户端技术的综合防护体系研究,对运营商保障移动互联网的安全具有重要意义。

3 运营商恶意软件防护体系

3.1 网络侧和客户端恶意软件防护技术

目前业界主流的恶意软件防护架构主要有客户端技术和网络侧技术两种。

客户端技术通过在移动终端上安装安全软件实现防护,这种防护模式需要通过应用商店或用户举报途径搜集恶意软件样本,识别出恶意软件的特征码或特征行为,再将恶意软件签名和防护规则下发到恶意软件客户端,实现对移动用户的实时保护。

网络侧技术主要通过监控网络流量分析识别出网络中传播的恶意软件,并通过流控系统、DNS 解析拦截技术

对恶意软件的传播进行封堵。从表 1 对网络侧和客户端侧防护技术的分析可以看出,客户端侧防护技术通过软件自动检测和用户举报获得的恶意代码样本的数量较大,但检测和上载样本会消耗大量手机计算资源和流量资源;网络侧检测不需要安装客户端安全软件,可以保护全网用户,且不消耗终端资源,但已经感染恶意软件的手机不能彻底清除恶意程序,用户手机仍然可以执行用户不知情业务订购、恶意扣费、上传隐私数据等行为,因此对用户的保护也是不全面的。两种防护技术各有优势和劣势,需要将两种技术进行有机地整合,为运营商网络提供综合防护能力。

3.2 网络侧与客户端联动的恶意软件防护体系

本文提出了一种网络侧与客户端联动的恶意软件防护体系,如图 1 所示。运营商在全网各省公司的 Gn 端口部署监控程序,对网络中传输的 Andriod、Symbian 等平台应用程序的下载、传输行为进行监控。在网络侧部署集中恶意软件管控平台,集成恶意软件样本搜集和研判、网络封堵和客户端服务的能力。同时,应通过手机预置或合作运营等方式,在用户终端上部署客户端安全软件,执行客户端恶意软件的防护策略部署、查杀、投诉和样本上传等功能。

运营商通过 Gn 口的网络流量监控、客户端用户举报

和应用商店的应用程序爬取获得软件样本,利用静态和动态检测技术进行研判,形成恶意软件黑名单和白名单签名数据库,包括恶意软件的标准名称、MD5 签名、主控 URL (域名、IP 地址)等信息。运营商通过集中管控系统在网关和 DNS 上实施对恶意程序的主控 URL、域名和 IP 地址的封堵和屏蔽,阻断恶意程序的下载传播渠道。

运营商恶意代码集中管控平台与内部 BOSS 和客户服务系统进行互联,通过分析用户上网日志、投诉信息、网络流量,获得恶意软件网络行为规则及全网恶意软件下载和主控 URL、恶意软件 MD5 签名,并将上述信息下发到客户端安全软件。客户端软件利用特征库对终端软件进行扫描,检测并删除用户手机上的恶意代码;也可以在用户访问恶意 URL 时,及时阻断下载行为。如果终端安全软件监控到驻留用户手机上的其他软件有恶意行为,将自动上报软件样本。

这种网络侧与客户端联动的恶意软件防护体系可以借助云检测等技术,将恶意代码的检测计算集中在网络侧完成,极大地减轻了对用户手机资源的消耗。此外,客户端安全软件作为独立于网络侧的恶意代码样本来源,扩充了恶意代码样本,能在网络侧封堵更多的恶意 URL,提升运

表 1 主流恶意软件防护技术对比

网络侧防护技术	客户端侧防护技术
优势 实现运营商网络的防护全覆盖, 保护没有安装客户端安全软件的用户; 防护功能不消耗终端资源	清除终端恶意软件, 消除恶意扣费和网络资源消耗等不良影响; 举报软件恶意行为, 对恶意软件进行个性化处理
劣势 不能彻底清除恶意软件, 终端恶意软件持续损害用户利益, 消耗终端资源; 恶意软件心跳连接等行为持续消耗运营商网络资源	终端安全软件杀毒功能对用户计算和电池资源消耗较大; 对没有安装安全软件的用户无防护能力

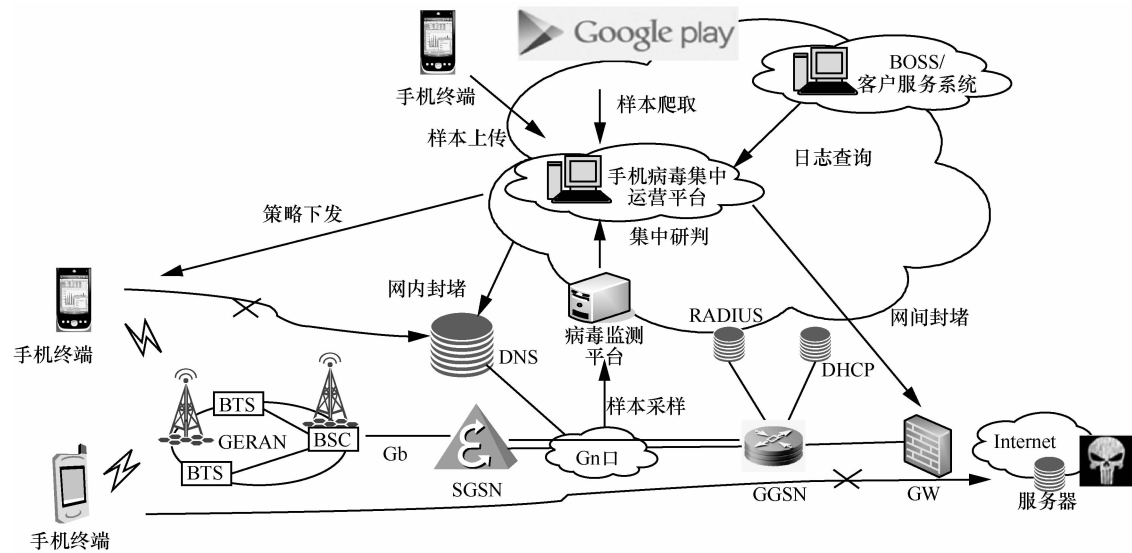


图 1 网络侧与客户端联动的恶意软件防护体系



营商全网的恶意代码封堵效率。网络侧恶意软件集中管控平台与运营商内部的客户服务系统和 BOSS 相连, 可以充分利用用户访问日志对恶意软件进行精准研判。

4 运营商恶意软件防护关键技术

4.1 恶意软件样本采集技术

运营商恶意软件防护系统能否准确识别并处置恶意软件, 与搜集并分析的恶意软件样本数量及行为特征有直接关系。在本文的防护体系中, 恶意软件样本的来源主要有 3 个渠道: 运营商网络采样、应用商店爬取和用户举报。

运营商可通过网络 Gn 口采样, 获取恶意程序样本。这种监控技术主要完成如下功能: 获取当前活跃的疑似恶意软件样本。监控系统对网络中传输的所有应用流量进行实时监控, 恢复利用 Web、彩信、邮件等渠道传播的应用程序样本, 上报黑名单和白名单之外的未知应用程序; 监控恶意软件传播事件。Gn 口采样检测系统可以针对常见恶意软件行为进行监控, 如某网络通信使用 HTTP, 并在请求中包含用户的 IMSI、IMEI、终端型号等信息; 传播同一个手机软件文件数量超过门限阈值/天; 网络数据分组包含异常特征字等。如果发现上述异常行为, 则对相关网络疑似安全事件进行上报, 协助运营商掌握网络中的恶意软件传播情况。

应用软件商店样本可以通过改造并集成现有爬虫工具 Scrapy 或 Lucene 进行爬取。用户举报指当用户发现可疑应用软件行为时, 借助客户端安全软件的举报功能或运营商客户服务体系, 报告恶意软件行为日志或主控 URL 地址。多通道恶意软件样本与日志采集技术架构如图 2 所示。

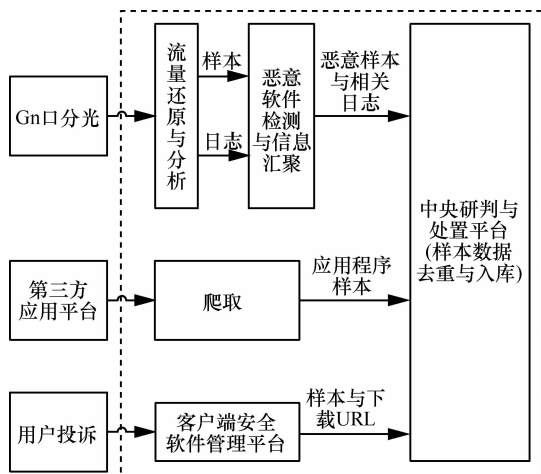


图 2 多通道恶意软件样本与日志采集技术架构

4.2 研判技术

运营商恶意软件防护系统整合动态和静态研判技术, 对采集到的应用软件样本进行研判。系统通过扫描应用程序的应用许可、系统 API 或监控程序短/彩信收发、连接远程 URL 等行为, 给出研判结果。运营商的研判优势在于可以结合网络日志, 查找用户手机是否访问过恶意软件下载 URL 或主控 URL、是否有泄露用户的 IMSI/IMEI/终端型号等关键字信息, 判断手机终端是否中毒, 并通过客户服务系统及时通知用户处置。

若疑似样本确定为新型手机恶意软件, 则提取特征码信息, 将其新增到全网已知手机恶意软件库。系统维护恶意软件下载 URL 和主控端 URL 库、恶意软件行为特征库和正常软件 MD5 签名库, 逐渐补充恶意软件识别特征, 提升恶意软件研判的准确率。一般系统应能自动识别网络中 99% 以上的恶意程序, 其他通过人工研判进行处置。

4.3 封堵技术

恶意软件的封堵指在运营商流控系统和 DNS 上阻止用户访问恶意软件下载 URL 和主控 URL, 从而对运营商网络实施保护。

运营商将恶意 URL 下发到流控系统前置机上形成封堵黑名单。通过 DPI 设备对网内及网间流量进行解析, 取得用户访问的 URL 或域名请求后, 如果命中黑名单, 则由前置服务器向用户发送 reset 报文或 DNS 重置页面报文, 由于正常网站返回结果或正常 DNS 解析结果返回较慢, 会被用户主机丢弃, 从而阻断恶意 URL 的访问^[9]。系统还需要将恶意软件 IP 地址黑名单下发到防火墙进行封堵。恶意软件的全网封堵架构如图 3 所示。

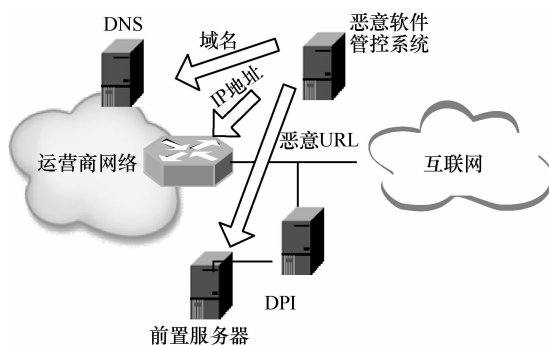


图 3 恶意软件的全网封堵架构

4.4 终端安全软件杀毒技术

运营商可以通过手机预置或厂商合作的方式在用户手机上安装终端安全软件。终端安全软件主要完成恶意软



序号	恶意软件名称	中文名称	事件数	恶意软件类型	影响系统	用户数
4	A.Payment.gamejng.d	伪游戏宝库病毒变种	4 706	恶意扣费	Android	2 794
5	S.Privacy.SystemSQL.a	伪系统数据库病毒	8 928	系统破坏	Symbian	2 623
6	A.Remote.aseiel.b	阿瑟下载木马变种	4 893	远程控制	Android	2 439
7	S.Rogue.GameOfLife.eb	伪“游戏使命”病毒变种	2 747	诱骗欺诈	Symbian	2 044
8	S.System.InstallGuideDY.b	伪安装向导病毒变种	84 744	系统破坏	Symbian	1 991
9	S.Expense.InstallGuide.b	伪安装向导家族病毒变种	84 702	资源消耗	Symbian	1 978
10	S.Privacy.sysdS.a1	伪精美手机主题家族病毒变种	11 172	隐私窃取	Symbian	1 748
11	S.System.mencache.a	伪无限手机主题病毒	11 182	系统破坏	Symbian	1 747
12	S.System.mencache.a1	伪无限手机主题家族病毒	11 170	系统破坏	Symbian	1 739
13	S.Privacy.AppStore.a1	伪应用程序商店家族病毒变种	11 166	隐私窃取	Symbian	1 737
14	S.Privacy.sysdS.a10	伪精美手机主题家族病毒变种	11 142	隐私窃取	Symbian	1 737
15	S.Privacy.AppStore.b	伪应用程序商店病毒变种	11 154	隐私窃取	Symbian	1 736

图7 高发病毒统计

营商带来了严重的威胁,运营商在恶意软件的采样、研判和封堵、查杀中具有很大的优势。本文从运营商的角度提出了网络侧与客户端联动的恶意软件防护体系,并研究了相关实施技术,对提高运营商全网防护水平有重要意义。

本文所述技术尚有如下不足需要进一步研究与完善:运营商网络中恶意软件研判的准确度还不高,未来需要借助机器学习、模式分类等方法提取恶意程序的研判特征,进一步提高研判的能力;虽然可以从三大渠道获得恶意软件样本,但由于目前 2G/3G 网络上网速度较慢,用户习惯于借助 PC 下载移动互联网应用,然后安装到手机上,本文所述监控技术尚不能覆盖这种场景。未来需要借助用户上网行为分析技术,发现通过这种途径传播的恶意软件。

随着 4G 网络的部署,网络传输速度的增加,需要加快病毒样本的研判速度,此外,由于恶意软件的时延激发特性,研判过程的耗时也越来越长,需要研究代码注入检测技术、改进沙箱技术和并发检测技术,缩短恶意软件的研判时间,适应大量恶意软件研判的需求。

参考文献

- Jiang X. Dissecting Android malware: characterization and evolution. Proceedings of 2012 IEEE Symp on Security and Privacy, San Francisco, California, 2012: 95~109
- Erturk E. Two trends in mobile malware: financial motives and transitioning from static to dynamic analysis. International Journal of Intelligent Computing Research (IJICR), 2012, 3(3/4): 325~329
- Venugopal D. An efficient signature representation and matching method for mobile devices. Proceedings of 2nd Annual International Workshop on Wireless Internet (WICON'06), Boston, MA, United States, 2006
- Zhou W, Zhou Y J. Detection of repackaged smartphone applications on Android. Proceedings of the Second ACM Conference on Data and Application Security and Privacy, San Antonio, USA, 2012: 317~326
- Zheng M. DroidAnalytics: a signature based analytic system to collect, extract, analyze and associate Android malware. <http://arxiv.org/abs/1302.7212>, 2013
- Elish K O. A static assurance analysis of Android applications. <http://people.cs.vt.edu/~danfeng/papers/user-intention-PA-2013.pdf>, 2013
- Grace M. RiskRanker: scalable and accurate zero-day Android malware detection. Proceedings of the 10th International Conference on Mobile Systems, Applications, and Services, Paphos, Cyprus, 2012: 281~294
- Enck W, Ocateau D, McDaniel P, *et al.* A study of Android application security. Proceedings of the 20th USENIX Security Symposium, USENIX Security'11, San Francisco, CA, 2011
- Zhao M. RobotDroid: a lightweight malware detection framework on smartphones. Journal of Networks, 2012, 7(4): 715~722
- Zhao M. A smartphone malware detection framework based on artificial immunology. Journal of Networks, 2013, 8(2): 469~476
- Shabtai A. Andromaly: a behavioral malware detection framework for android devices. Journal of Intelligent Information Systems, 2012, 38(1): 161~190
- Aung Z. Permission-based Android malware detection. National Journal of Science & Technology Research, 2013, 2(3)
- Burguera I. An Android application sandbox system for suspicious software detection. Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices, Berlin, Germany, 2011: 15~26
- Iland D. Detecting Android malware on network level. <http://www.ijcset.com/docs/IJCSET13-04-04-094.pdf>, 2011
- Park Y. An Android security extension to protect personal information against illegal accesses and privilege escalation attacks. Journal of Internet Services and Information Security (JISIS), 2012, 2(3/4): 29~42
- Beginners guide to Android reverse engineering. http://events.ccc.de/congress/2012/wiki/Beginners_Guide_to_Android_Reverse_Engineering, 2012
- Zhou Y, Wang Z, Zhou W, *et al.* Hey, you, get off my market: detecting malicious apps in alternative Android markets. Proceedings of the 16th Network and Distributed System Security Symposium, NDSS '12, San Diego, California, 2012

18 Su X. Smartphone dual defense protection framework: detecting malicious applications in Android markets. Proceedings of 8th International Conference on Mobile Ad Hoc and Sensor Networks, Chengdu, China, 2012

19 粟栗, 从健, 赵乐意. 涉黄域名二次中标问题研究. 电信工程技术与标准化, 2011(10): 11~14



杜雪涛,女,中国移动通信集团设计院有限公司高级工程师,主要研究方向为信息安全评估。

[作者简介]



陈涛,男,博士,中国移动通信集团设计院有限公司高级工程师,CCF 会员,主要研究方向为信息安全评估、下一代可信网络。



薛 姗,女,中国移动通信集团设计院有限公司助理工程师,主要研究方向为移动互联网安全。



高鹏,男,博士,中国移动通信集团设计院有限公司研究所教授级高级工程师、所长,主要研究方向为无线通信网安全。



杨满智,男,博士,恒安嘉新(北京)科技有限公司高级工程师、技术总监,主要研究方向为移动互联网安全。

(收稿日期:2013-07-04)



· 简 讯 ·

2013 年 11 月通信业主要指标完成情况(一)

指标名称	单位	本年本月止累计到达	比上年同期累计	本月
电信营业收入	亿元	12 316.5	12.3%	1 118.4
其中:电信主营业务收入	亿元	10 674.3	8.5%	961.0
电信固定资产投资完成额	亿元	2 643.0	-6.9%	335.2
固定本地电话通话时长合计	万分钟	27 747 979.0	-15.6%	2 397 634.5
区间电话通话时长	万分钟	2 915 430.5	-20.4%	252 890.0
区内电话及拨号上网通话时长	万分钟	24 832 548.5	-15.0%	2 144 744.6
固定长途电话通话时长合计	万分钟	5 408 529.5	-16.2%	480 420.0
国内长途电话通话时长	万分钟	5 284 104.3	-16.1%	470 420.6
国际电话通话时长	万分钟	75 966.4	-18.1%	6 146.9
港澳台电话通话时长	万分钟	48 458.7	-18.2%	3 852.5
移动电话通话时长合计(含本地)	万分钟	264 999 378.6	5.1%	24 142 561.9
移动电话国内长途通话时长	万分钟	61 428 748.5	5.8%	5 749 250.6
移动电话国际电话通话时长	万分钟	120 068.0	7.8%	11 207.8
移动电话港澳台电话通话时长	万分钟	88 771.6	-3.9%	7 942.1
移动短信业务量	万条	83 144 715.5	1.6%	6 210 319.6
移动互联网接入流量	万吉字节	118 643.7	70.6%	13 098.2

注:(1)收入增长率按可比口径计算。(2)固定长途电话通话时长和移动电话通话时长均包含相应的 IP 电话通话时长。(3)通话时长各项指标均为去话通话时长。

(来源:工业和信息化部运行监测协调局)