2009年10月27日 星期二 主编 王绍禹 编辑 荷光华 校对 广勒 版式 宋笑娟
郑州晚报

“每个人的手机都是一部窃听器，不管你开不开机，都能被窃听。”吴彦祖不久前在《窃听风云》中说出了这样一句令人胆战心惊的话。随着影片热映，“手机窃听”的问题被更多的人顾虑，网络商家也大肆推出各种窃听软件和设备，一场窃听和反窃听的斗争俨然从谍战片里来到了我们的现实生活中。我们的手机真的能变成窃听器吗？我们的秘密真的随时处于被窃听的危机中吗？记者经过一系列调查，发现手机窃听确实可以实现，但并不像影片中所说那么容易，而且并非没有预防和抵挡的办法。

“每部手机都是窃听器，不管你开不开机，都能被窃听”

“窃听风云”，照进现实？

如何搞窃听？

工具：GSM阻截器　现实：内部构造复杂成本很高

“其实，现在每个人身上都有偷听器，我们的GSM阻截器只要输入目标的手机号，就可以截听到对方的通话，哪怕对方没有开机，只要电池没有拆掉一样能听到。”影片《窃听风云》这样解释手机窃听的秘密，而网店热卖的各种窃听软件和器材中也确实有“GSM阻截器”。

所谓的GSM阻截器真有这么神奇吗？

记者在不少网络商家的店里看到这种“GSM阻截器”，称“利用GSM阻截器技术窃听别人通话信息。即通过在手机上安装GSM阻截器，只要知道对方电话号码，发出窃听程序信号，即使对方手机关机也会自动执行程序，将带手机者的谈话发射至监听装备”。一般服务费用在500元到800元，使用的时候一分钟按0.8元收费。

据记者向从事移动通信网络建设工作的工程师了解，这种技术的确是存在的，但是实际操作起来绝非那样简单。据介绍，这种手机窃听系统内部构造复杂、成本高昂，绝不是一般人能够买得起的，普通的电子市场上不可能有这类产品公开销售。所以网商卖的几百元的所谓“GSM阻截器”应该不会是真的。

方式一：复制SIM卡　现实：大多是修改来电显示的小把戏

记者从专家口中了解到，目前手机窃听的方式主要是硬件和软件两种。硬件方式中，最常见的方法是复制SIM卡。

北京邮电大学通信工程专家崔鹏指出：“利用SIM卡烧录器复制指定SIM卡，监打或者接听他人电话，这种方式由于容易被察觉，现在用的人很少，它一般不是为窃听，而是为了窃话费。而且，复制SIM卡必须要拿到被监听人的SIM卡，承诺不用拿到SIM卡就能直接复制的，是用改号软件进行诈骗的。”

记者通过和一些网商联系，发现复制SIM卡者大有人在，而且称只需提供目标手机号码即可，标价1800元到2000元不等，他们称“对方无论是拨打、接听电话，又或者是收发短信，你都可以同时听到、收到”。一些通信行业的专家认为，这其实是个彻头彻尾的骗局，是不法商家利用手机来电号码修改软件所做的文章。

“他们给你一张所谓复制了的SIM卡，然后让你用这张SIM卡拨打自己的手机号码，通过改号软件修改这张SIM卡的来电显示号码，在你的手机上显示出你想窃听的手机号，这就让你信以为真。等你付钱后发觉不对，他们早就逃之夭夭了，甚至他们之前跟你联系的手机号码都是使用改号软件修改过的，你肯定是找不到他们的。”说白了，这种所谓的SIM卡复制，只不过是“来电显示修改”的小把戏而已。

方式二：窃听软件　现实：专攻智能手机，不针对所有用户

其实，对普通百姓的手机隐私威胁较大的是手机窃听软件，也就是曾经流行一时的手机间谍软件。这类软件类似于电脑上的病毒程序，一旦被安装在手机里面，这些电子终端会自动记录反馈用户信息，甚至能被远程遥控来进行窃听。这意味着，只要是智能手机并能上网就有可能被安装。和电脑的“间谍软件”一样，它在后台隐身运行，手机菜单上不留丝毫痕迹。

“关机是没用的，手机即使关机，同样还是会跟无线基站进行信号联系，要不然我们拨打朋友的电话时，怎么会听到‘对方电话已关机’和‘对方电话正在通话中’这些不同的语音提示呢？”通信器材经销商王先生告诉记者，“其实也没有有些人说得那么神，通过彩信、蓝牙、红外就能安装，技术上不太可能。如果承诺在不拿到对方手机的情况下进行安装，多半是骗人的。”

据了解，手机窃听软件自从几年前问世，销售状况一直暗流汹涌，相当红火，以至于版本不断升级。王先生告诉记者，例如著名的“卧底”软件，普通版本可以监控手机的所有收发短信，也可以监听环境音；升级版本又增添了窃听通话内容的功能。不过，手机窃听软件需要安装才能被植入到手机之中，而且也主要针对的是智能手机，并不会对所有手机用户产生效果。

案例：送你新款智能手机，其实是个“密探”

通过调查，记者发现目前手机泄密的状况确实不容忽视，窃听软件不断推陈出新，越来越隐蔽，窃听效果和功能也在不断完善，而销售这些软件的商家已经形成网络，甚至成为一个潜在水面下的新产业。

记者在询问一个最新版本的“卧底”软件情况时，销售商为了增加他们的“诚信度”，告知记者：“我们在全国30多个城市已经有上百个代理了，销售量最小的一个月也能卖出20多个……”销售商可以发展自己的下线，据说一条线一个月在全国范围内就能卖出1000多个。

王先生告诉记者，据他所知，有些手机软件经销商甚至直接建议那些心怀鬼胎的客户“买个智能手机，装好软件，送给要窃听的对象”，这样“比较容易实现自己的目的”。因为一些昂贵的新款智能手机有很大一部分是用来作为礼物的，收到这样的礼物，等于在自己身边安插了一个“密探”。

这种事情并非耸人听闻，而是真实地发生着。王先生告诉记者，这种被动过手脚的“黑客手机”销路很不错，买的人相当一部分是用来送给“另一半”的，查找对方的偷情证据；还有是送给合作伙伴或搭档的，出于商业目的；甚至还有是老板作为奖品发给员工的，以监视手下的言行和动向。

窃听题材电影

《窃听风暴》：可能是影史上唯一将东德“斯塔西”情报工作曝光的电影，它非但精准传达出当时白色恐怖的氛围，更不忘在人性最艰困的时代中，保有温暖的曙光。

《生死谍变》：经典的谍战片当然缺乏不了极具创意的窃听手法，韩国电影《生死谍变》将一幕幕惊心动魄的间谍较量呈现在我们眼前，而冷战时代也是各种创新间谍技术辈出的年代。

《翻译风波》：本片中妮可·基德曼饰演的翻译员的窃听行为是无意而且偶然的，正所谓无心插柳柳成荫，阴差阳错的线路错误让她卷入一场政治暗杀阴谋。

《被窃听的隐私》：讲述了一个看似与普通人生活关联不大的故事，实则探讨了窃听技术的合理合法性，片中主人公为了捍卫自我的尊严与人权还使用了先进的窃听技术反制对方。

如何识别窃听？

一：话费暴增最可疑

由于窃听软件的泛滥，一些反窃听方式正在逐渐成为普通人的生活常识。

电话费突然暴涨是手机被窃听的一个明显线索。据专家分析，按照其操作原理，在手机被当做窃听器来使用时，实际上正处于通话状态，必须按照相应的资费标准缴纳通话费；在监控短信、通信簿等数据时则开启了GPRS无线上网，被盗取数据者也将因此背负上数据业务费。“一旦监控频率过高，窃听时间太长，话费肯定会出现不正常暴增。不过用户只要查询话费详单，窃听者的身份也就不难识破。”

二：手机易没电是信号

手机很容易没电也是一个危险信号，排除电池故障之后，就应该到手机维修部门排查一下手机是否被人放进了芯片式窃听器，因为芯片向外界传输的信号距离越远，所耗电量就越大，手机受到监听时间越长，电池也就越容易没电。

如何成功反窃听？

一：拆下电池最简单

最简单的反窃听方法，如《窃听风云》所说，谈私密话时，拔下手机电池就可以了。据说在一些公司的高层会议中，通常要求参加者拆下手机电池，也是出于反窃听目的。

二：聊天时玩手机游戏

和别人聊天时玩手机游戏的不礼貌行为倒是一个反窃听的好办法，因为在环境音被监听时，如果被窃听手机有任何操作，比如收发短信、拨打电话，或者玩游戏，监听会立刻中断。

三：不要把手机交给他人

同时，专家还建议，用户自己要小心，不要把手机的识别码等底层信息轻易告诉别人。手机也不要随便放置，而且不要把手机和SIM卡轻易交给他人。

【调查手记】　生活不是谍战剧，希望监管更到位

生活毕竟不是谍战剧，作为一个普通人，需要的是方便而安定的生活，一个需要用间谍和反间谍装备的社会是人人自危的，从网络、从手机，我们的秘密似乎被泄露殆尽。

《垃圾时代》的作者乔姆斯曾预言：“未来，间谍软件同病毒和垃圾邮件一样会长期存在。信息时代的道德约束在50年内似乎无法可循。”

道德约束似乎指靠不上，除了自我保护，人们更多是期望有关部门加强监管。据了解，对于生产销售间谍软件的行为，目前的办法只是报警，因为销售或使用这种具有间谍功能的软件，已经涉嫌违法。

本版均据《北京晚报》

地址：郑州市陇海西路80号　邮编450006　广告经营许可证：4101003000030　新闻监督电话：67655756　总编室　67655526　印刷：郑州日报社印刷厂　67655623　印刷厂地址：郑州市工人路30号
办公室67655506　采访中心　67655633　编辑中心67655757　文体中心　67655768　周刊中心　67655728　区域中心67655026　广告经营中心　67655668　传真　67655766　月价12元　全年144元