小心，你手机里有“食人鱼”

恶意代码“食人鱼恶意软件”藏手机里暗扣话费
超21万部手机用户感染恶意代码
一款恶意代码一年暗扣超5000万

如果您的手机话费莫名其妙地增加了，不知道您是否能够及时地发现。有些用户就遇到了比较奇怪的现象，手机通话频率并没有什么明显的变化，但是话费却增加了不少，是什么原因导致了手机话费莫名其妙地增加？

你的手机话费为何莫名大增？

河北省石家庄市的赵小姐发现自己没打多少电话，但是最近两个月手机话费却比以前增加了一倍。碰到这种怪事的绝不止赵小姐一个人，北京市的李先生也称，自己的手机没坏，刚充的100元话费不到3天就用完了，而且什么提示都收不到。

为了查清手机里的问题，赵小姐和李先生随后都找到北京一家手机安全公司寻求帮助。

专业技术人员对赵小姐和李先生的手机做了仔细检查后发现，他们手机里的应用软件中，都暗藏着一个极其隐蔽的小插件，而这个小插件，其实是一种手机恶意代码，它把应用软件变成别有用意的恶意软件，会偷偷扣除用户话费：“我们公司在2月6日已将这种含恶意(代码的)软件命名为‘食人鱼恶意软件’。”

恶意软件代替用户定制付费服务

北京邮电大学信息安全中心博士生导师徐国爱教授告诉记者，目前第三方软件应用商店、手机论坛等渠道对软件安全验证力度小，甚至根本就不进行安全验证，暗扣话费的一些恶意代码、病毒等软件插件，往往选择潜伏在市场知名度大、应用广泛的一些手机软件中，很容易蒙骗用户。不仅如此，藏有恶意代码的软件发起攻击时，会对运营商的业务短信号段进行屏蔽，也就是说，它会让手机用户根本看不到电信运营商要用户确认是否要定制付费增值服务的短信提示。

“运营商看来就是你这个手机在交易，实际上也是这个手机跟他们做交易，只不过用户自己没参与，那个恶意软件替代了用户参与这个事情。恶意软件隐藏在手机里用户不知道。”

如何清理恶意软件

“国家互联网应急中心共鉴定恶意程序445个，其中危害较大的有212个。”看到这样的数据，让许多使用智能手机的市民不免担心起来，自己的手机会不会也被恶意软件入侵了？

昨日，记者采访了我市专业经营智能手机的e酷手机连锁店的负责人魏振军。“遇到这种情况不必慌，平时我们在维修手机的时候也常遇到，类似的恶意软件很常见，也不少。”魏振军说，如果市民发现或者感觉自己的手机话费出现异常，最简单快捷的办法是刷机，“就像电脑中毒了，重装系统一样，一刷机就是一个全新的系统了，不过在刷机前一定要把自己的电话簿、照片等信息从手机中导出来保存好，因为刷机后这些东西都会没有了。”

那需不需要把手机拿到维修店里去检测呢？魏振军说，刷机非常简单，懂电脑的直接在网上就可以找到刷机的步骤，不懂电脑的找个正规的手机维修店就可以搞定。而检测一下不仅需要花钱，而且这样的恶意软件往往比较小，检测起来不仅麻烦还费钱，“不过为了避免手机再次被恶意软件入侵，建议大家下载软件的时候一定要到相应的官方网站进行下载”。

记者 李丽君

至少21万部手机感染恶意扣费软件

监测发现，截至3月10日，仅国内就有超过21万部手机感染了这种恶意扣费的软件。这意味着至少有21万部手机的用户，面临话费被暗扣的威胁。

据了解，这类扣费软件采取多次小额扣费的方式，每次只扣两块钱到5块钱，然后每隔一段时间重复扣费。如果用户不打出话费详单仔细核查的话，根本就不知道被暗扣话费了。

每年暗扣话费超过5000万元

调查数据表明，超过40%的手机恶意代码来自于手机应用(软件)商店和手机论坛，部分的手机应用商店里面含有恶意代码的应用软件超过了7%，也就是说，将近十分之一的手机应用软件被作了修改，里面夹杂着恶意代码。

手机安全专家向记者透露，这种暗扣用户话费的恶意代码会在不同的时间段，用不同SP电信增值业务提供商计费代码，暗扣用户话费。

一般一条SP业务定制短信的费用2块钱，由于运营商可以收到确认定制增值服务的短信，所以说，按照规定，运营商可以提取30%的费用(0.6元)，剩下70%的费用中，有10%由SP(计费)代码公司获得，也就是1毛4分钱，而剩下的90%，也就是一块两毛六，由(恶意)代码制作者获得。

记者从相关手机安全公司获悉的数据显示，截至今年3月10日，我国已经有超过21万部手机感染了暗扣用户话费的恶意代码。样本分析发现，每部感染暗扣恶意代码的手机，平均每个月至少被直接扣费20元，这就意味着，仅这一款暗扣话费的恶意代码，每年直接偷偷暗扣手机用户的话费就超过5000万元。

恶意代码如何进入手机

专业机构对这类含有暗扣用户话费恶意代码的软件样本进行研究分析后发现，目前，这类恶意代码的传播机制主要是通过嵌入正常手机应用软件的方式，来诱骗用户下载安装。赵小姐告诉记者，她手机里这款嵌入了恶意扣费代码的百吉历软件，是从一家手机软件应用商店里下载的。记者随后请专业技术人员随机从手机软件应用商店、手机网站论坛，下载了2个“百吉历”手机应用软件包，并用专业软件工具进行解析，结果发现，这些手机应用软件包，都隐藏有暗扣话费的恶意代码。

技术人员告诉记者，由于这款百吉历软件使用的是一个可供公共使用的签名，因此，从软件签名信息，无法查找到百吉历软件的真正作者。北京邮电大学网络信息安全中心研究发现，手机应用软件隐藏的恶意代码，有2%～3%的比例是应用软件作者自己所为，而大多数都是手机应用软件在软件应用商店、网站论坛上推广的时候，才被人做了手脚，嵌进了恶意代码。

手机安全专家在深入分析这款暗扣话费的“食人鱼”恶意代码时，发现在手机里潜伏的恶意代码，在用户毫不知情的情况下在后台偷偷联网后，会跳转到www.yangruiling.com、IP地址为61.191.55.43的一个网站。

然而，奇怪的是，当记者上网登录这个网站时，却显示为不可登录。手机安全专家用技术手段进行了长时间跟踪监测后发现，只有当恶意代码运行的时候，手机才会在后台去联网，而普通用户登录这个网址是无法打开的，这样做，即使有人发现了这个网址，但打不开也就不会再去调查它了。

记者调查发现，有大量的网站以及网络论坛等网上空间，都可以随意上传或下载手机应用软件。要想揪出制造传播恶意代码的元凶，极其不容易。

加大监管力度

受工业和信息化部通信保障局委托，国家互联网应急中心近期组织通信行业首次开展了移动互联网恶意程序专项治理行动。截至2月10日，国家互联网应急中心共鉴定恶意程序445个，其中危害较大的有212个。有关部门已经对其中与手机病毒关联的100多个控制端进行了有效处置，使这些控制端无法直接危害已经感染恶意代码等手机病毒的受控手机用户。

专家建议，要想有效地遏制手机恶意代码等病毒的传播，一方面需电信运营商加大重视程度、加大技术投入，而另一方面更需要有关监管部门加大监管力度，尤其是要加大惩处力度，提高手机话费恶意代码等手机病毒的制作者和传播者的违法成本，能够起到更加有效地惩戒和警示作用。只有这样才有可能遏制手机病毒的传播。

据央视《每周质量报告》

哪些游戏可能藏有恶意软件

最新监测数据表明，截至2012年3月10日，这类暗扣话费的恶意代码已利用过100多款安卓手机应用软件，潜伏在用户手机里。手机百吉历、功能计算器，以及贪吃蛇、扫雷、打地鼠、魔法棋、仙魔劫、象棋争霸、愤怒的小球等时下较为流行的手机游戏，是恶意代码最喜欢用来藏身的地方。