一名黑产设备卖家的QQ空间。

“准空姐”30秒收29条验证码短信

每每回忆起不久前一天下午的遭遇，小程总是眉头紧皱。“觉得隐私被泄露了，很害怕。”

那天，正打算去逛街的她刚刚走出校门没多远，一向安静的手机突然提示声音不断，来自各个APP的验证码短信接踵而来。

小程是一名“准空姐”。不久前，经过6次和竞争对手的角逐，她终于在南方航空的面试中脱颖而出，等待着培训的到来。“看到南航短信验证码的时候像木头人一样，十分害怕会对未来有影响。”除了网贷和一些支付平台的密码外，两条来自南

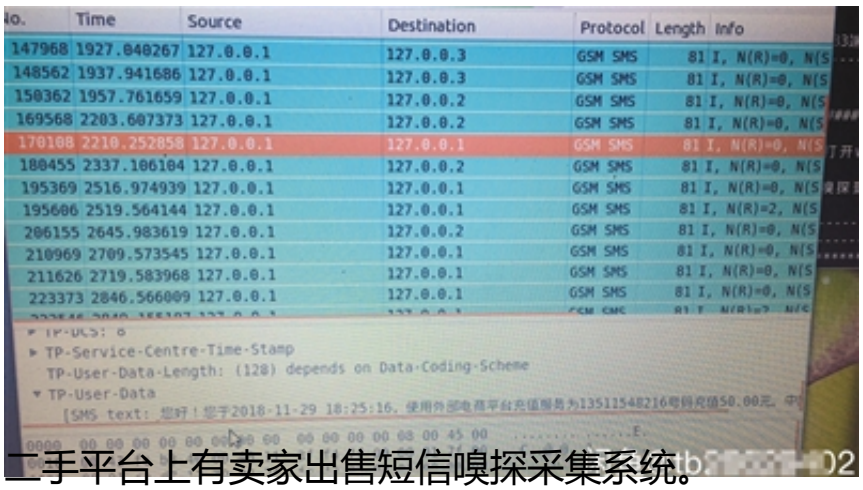
方航空的验证码让小程格外担心。对她而言，所有包含“南方航空”这四个字眼的信息都可以轻而易举触及她的未来。

“从来没碰到过这样的事情。”为了躲避这些突如其来的短信提示声，小程在愣了不到两秒钟之后，将手机调为了飞行模式。“因为我点开一个看了一下，每个验证码后面都写着有效时间，就本能地这么做了。”

事后，据统计，小程在不到30秒的时间里，共收到29条验证码短信。

小程不知道的是，她的这次特殊经历的背后，极有可能隐藏着一条盘踞已久的黑色产业链。有类似遭遇的，也并非只有她一个人。不过，其他人不是每个都像小程一样幸运。

“通过一种短信嗅探设备，可以直接嗅探到电信用户所有的手机短信。”意图“上岸”的老吕（化名）介绍。“上岸”是黑产从业者中的行话，为了规避风险，一些黑产从业者会在从事一段时间后“金盆洗手”。他表示，“黑产从业者有专门的手机号采集装备，利用采集到的手机号，可以在点卡网等实行找回密码等操作，实现盗刷。但是，这种设备只能攻击2G网络条件下的手机。配合降频设备，也可以强制让覆盖范围内手机网络状态变为2G，从而实现降频攻击。”



二手平台上有卖家出售短信嗅探采集系统。

售价1000元的嗅探技术其实只要30元？

新京报记者调查发现，短信嗅探设备易得、操作简便，实际上为黑产从业者设立了相当低的门槛。

“只需要一部摩托罗拉C118手机就可以实现短信嗅探。”一位业内人士告诉新京报记者，“在网上，可以很容易地买到。”

在某电商平台，记者通过搜索关键词“采集C118”后，出现12个名为“C118采集器系统软件全套”的商品。其中绝大多数商品封面或为嗅探成功的系统后台，或为已经改装好的摩托罗拉C118。新京报记者在一个系统后台的封面图片底部中注意到，“您好！您于2018-11-29 18:25:16.使用外部电商平台充值服务为135××××××××号码充值50.00元”这句话被用红线标注。“在线学习，包教会设备和系统，可以监测直径约500米范围的2G短信。”其中一名卖家告诉新京报记者，“全套设备和系统代码共1000元。”

新京报记者以买家身份和多名嗅探设备卖家取得联系。为了展示产品的真实性，几乎每个嗅探设备的卖家，都会主动给记者展示大量其设备正常运行的视频。在嗡鸣的风扇声中，他们将改装过的摩托罗拉C118与笔记本电脑连接妥当。登录系统后不久，实验手机接收到的短信内容便会出现在视频中泛黄的屏幕中。

然而，对于这项技术而言，其实“并不值1000元”。

“那些都是骗刚入行的小白的，这套设备的价格完全等价于硬件的价格，不会超过100元。”老吕告诉记者。据其介绍，硬件上，只需要购买一个不到30元钱的摩托罗拉C118手机，用几个常用电子元件改装便可；而软件上，将修改过的OsmocomBB编译进摩托罗拉C118手机里面，就可以为手机添加嗅探功能。

公开资料显示，OsmocomBB是从硬件层到应用层彻彻底底开源的GSM协议实现项目。因为是开源，黑产从业者可以轻而易举获得该代码，甚至不必大量去学习通信相关专业知识，就能实现并模拟GSM协议，按照自己的需求随意更改，添加功能。

据安全圈人士于小葵（化名）向新京报记者介绍，除了摩托罗拉C118，还有摩托罗拉、索尼爱立信的多个机型，均可被用于该技术。但是，摩托罗拉C118却成为众多黑产从业者的不二选择。“摩托罗拉C118兼容性最好，价格便宜，所以也就成为了最合适的手机。”于小葵说。

值得一提的是，部分平台短信验证码内容的不合理，实际上也间接提供了犯罪的温床。“其实，这个设备只能嗅探到2G短信内容，但并不能嗅探到手机号。”老吕坦言，“用户手机中很多短信内容都包含用户的手机号，用这个手机号登录一些充值平台，然后点击更改密码或者直接充值，就可以技术变现。”

在老吕看来，一些平台发送给用户的验证码中直接包括电话号码，实际上也为黑产从业者提供了一定的便利。“不过，也有专门的手机号码采集器可以采集到用户的手机号。”

只针对2G信号？从4G降为2G也要小心

去年9月17日，2018国家网络安全宣传周——网络安全博览会开幕，有展馆展出了多种网络黑灰产作案工具，其中便包括能够悄无声息偷走手机短信的“2G短信嗅探设备”。

据介绍，2G短信嗅探设备总材料价格不足100元，但可以做到获取周边任何人的短信内容，危害特别大。基站以广播方式转发到用户手里的加密短信，可被这套设备所截取并破解还原出来，最终被黑产用户实现信息窃取、资金盗刷和网络诈骗等犯罪。此前此类犯罪只针对移动与联通，不针对电信，同时这种犯罪只针对2G信号。

“但其实，手机在3G或4G时的特定情景下也有可能被监控到，原因是通过特殊设备压制或者信号质量不佳导致信号降频。”知道创宇404实验室副总监隋刚告诉新京报记者。

“2G本来就是开源的，在数据传输过程中也没有加密。”隋刚向新京报记者介绍说，在短信嗅探中，C118手机只是扮演着一个伪基站的角色。

伪基站又称“假基站”，可以利用移动信令监测系统监测移动通讯过程中的各种信令过程，获得手机用户当前的位置信息。按照通信协议世界的“游戏规则”，谁来先跟你“握手”，设备便会优先作出回应。伪基站启动后就会干扰和屏蔽一定范围内的运营商信号，之后则会搜索出附近的手机号，主动握手，并将短信发送到这些号码上。屏蔽运营商的信号可以持续10秒到20秒，短信推送完成后，对方手机才能重新搜索到信号。

给不法分子可乘之机的，却是2G网络的天然缺陷。“2G网络其架构本身就是开源的，其使用的GSM协议也都是明文传输。因为并没有加密，所以在传输的过程中就可以嗅探到。将C118连接至电脑，然后用类似Wireshark的网络抓包工具直接抓包，就可以抓出来通信过程中的所有指令。”隋刚说。

其实，听起来骇人听闻的GSM短信嗅探技术并非没有自己的软肋。据隋刚介绍，GSM短信嗅探技术的短板，主要有两方面，“一方面是摩托罗拉C118发射功率有限，黑产从业者只有在‘猎物’附近时才能实现嗅探，距离被严重限制；另一方面是这种方法获取的信息比较单一，只能获取短信验证码，所以只能做与短信验证码相关的事情。”

隋刚说：“我们能做的事情还有很多，比如说U盾等实体二步认证硬件就可以很好地防范这种攻击。”

全链条：获取身份证号、银行账号、支付账号

新京报记者进一步调查发现，GSM短信嗅探攻击已基本实现全链条化。在电信用户的短信验证码、手机号码被劫持的的基础上，黑产从业者可以通过社工库等方式获取身份证号码、银行账号、支付平台账号等敏感信息。

在一个名为“C118研究社嗅探学习群”的QQ群中，一则与查询个人信息相关的广告显示，“可查卡查证”。有媒体曾在报道中提及，记者花费700元就买到同事行踪，包括乘机、开房、上网吧等11项记录。在另一个名为“短信设备”的QQ群中，一名自称出售短信号码采集器的卖家表示，“通过号码采集器可以采集到一定范围的手机号码。”

在这个QQ群里，共聚集着377名黑产从业者。每天，如何“赚大钱”成为群内学习和讨论的焦点。

那么，黑产从业者是如何通过手机号来查到多种个人信息的呢？新京报记者发现，通过社工库并不难实现个人信息的查询。所谓社工库，即一个数据资料集合库，包含有大量被泄露的数据。通过这些数据，社工库的使用者可以轻易勾勒出一幅用户的网络画像。

有接近黑灰产的人士指出，随着国内监管愈发严格，社工库一般只供黑产团伙内部使用。并且，目前灰产从业者有向国外转移的趋势。在暗网上的某个交易市场中，新京报记者发现大量包含“个人信息查询”的交易帖。其中一则帖子中显示，可以查户籍信息、开房信息、婚姻、宽带。在该交易帖中，根据查询信息不同，价位也从0.014BTC-0.15BTC不等。交易信息一览中显示，该商品单价为1美元，用户可以通过调整购买数量来满足不同需求。在不可追踪的暗网交易市场中，该服务“颇有卖相”，截至4月28日，该商品显示已被购买1368次。

■ 分析

短信验证码安全吗？

愈演愈烈的黑产，引发人们对手机短信验证码本身是否足够安全的讨论。有关人士表示，现在手机验证码能做到的东西（转账、实名等）已经远远超出了它本身安全性的范围。

据《2018网络黑灰产治理研究报告》估算，2017年我国网络安全产业规模为450多亿元，而黑灰产已达近千亿元规模；全年因垃圾短信、诈骗信息、个人信息泄露等造成的经济损失估算达915亿元。而且电信诈骗案每年以20%至30%的速度在增

长。

另据阿里安全归零实验室统计，2017年4月至12月共监测到电信诈骗数十万起，案发资金损失过亿元，涉及受害人员数万人，电信诈骗案件居高不下，规模化不断升级。2018年，活跃的专业技术黑灰产平台多达数百个。

那么，面对规模如此庞大的黑灰产，短信验证码是否已经显得捉襟见肘了呢？对此，隋刚认为，虽然在嗅探的情景下，短信验证码并不安全，但是就目前来说，短信验证码仍是一个切实可行的方案。

“就目前情况来看，如果将短信验证码换成其他的验证方式，无形之中肯定会加大使用成本。”隋刚告诉新京报记者，“安全是相对的，就看愿意付出多大的代价。与便捷性相平衡，短信验证码相对合适。安全本身就是提升攻防双方的成本，并没有绝对的安全。”

如何防范短信嗅探？

那么如何防止被黑产截获短信呢？2018年2月，全国信息安全标准化技术委员会秘书处发布《网络安全实践指南——应对截获短信验证码实施网络身份假冒攻击的技术指引》。

该指引指出，攻击者在截获短信验证码后，能够假冒受害者身份，成功通过移动应用、网站服务提供商的身份验证安全机制，实施信用卡盗刷等网络犯罪，给用户带来经济损失。指引同时指出，缺陷修复难度大。目前，GSM网络使用单向鉴权技术，且短信内容以明文形式传输，该缺陷由GSM设计造成，且GSM网络覆盖范围广，因此修复难度大、成本高。攻击过程中，受害者的手机信号被劫持，攻击者假冒受害者身份接入通信网络，受害者一般难以觉察。

那么，面对GMS短信嗅探的威胁，我们是否真的束手无策呢？有专家建议，用户可以要求运营商开通VoLTE功能（一种数据传输技术），从而防范短信被劫持的可能。“也就是说，不再使用2G网络传输短信，而是让短信通过4G网络传输，从而防范无线监控窃取短信。”也有专家认为，运营商应尽快替换掉2G网络。通信运营商应考虑加快淘汰2G网络技术，以更大程度确保信息安全。据介绍，在国际上，2G网络已被诸多运营商所抛弃。

上述指引也建议各移动应用、网站服务提供商优化用户身份验证措施，选用一种或采用多种方式组合，加强安全性：如短信上行验证（提供由用户主动发送短信用以验证身份的功能）、语音通话传输验证码、常用设备绑定、生物特征识别、动态选择身份验证方式等。

(来源:新京报)