来源:科技日报

图集

近日，河北省唐山市警方捣毁了一个使用“短信嗅探器”流窜作案的电信诈骗团伙。据嫌疑人交待，他们是趁受害人夜间熟睡时，使用“短信嗅探设备”，截取用户手机短信内容。随后，利用各银行、移动支付平台等存在的漏洞，窃取个人账户信息，并通过截取短信验证码，盗刷受害人资金。

据了解，近年来通过这一手段实施诈骗的案例不在少数。

那么，“短信嗅探”是如何在受害人毫无知觉的情况下发生的？应当如何消除手机被“嗅探”的风险？对此，记者采访了业内专家，扒一扒“短信嗅探器”的真面目。

利用“短信嗅探” 无需接触手机即可拦截短信

想明白“短信嗅探”的原理，需要先了解短信传输的过程。北京理工大学计算机网络及对抗技术研究所所长闫怀志介绍，短信是一种电信服务业务，可分为点对点短信和小区广播短信两种类型。其中，点对点短信传输是利用信令和信道来进行简短信息的传送，可在手机之间或从电脑端向手机发送信息。

“当别人给你发短信时，该短信作为小型数据包，会先通过短信业务中心发送至你手机信号所在范围内的基站，再由基站将该短信发送至你的手机。由此可知，基站在短信传输中发挥着至关重要的作用。”闫怀志介绍。

“短信嗅探”是一个怎样的过程？闫怀志解释说，“短信嗅探”其实是通过伪基站等特殊设备，对特定信号范围内的手机号码和数据信息进行采集和拦截，该过程并不会对手机产生物理接触。

不法分子可以在伪基站范围内获取到用户收到的所有短信，而用户却毫无知觉。

360未来安全研究院相关专家表示，不法分子一般会用一部改装手机连接笔记本电脑作为伪基站，其功率在几十瓦左右，覆盖范围在500米到三四千米。这种设备启动后，能够伪装成2G基站发送信号，干扰和屏蔽在其覆盖范围内的用户手机的4G信号，“嗅探”扫描周围的手机用户，将附近的手机“吸附”到这台设备上。

由于2G网络存在单向鉴权的漏洞，只有网络对用户手机的鉴权认证，用户手机无法识别出基站真伪，只能进行回应，这样伪基站就可以获得用户手机的IMSI（国际移

动用户识别码，在所有蜂窝网络中均具有唯一性），可以向其发送短信并拦截收到的短信。

其后，不法分子就会通过窃取到的短信内容获取目标手机的短信验证信息，然后通过登录其他一些网站进行“撞库”（即多个数据库之间碰撞），试图将机主的身份信息匹配出来，包括身份证、银行卡号、手机号、验证码等，继而在一些小众的便捷支付平台开通账号并绑定事主银行卡，冒充事主消费或套现，从而盗取事主银行卡资金。

2G网络便于犯罪 不法分子改装伪基站强制手机降网

据了解，“短信嗅探“技术大多数是在2G网络下实现，据360未来安全研究院相关专家介绍，原因是在4G网络中已经实现了双向鉴权，手机用户也可以对网络进行鉴权，这样伪基站就很容易被识别而难以“欺骗”用户的手机。但随着5G时代的到来，犯罪分子又是如何利用2G网络来实施犯罪的呢？

闫怀志表示，2G网络之所以会被用来犯罪，是因为2G通道下的短信内容是无加密传输的，攻击者很容易劫持并迅速解析。3G之后，数据的通信安全性大大增强，显著提升了攻击者破解短信内容的难度。因此，不法分子会通过“强制降网“的方式来强迫用户手机从4G、5G被动转向使用2G网络。

“具体的做法就是通过特殊电磁设备实现通信信号干扰、压制或令信号质量不佳，无法实现4G、5G等高质量通信，转而启动最基本的2G通信模式，从而实现通信信号降频和强制降网。这个过程本身从技术上实现并不复杂，因此攻击者经常使用。”闫怀志称。

此类犯罪中,摩托罗拉C118型号手机反复被提及，它又是为什么被不法分子选中呢？记者了解到，这款手机是2006年上市的2G手机，仅有短信和通话等基础功能，目前的价格十分便宜，网络售价还不到30元。据360未来安全研究院相关专家介绍，这款手机具有较高的兼容性，在软件上易于改装，经过简单的电路改造与配置,再与电脑连接妥当，便可实现短信拦截。

闫怀志认为，实施“短信嗅探”不法行为的核心和前提是拥有非法的“短信嗅探”装置，而实现这种装置的重要技术手段之一就是2G手机改造，因为手机具有收发天线和处理电路，自身就是较为完善的通信节点，技术上天然具有改造成为伪基站等“嗅探设备”的可能。

已成黑色产业链 专家支招保护自身财产安全

此前有媒体报道，在河南郑州、新乡等地多个小区的居民半夜同时遭遇了“短信嗅探”，这些居民绑定手机支付平台的银行卡一夜之间被刷爆，受害用户的覆盖范围达到了方圆3公里。

据了解，线上兜售“嗅探设备”、线下交易、远程指导犯罪，已经成为了一条黑色利益链。更可怕的是，购买“嗅探设备”，非法卖家还会赠送通过各种非法渠道搜集来的个人信息材料。还有一种更高级的个人信息，就是银行卡号、开户行，甚至还包括银行卡密码。

那么，“短信嗅探”真的防不胜防吗？

闫怀志认为，首先运营商应当提供高质量的4G/5G通信网络，最大限度减少手机主动降网的需求及可能性，这有助于规避短信被劫持的风险。另外，从用户角度来说，发现手机短信验证码发送频繁或来路不明可采取关机、启动飞行模式、移动位置等应对措施；发现手机突然变回2G，应提高警惕。

同时，360未来安全研究院相关专家建议，用户可以向运营商申请开通VoLTE功能，使数据和通话都只能在4G网络传输，而不会在通话过程中回落到2G；如果用户手机支持，也可以在网络设置中，将手机网络模式选为“LTE only”，即只支持4G网络。

“对于大额资金的个人银行账户，建议不开通短信验证转账功能，而小额资金账户短信验证码支付功能应设置每日、每笔支付限额；在应用App和网址支付时增加用户身份验证措施，选择多种支付方式组合的形式，尽可能增加安全性。”360未来安全研究院相关专家补充说。（记者 张 蕴）

责任编辑： 薛涛