安全小课堂六十一期【如何对抗伪基站】

京东安全应急响应中心 2017-06-16

“伪基站”即假基站，设备一般由主机和笔记本电脑组成，通过短信群发器、短信发信机等相关设备能够搜取以其为中心、一定半径范围内的手机卡信息，通过伪装成运营商的基站，冒用他人手机号码强行向用户手机发送诈骗、广告推销等短信息,JSRC **安全小课堂第六十一期**，邀请两位老师分享如何对抗伪基站，本期小课堂邀请到了ggggwwww、仙果老师进行分享,同时感谢JSRC白帽子们的精彩讨论。

伪基站的危害有哪些?

京安小妹

1.窃取你网络交易中的短信验证码。
2.可以模拟你的号码给你的家人打电话或者拨打高额付费长途电话。
3.可以模拟银行或110的电话号码给你打电话，进行诈骗。
4.可以劫持你的网络流量。
5.可以给你发垃圾短信。
6.推送“钓鱼短信”，可以用户诱骗安装手机木马。
7.伪基站每年诈骗100个亿。

讲师： ggggwwww、仙果

简述伪基站的原理?

京安小妹

1. 2G的网络鉴权过程为单向鉴权，终端不对网络进行鉴权，使得手机用户无法判断基站的合法性。
2. 软件无线电设备及配套软件的出现，使得犯罪分子可以简单地伪造基站的频率及信令，设备的小型化及便携性的提升使得犯罪分子可以把一个伪基站装到一个背包里，流动进行作案。

这个的工作原理就有点像有人伪造你们家的路由器wifi名称，而且wifi信号比你们家里的路由器还强，你的电脑或手机就自动连接上这个伪造的wifi路由器上。你的所有的网络通信可能都被窃取或伪造。而且犯罪成本比较低，几千块钱就可以购买到这样的设备，操作简单，携带方便。

讲师： ggggwwww、仙果

作为普通人有哪些可行的方式防范伪基站?

京安小妹

1. 提高安全意思，不要点击不明来源的短信链接及盲目根据来电电话号码，就相信对方的的合法性。
2. 我们可以购买4G网络的手机，4G网络已经很好解决了手机不对网络进行鉴权的问题。另外在我们的手机的网络模式里，设置->首选网络，应该设置为4G/3G/2G.这样的网络登录顺序。
3. 有些手机自带了识别伪基站的功能模块。如华为，360等。
4. 有些手机app带了识别伪基站的功能（如腾讯手机管家，百度手机卫士，360手机安全安全卫士等)。
5.不要轻易相信陌生人发送的信息。

讲师： ggggwwww、仙果

白帽子提问:网络电话跟伪基站的区别是什么

网络电话主要是语音，伪基站主要是短信。诈骗的信息载体不一样。
网络电话是利用的运营商的缺陷,不是移动基站的方式 ,伪基站的根本目的是 伪造一个合法的移动基站，

讲师： ggggwwww、仙果

据说现在有些大企业有搭建伪基站监控系统帮助打击犯罪，两位老师能否简述监控伪基站的原理，以及效果?

京安小妹

1. App侧，由于合法基站的位置及基站编号基本是固定的，app通过获取手机当前网络的LAC值及手机位置与云端的位置及LAC编号进行比对，判断是否是伪基站。
2. 手机底层通过根据伪基站与普通基站显著不同的特征，即位置区LAC值、发射功率、C1/C2小区选择和重选参数等显著不同，可以在手机通信底层识别所在基站是否为伪基站。
3. 定点监控。在重要场所布控 伪基站监控终端，通过终端采集所在地的伪基站的网络信息，通过和后台服务器进行比对，判断是否是伪基站。
4. 无线管理局用专门的设备定期在某个地点进行监控，发现一起，查办一起。
5. 警方实时侦查伪基站通常靠的是无线车测向车，通过监测伪基站释放的信号确定大体方向，然后进行追踪。这是政府层面的监控

大唐电信，华为，百度，360等公司都有相关的产品，这些措施都可以很好的解决伪基站的问题，另外4g手机及基站的普及，也解决了相关的安全问题

讲师： ggggwwww、仙果

本期JSRC 安全小课堂到此结束。更多内容请期待下期安全小课堂如果还有你希望出现在安全小课堂内容暂时未出现，也欢迎留言告诉我们。

安全小课堂的往期内容开通了自助查询，回复“安全小课堂”或者点击阅读原文进行查看。

简历请发送：cv-security@jd.com

微信公众号：jsrc_team

新浪官方微博：京东安全应急响应中心

阅读原文