

面对一条短信，



怎么破？！

短信有着辉煌过去



- 1、基于传统信令协议，端到端或端到网发送，不受对方开机状态影响；
- 2、最方便、最重要的无线数据接入方式；
- 3、内容长度70个字；
- 4、可提供新闻、天气、商业、娱乐、电视、文化、租赁、股票等信息服务；
- 5、收费简单，1毛一条；

2002年短信的出现更是给全球低迷的经济注入了一针强心剂

短信有着辉煌过去



某运营商全球的SP数目曾达700家，本地SP数量超过了2000家，短信中心有277个

好端端的短信被玩坏了.....

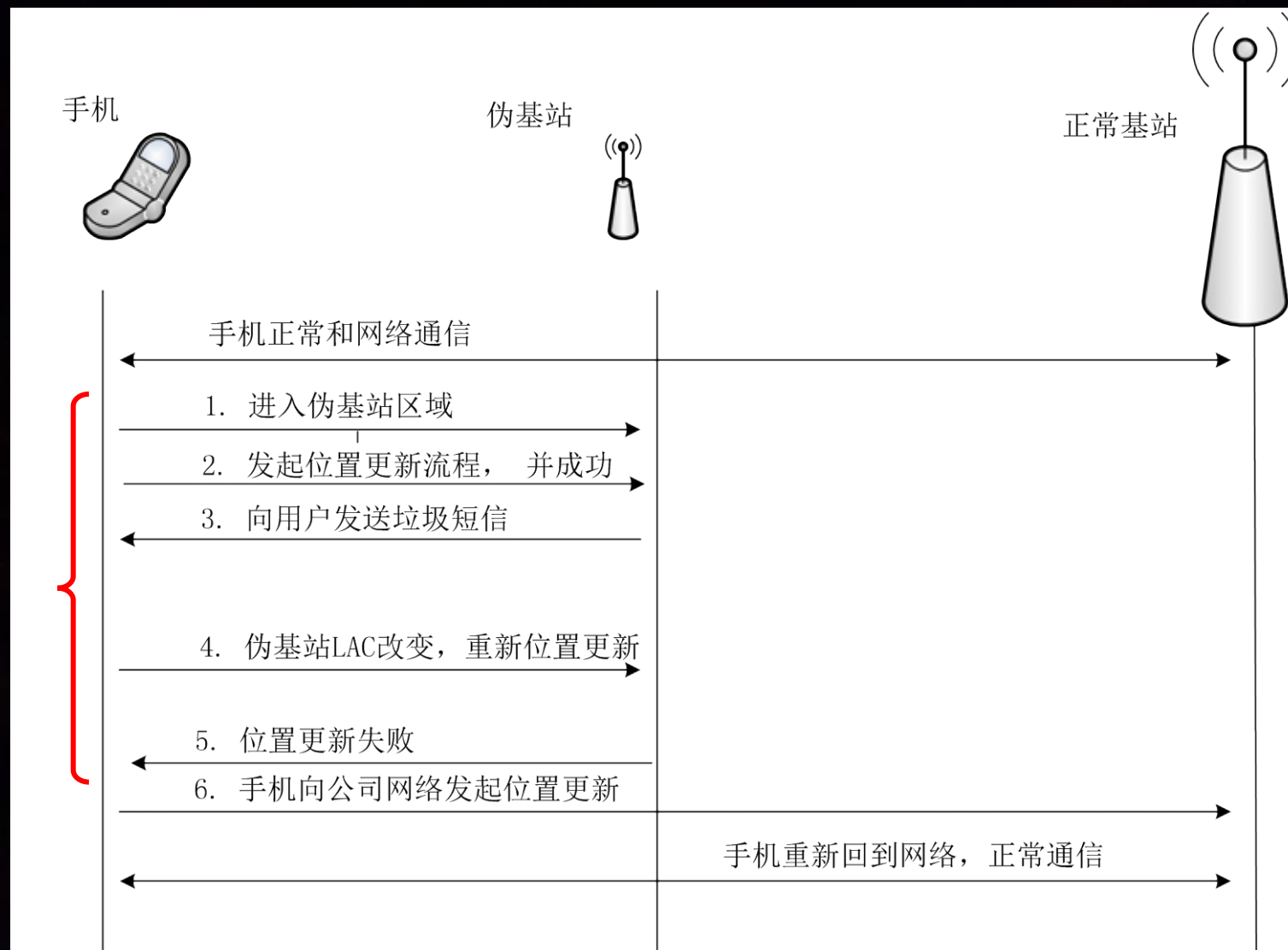


- 看似官方号码发送的
- 内容具有获利诱惑性
- 获利成本看似很便利

好端端的短信被玩坏了.....



伪基站是怎么搞破坏的



伪基站是怎么活动的

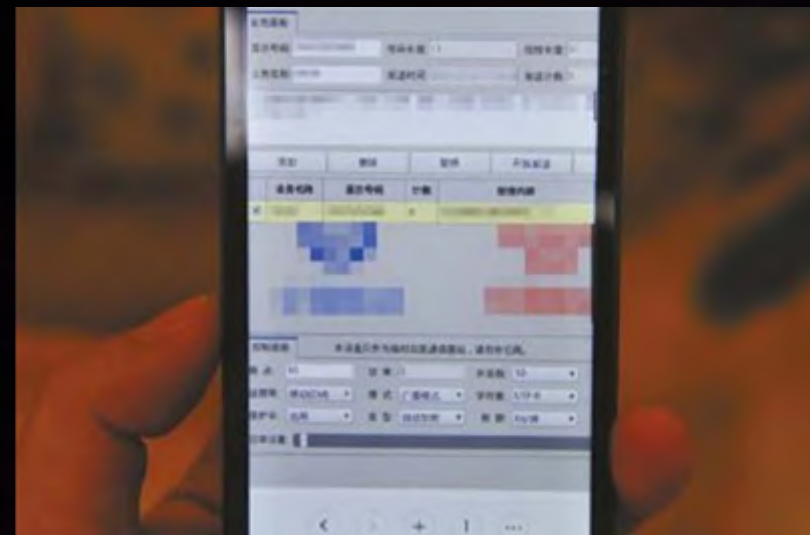


背包哥：
200元/天
5万条/天
网络联系不见面

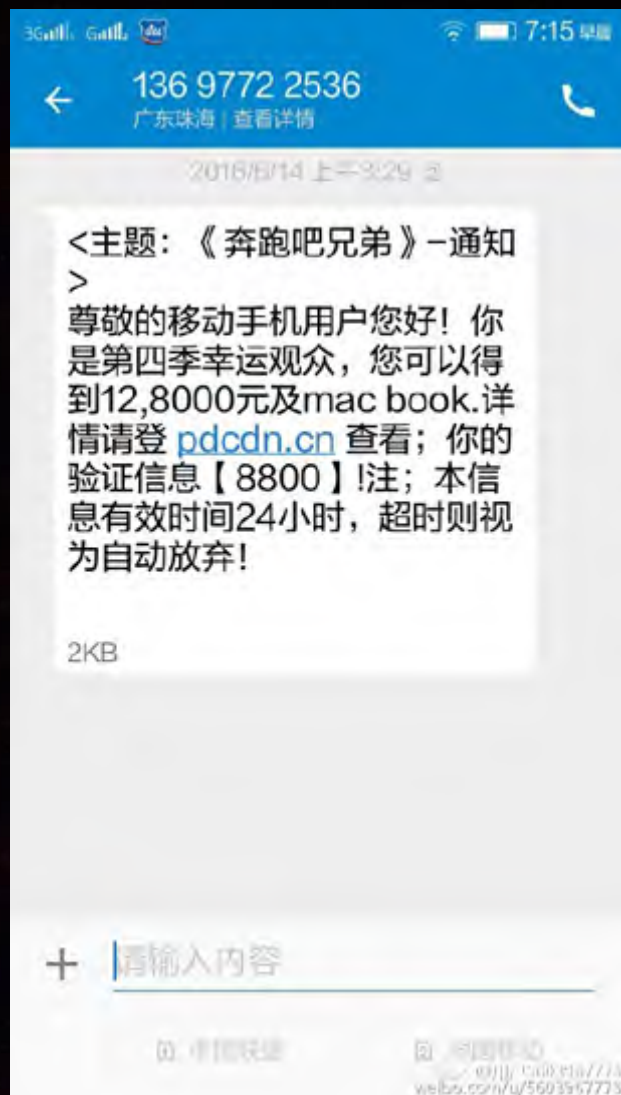


伪基站全套设备
重约30斤

便携式的伪基站
控制台



无辜被仿冒的不止我一个.....



无辜被仿冒的不止我一个.....

2015年11月钓鱼网站TOP 10



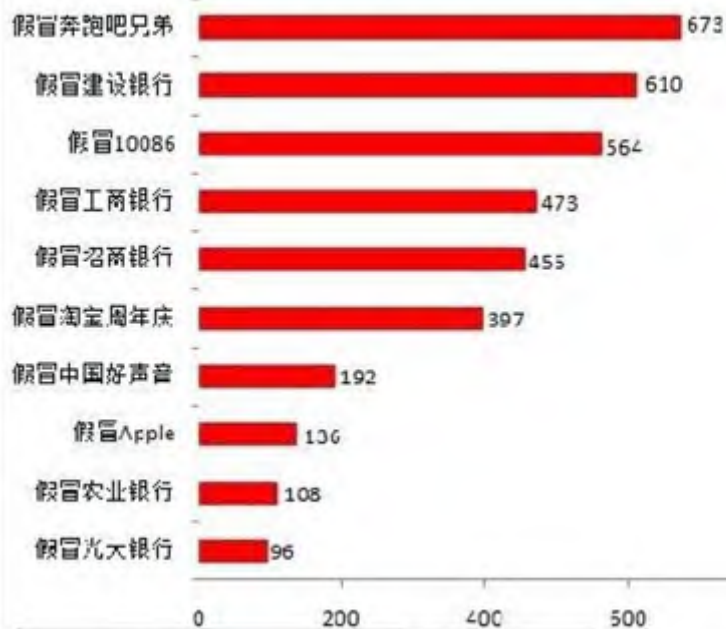
©12321举报中心 (www.12321.cn)

2015年12月钓鱼网站TOP 10



©12321举报中心 (www.12321.cn) @平安泰州
weibo.com/jspatz

2016年1月钓鱼网站TOP 10



©12321举报中心 (www.12321.cn)

2016年4月钓鱼网站TOP 10



©12321举报中心 (www.12321.cn)

2016.5

黑锅就这么背上了.....



尊敬的客户：您好！您
码积分27900可兑换279.0
元，积分即将过期，登
取：10086bcp.com，感
的支持！



钓鱼诈骗网站处置难度大



- ✓域名注册30元，实时生效
- ✓钓鱼网站500元，重复利用



- ✓68%托管在亚太，25%托管在欧美



- ✓平均生命周期12小时



- ✓主动交出银行卡密码
- ✓年龄段70-90后之间

托管在境外

安全意识低

坏蛋是很狡猾的.....



选择查询类型: 日 选择时间: 2016-06-13 排名: 100 提交

排名	钓鱼网站域名	钓鱼网站IP	钓鱼网站IP归属	累计访问次数
1	http://l0086a...d.com	103.25...97.26	香港	990
2	http://l0086v...f.com	123.1...0.22	香港 新世界电讯数据中心	745
3	http://jfw.l00...kac.com	103.56...14.152	香港	740
4	http://l0086x...d.com	103.25...97.26	香港	613
5	http://jfw.l00...dhy.com	103.25...97.254	香港	522
6	http://www.c...0086z.cn	70.39...0.50	美国 科罗拉多州丹佛市SharkTech数据中心	444
7	http://jfw.l00...xkc.com	103.56...14.152	香港	377
8	http://l0086v...u.com	123.1...0.22	香港 新世界电讯数据中心	317
9	http://jfw.l00...kes.com	103.56...14.152	香港	296
10	http://www.l...36xri.com	69.165...7.34	香港 新世界电讯	265



宝宝心里委屈
心里苦

运营商积极主动应对



运营商采用**五点**联动模式，积极斩断钓鱼诈骗链的关键节点，有效降低诈骗成功率

①主动检测并攻击伪基站

自动识别伪
基站

远程攻击使
伪基站瘫痪

不影响现网
2/3/4G网络

对数十台伪基站破解，几十万行代码深入研究，**基于无线网络攻防对抗**技术。远程攻击致其瘫痪

重点区域
定点部署

流动型
路测部署

②主动管控访问钓鱼网站



③访问钓鱼网站善意提醒



④钓鱼网站主动挖掘管控

Whois 115.144.58.53 :

inetnum: 115.144.0.0 - 115.144.255.255
netname: HAIONNET
descr: HAIonNet
descr: 705, EnC Venture Dream Tower 3-cha, Guro 3dong, Guro-gu, Seoul-si
descr: *****
descr: Allocated to KRNIC Member.
descr: If you would like to find assignment
descr: information in detail please refer to
descr: the KRNIC Whois Database at:
descr: <http://whois.nic.or.kr/english/index.htm>
descr: *****
country: KR
admin-c: SL1891-AP
tech-c: SL1891-AP
status: Allocated Portable

15 Websites use this IP address :

10086bjrd.com
l0086xhn.com
10086vntb.com
10086feun.com
l0086xxin.com
10086gthv.com
10086gjr.com
10086bjrb.com
l0086obc.com
jfw10086lhk.com
xal0086jf.com
sdl0086us.com
l0086mwy.com
appleva-icloud.com
applemat-icloud.com

⑤配合钓鱼诈骗链条侦测

[重庆配合公安捣毁22起伪基站 网易新闻](#)

2016年5月5日 - 4月,重庆市无线电办公室与重庆市公安局刑警总队密切配合,协同联动,开展打击治理伪基站违法犯罪专项活动,成功摧毁一批伪基站,查处一批违法犯罪人员,有...
[news.163.com/16/0505/0...](#) - [V3](#) - 百度快照 - 705条评价

[江苏移动配合公安斩断伪基站“利益链”-新华网](#)

2015年12月21日 - 截至目前,2015年江苏移动已配合公安,无线电管理委员会发现伪基站线索158起,缴获设备160台,抓获不法分子198人。江苏移动提醒广大消费...
[www.js.xinhuanet.com/2...](#) - [V3](#) - 百度快照 - 84%好评

[四川移动配合公安部门出重拳打击伪基站背包客 科技 腾讯网](#)



2015年11月13日 - 四川移动配合公安部门出重拳打击伪基站背包客 文章来源:中国信息产业网 最近一段时间,一种被称为“背包客”的新型伪基站在成都悄然出现。面对这种情况...
[tech.qq.com/a/20151113...](#) - 百度快照 - 61条评价

[江苏移动配合公安斩断伪基站“利益链”最高人民检察... 新浪新闻](#)

2015年12月4日 - 原标题:江苏移动配合公安斩断伪基站“利益链”近年来伪基站案件让消费者不堪其扰。据不完全统计,每年通过伪基站设备发送的诈骗、赌博、推销、中奖等...
[news.sina.com.cn/a/201...](#) - 百度快照 - 196条评价

[中移动配合公安机关破获仿冒10086特大诈骗团伙 运营 中国信息产业网](#)

2016年6月8日 - 据统计,截至2015年4月,中国移动共配合执法机关侦破伪基站案件2955例,缴获设备3495套,抓获犯罪嫌疑人4396名。关键词:公安机关 诈骗团伙 钓鱼网站 破获...
[www.cnii.com.cn/teleco...](#) - 百度快照 - 72%好评

给手机用户的一点建议

- 短信内的链接都别点
- 访问钓鱼网站要提防
- 打死不说卡号和密码
- 誓死保卫短信验证码



千万千万要记得！！！！

- 不相信
- 不点击
- 不联系
- 不汇款

谢谢！