2016 中国互联网安全大会
China Internet Security Conference

协同联动 共建安全+命运共同体

画地为牢-公共Wi-Fi的黑白暗战

by:p0tt1

About Me

姚威
ID:黑客叔叔p0tt1
广州凌晨网络科技有限公司CEO
雨袭团RainRaid信息安全团队负责人
凌晨三点3AM安全实验室负责人
2015发布《中国一线城市公共WiFi安全与潜在威胁调查研究报告》

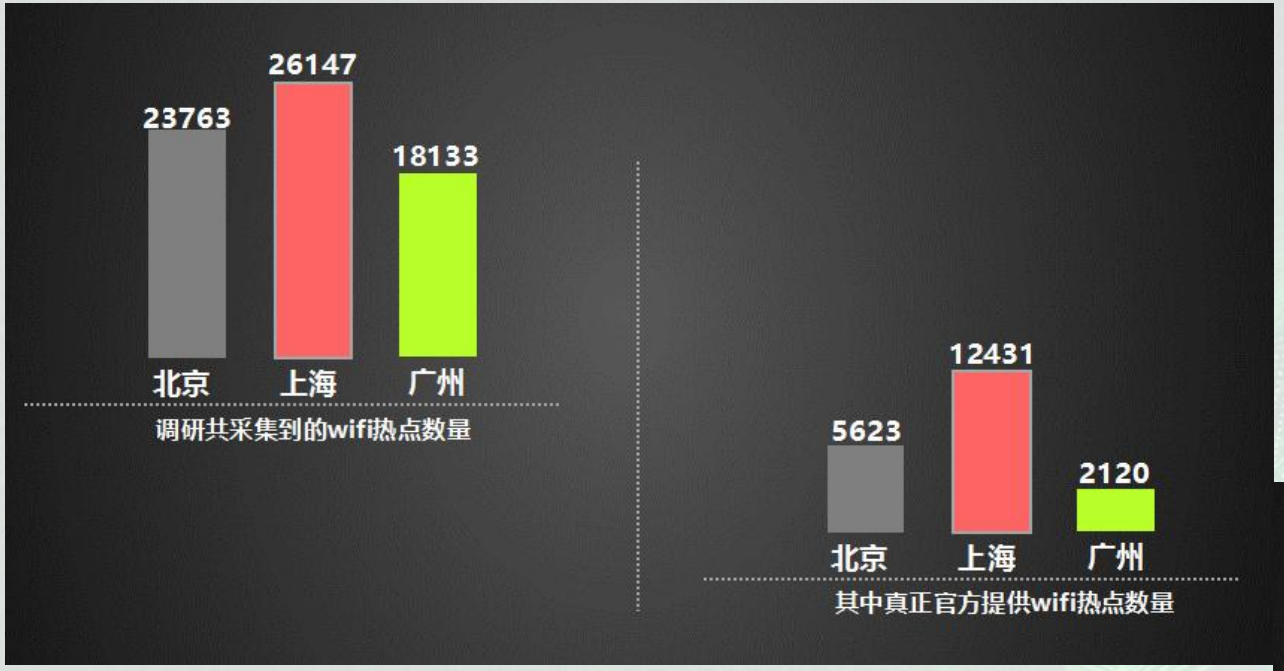
凌晨网络科技

ISC 2016 中国互联网安全大会 | HACK PWN 安全极客狂欢节

目录

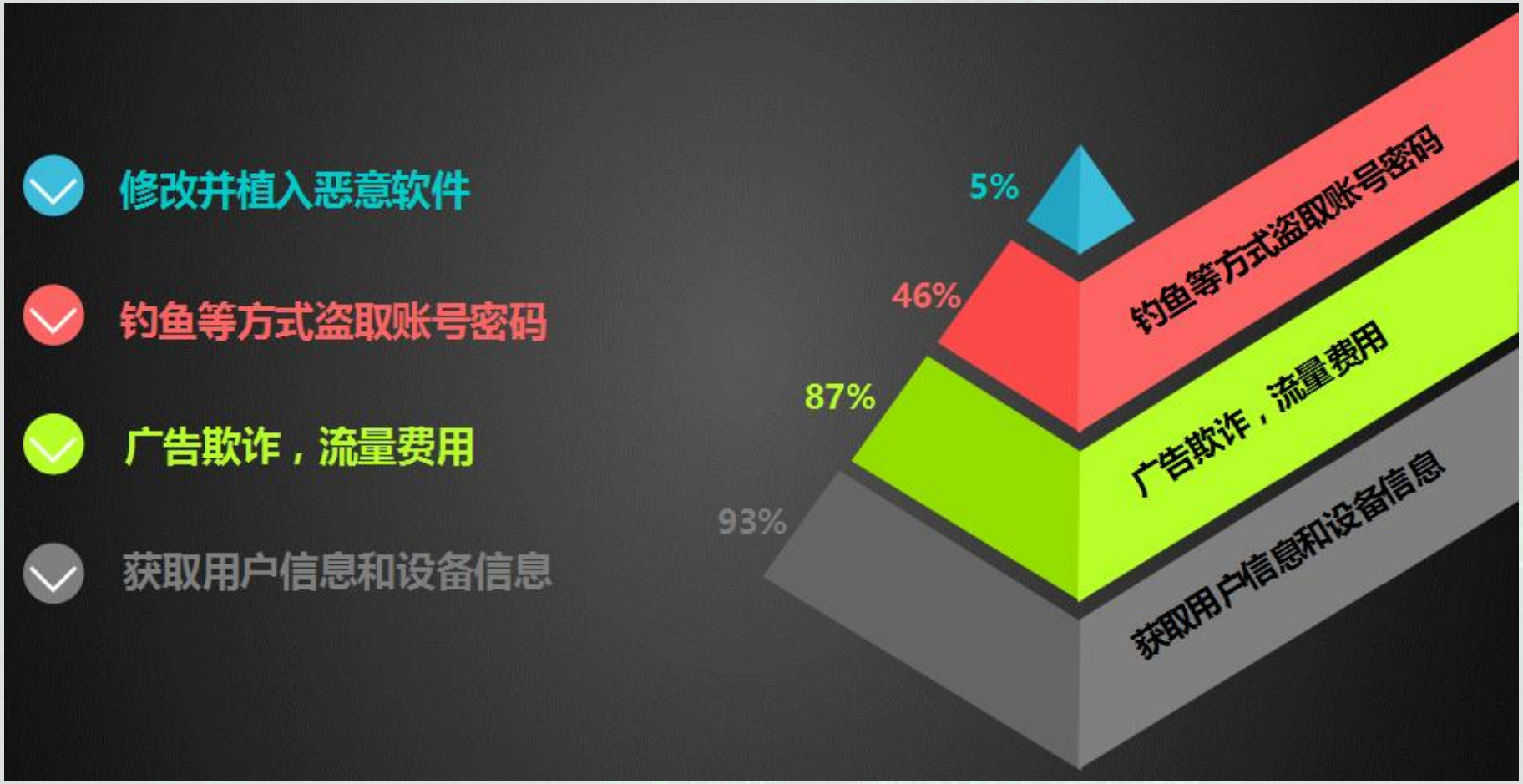
时隔一年，物是人非

时间回到一年前：数据


23763
26147
18133
北京
上海
广州
调研共采集到的wifi热点数量
5623
12431
2120
北京
上海
广州
其中真正官方提供wifi热点数量

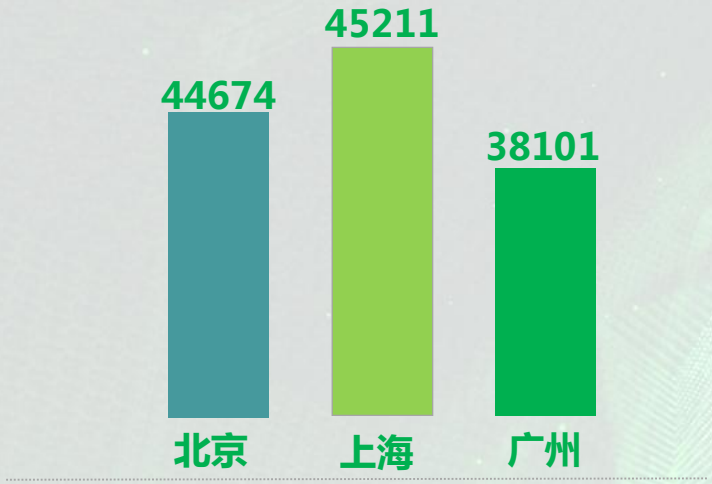

公共设备
家庭热点
第三方公司业务
店铺自建热点
寄生虫热点
临时热点
钓鱼wifi
第三方公司业务 34%
店铺自建热点 23%
寄生虫热点 14%
公共设备 9%
钓鱼WiFi 8.5%
家庭热点 7.5%
临时热点 4%

时间回到一年前：行为

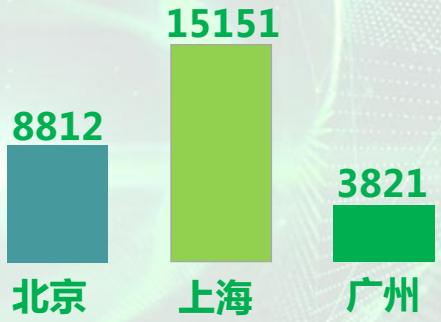

修改并植入恶意软件
钓鱼等方式盗取账号密码
广告欺诈，流量费用
获取用户信息和设备信息
5%
46%
87%
93%
钓鱼等方式盗取账号密码
广告欺诈，流量费用
获取用户信息和设备信息

时间回到一年前：寄生虫

重新审视现在：数据



调研共采集到的wifi热点数量



其中真正官方提供wifi热点数量

重新审视现在：行为

第三方公司业务　37%

店铺自建热点　26%

寄生虫热点　15.5%

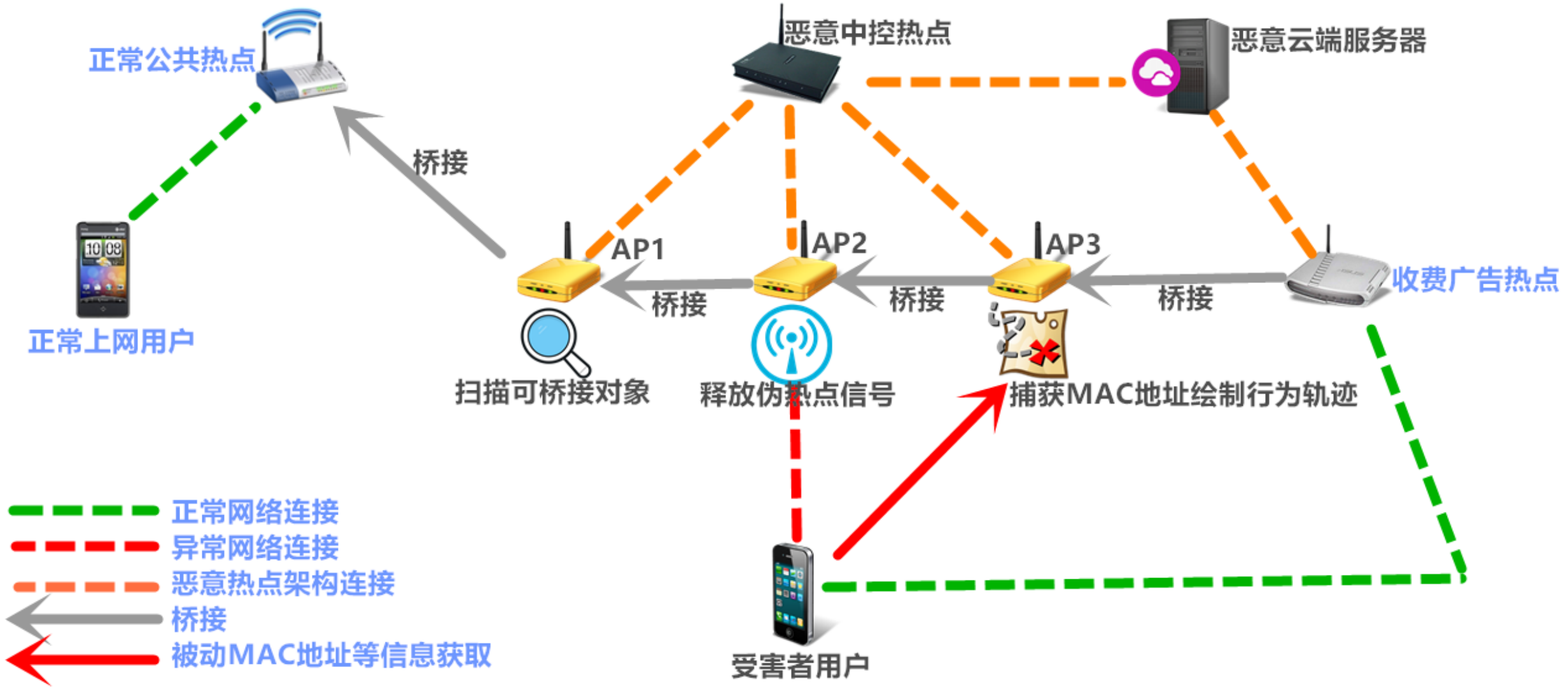
公共设备　1.5%

钓鱼WiFi　9%

家庭热点　7.5%

蜘蛛Wi-Fi　3.5%

重新审视现在：新问题-蜘蛛Wi-Fi



ISC 2016 中国互联网安全大会

HACK PWN 安全极客狂欢节

推陈出新，此消彼长

推陈出新，此消彼长

免费网络
验证页面

免费无线网络用户验证

身份证号码

手机号

选择线路 电信光纤

房号(选填)

提交 QQ登录

FreeWiFi与腾讯手机管家强强联手打造

使用QQ账号登录赠送3个月QQ会员体验

多运营商线路选择最快速的冲浪快感

可用唯一的证件号直接登录无需密码

推陈出新，此消彼长


和
中国移动
China Mobile
4G 2周年
新人充值1元
送10元话费
送
输入以下信息，即可畅享网络
请输入姓名
请输入身份证
请输入手机号
同意《公共WIFI用户守则》
QQ登录
登录
新闻中心 | 诚聘英才 | 采购信息 | 企业合作 | 联系我们 | 站点导航 | 中国移动研究院 | 中国移动设计院 | 网站地图 | 友情链接
掌上营业厅：wap.10086.cn 语音自助服务：10086 短信营业厅：10086 自助终端 营业厅 手机营业厅下载
Copyright©1999-2015 中国移动 版权所有
中华人民共和国增值电信业务经营许可证 经营许可证编号：A2.B1.B2-20100001
可信网站 身份验证
京ICP备05002571号

推陈出新，此消彼长

获取流量信息

获取个人隐私

收买广告营销

社交网络推广

魔高一尺，道高一丈？

魔高一尺，道高一丈？

1.移动安全软件防护

2.浏览器安全防护

3.黑白名单检测

4.支付流程保护

5.MAC地址校验

6.IP地址校验

7.安全意识教育

魔高一尺，道高一丈？

1.桥接正常网络

2.伪装智慧城市“钓鱼”

3.数据加密回传

4.动态伪造MAC地址

5.数据统一管理

6.使用者VPN校验

7.出售“正规”广告

利字当头，取之无道

利字当头，取之无道

￥126.00 0人付款

a手机wifi穿墙王大功率家用广告微信wifi广告营销商业路由器.

[redacted] 广东 广州

￥126.00 0人付款

a移动wifi家用无线穿墙1200Mwifi广告营销商业路由器.

[redacted] 广东 广州

￥184.80 0人付款

[redacted]双天线300M广告营销无线路由器商业WIFI控制器

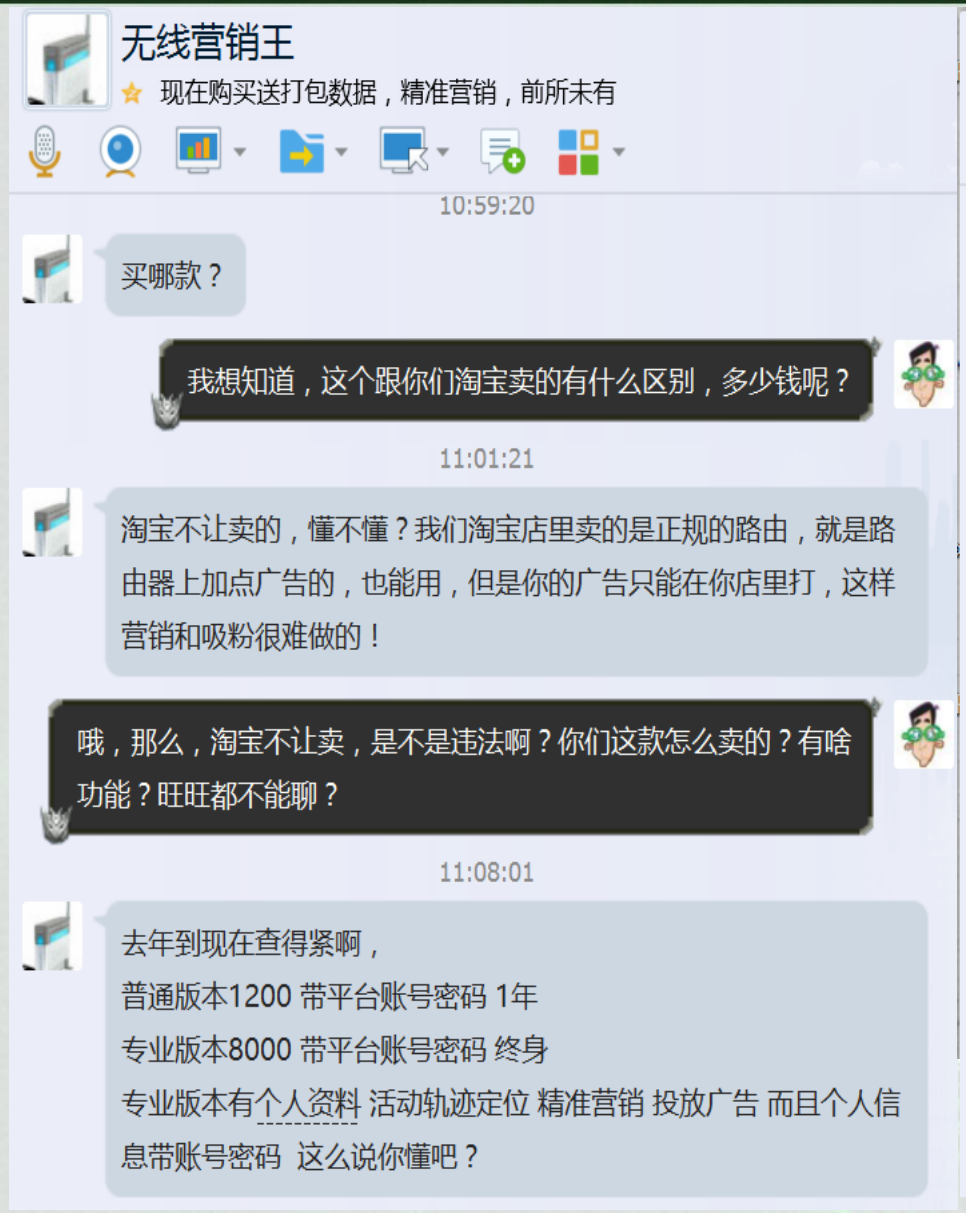
[redacted] 广东 广州

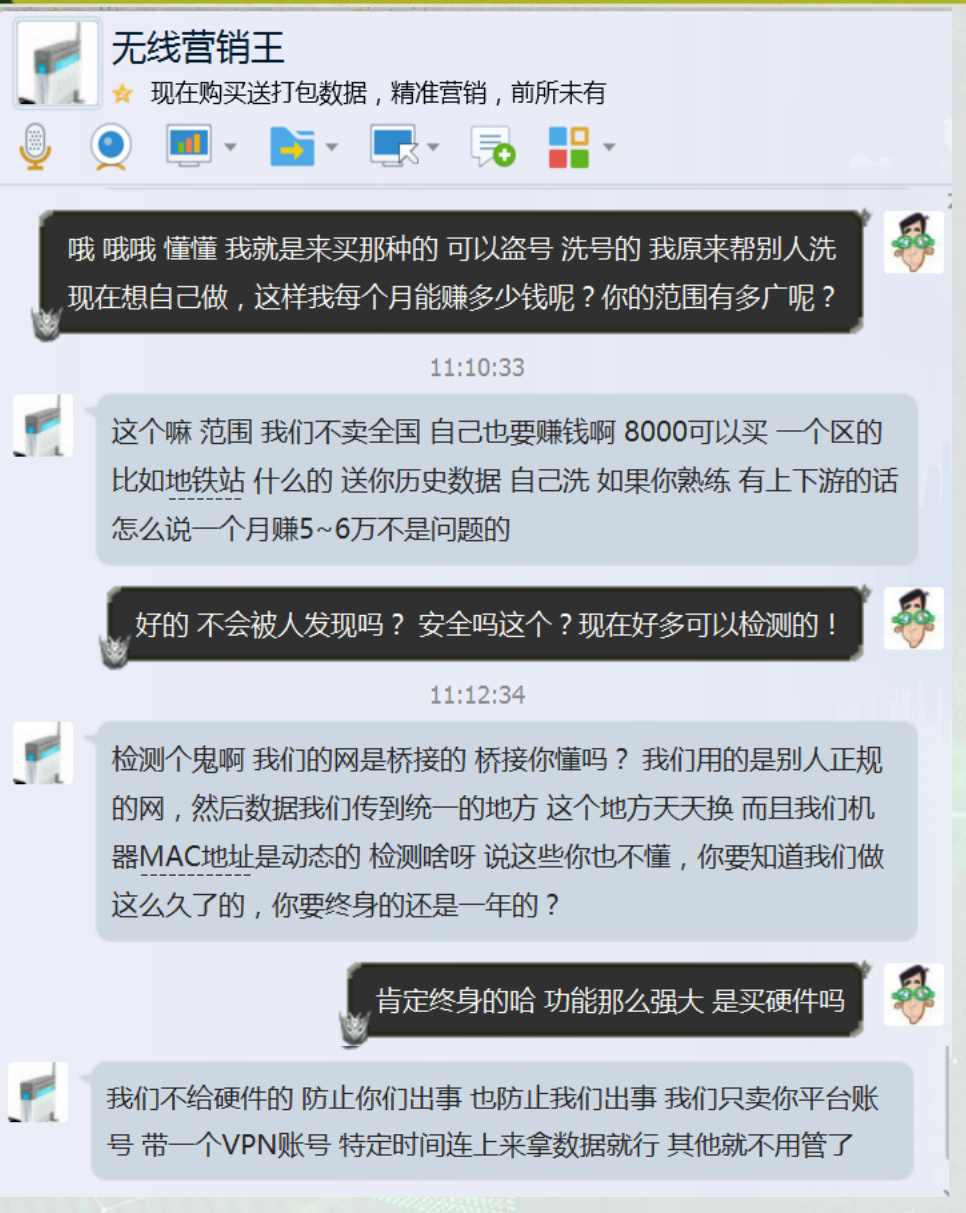
￥488.00 包邮 0人付款

基本型WIFI营销系统广告路由微信吸粉餐饮神器商业WIFI秀水美地

[redacted] 黑龙江 哈尔滨

利字当头，取之无道


无线营销王
现在购买送打包数据，精准营销，前所未有
10:59:20
买哪款？
我想知道，这个跟你们淘宝卖的有什么区别，多少钱呢？
11:01:21
淘宝不让卖的，懂不懂？我们淘宝店里卖的是正规的路由，就是路由器上加点广告的，也能用，但是你的广告只能在你店里打，这样营销和吸粉很难做的！
哦，那么，淘宝不让卖，是不是违法啊？你们这款怎么卖的？有啥功能？旺旺都不能聊？
11:08:01
去年到现在查得紧啊，
普通版本1200 带平台账号密码 1年
专业版本8000 带平台账号密码 终身
专业版本有个人资料 活动轨迹定位 精准营销 投放广告 而且个人信息带账号密码 这么说你懂吧？


无线营销王
现在购买送打包数据，精准营销，前所未有
哦 哦哦 懂懂 我就是来买那种的 可以盗号 洗号的 我原来帮别人洗 现在想自己做，这样我每个月能赚多少钱呢？你的范围有多广呢？
11:10:33
这个嘛 范围 我们不卖全国 自己也要赚钱啊 8000可以买 一个区的 比如地铁站 什么的 送你历史数据 自己洗 如果你熟练 有上下游的话 怎么说一个月赚5~6万不是问题的
好的 不会被人发现吗？ 安全吗这个？现在好多可以检测的！
11:12:34
检测个鬼啊 我们的网是桥接的 桥接你懂吗？ 我们用的是别人正规的网，然后数据我们传到统一的地方 这个地方天天换 而且我们机器MAC地址是动态的 检测啥呀 说这些你也不懂，你要知道我们做这么久了的，你要终身的还是一年的？
肯定终身的哈 功能那么强大 是买硬件吗
我们不给硬件的 防止你们出事 也防止我们出事 我们只卖你平台账号 带一个VPN账号 特定时间连上来拿数据就行 其他就不用管了

ISC 2016 中国互联网安全大会

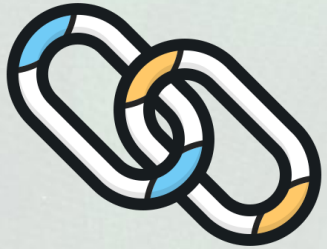
HACK PWN 安全极客狂欢节

千疮百孔，痛定思痛

千疮百孔，痛定思痛

SSID

MAC



NETWORK

千疮百孔，痛定思痛

检测

防护

谢谢

中国互联网安全大会

安全极客狂欢节