



# “黑产” 在做什么数据分析

Zer0ne(陈杨轲)

# About Me

陈杨轲

ID:Zer0ne

广州凌晨网络科技有限公司CIO

夜莺“反黑产”小组负责人

原Cnit.Pro站长

LL. 凌晨网络科技

***RainRaid***

*From the people  
For the people*

夜莺  
Nightingale

CNIT.PRO



# Contents

讲述一个真实的对抗故事



0x001 如今的'黑产'现状

0x002 短信蠕虫变种与集团作案介绍(SMS-EVO)

0x003 我们做了些什么，'夜莺'的歌声

0x004 '黑产'集团化，我们是否还孤军奋战



如今的'黑产'现状

## 说在前面-消息来源



不靠'线人'和'卧底'  
我们居然拿不到第一手信息了

# 社工库打击前 和 打击后

Baidu 百度 社工库 查询 百度一下

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多

百度为您找到相关结果约116,000个 搜索工具

[社工库-社工库在线查询-嗅密码-密码泄露查询](#)  
社工查询库 登陆 注册 票小组sS平台IP定位详细地址开房查询QQ群[需翻墙]社工裤2(免登录)帮助为了遵守国家道德法规 查询结果关键字段 已经用星号隐藏 敬请放心 本...  
sgk.fbisb.com/ - 百度快照 - 100%好评

[社工库-社工库查询-搜密码-密码泄露查询-找回丢失的密码](#)  
本社工库所有数据均来自网络,本社工库仅作技术交流之用,不可用于不良用途!... 社工库 搜密码 乌云 freebuf ©搜密码 2014-2016 联系: seventh@cnav.cn ...  
www.soumima.com/ - 百度快照 - 评价

[最全的社工库免费查询,太可怕了。。推荐都去查一下。-V2EX](#)  
2015年8月28日 - 社工库 可怕 查询 免费178 回复 | 直到2016-04-02 03:07:34 +08:00 1 2 < >  
101 ccbikai 2015-08-28 15:56:46 +08:00 直接明文,尼玛 ...  
www.v2ex.com/t/216... - 百度快照 - 85%好评

[社工库-你的密码泄露了吗?](#)  
本社工库所有密码泄露数据均来自网络,快速将社工库内扫描结果呈现出来,本社工库仅作技术交流之用,不可用于不良用途!  
www.shunmay.cn/ - 百度快照 - 评价

[社工库查询-哇哇社工库-防撞库攻击](#)  
社工库数据均收集于互联网,包含几乎所有网上已经公开的账号数据,并不断更新中。仅供查找自己的用>户密码,如存在请尽快更改自己的密码,防止被社工,被撞库攻击!! ...  
www.fangzhuangku.com/ - 百度快照 - 评价

[社工库-社工库查询-嗅密码-密码泄露查询-找回你丢失的密码](#)

Baidu 百度 社工库 百度一下

网页 新闻 贴吧 知道 音乐 图片 视频 地图 文库 更多

百度为您找到相关结果约262,000个 搜索工具

[句读科技大数据中心社工库](#) 广告  
社工库为您构建私有化的资源探测感知与漏洞预警能力,“社工库”稳定,安全,低成本”的产品服务咨询电话:18683081231  
www.colaeeye.com 2016-10 - V1 - 评价

[“社工库”网站成人肉搜索工具 可查开房记录?](#)  
2014年6月11日 - 前日,网上传出消息称,一家名为“我就是社工库”的网站,可以通过输入QQ号查看该号主人大量的隐私内容。社工库的搭建源代码和查询使用的用户数据库...  
news.eastday.com/eastd... - 百度快照 - 60条评价

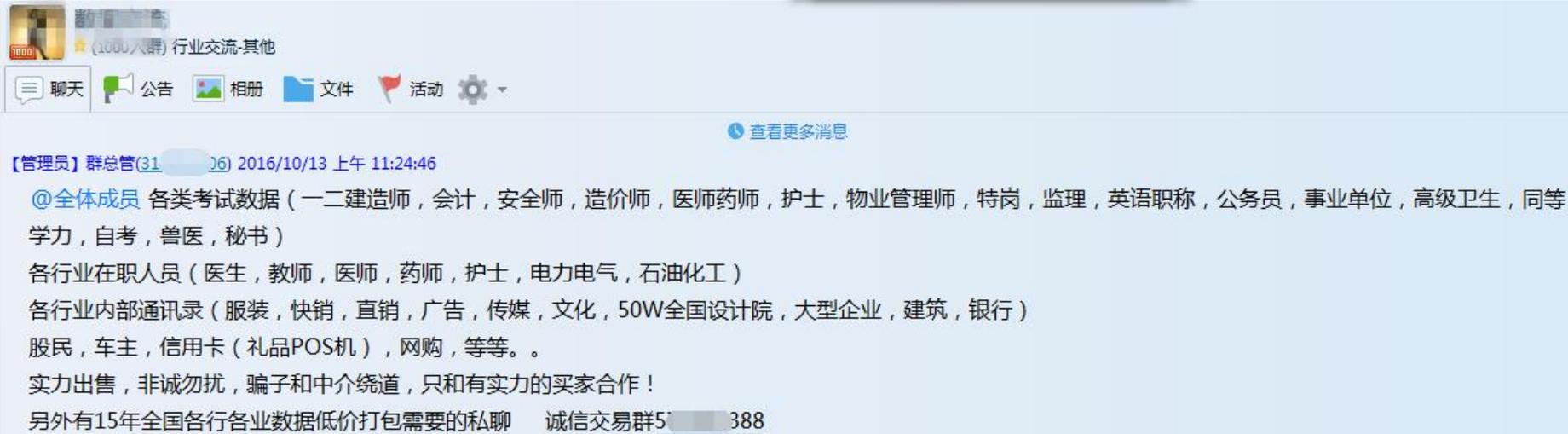
[“社工库”网站成人肉搜索工具 掌握多家网站用户数据-中新网](#)  
2014年6月11日 - 前日,网上传出消息称,一家名为“我就是社工库”的网站,可以通过输入QQ号查看该号主人大量的隐私内容。社工库的搭建源代码和查询使用的用户数据库...  
www.chinanews.com/life... - V3 - 百度快照 - 363条评价

[“社工库”查密码信息,警方六招帮助保密码安全](#)  
2014年6月18日 - 新华网浙江频道6月18日电(记者 岳德昊)近日,一家名为“我就是社工库”的网站,可以通过输入QQ号查看该号主人大量的隐私内容,甚至...  
www.zj.xinhuanet.com/n... - V3 - 百度快照 - 852条评价

[前日,网上传出消息称一家名为“我就是社工库”的网站,可以通过](#)  
2014年6月11日 - 前日,网上传出消息称,一家名为“我就是社工库”的网站,可以通过输入QQ号查看该号主人大量的隐私内容。社工库的搭建源代码和查询使用的用户数据库...  
www.sznews.com/tech/co... - 百度快照 - 99条评价

[“社工库”网站成人肉搜索工具 掌握多家网站用户数据-人肉网站-](#)  
2014年6月11日 - 社工库网提供多家网站用户数据,目前市面上有数种此类网站的社工库网,它们...

# 地下窝点的'贴靠'，卧底不是加个群那么简单！



聊天 公告 相册 文件 活动

[查看更多消息](#)

【管理员】群总管(31...26) 2016/10/13 上午 11:24:46

@全体成员 各类考试数据（一二建造师，会计，安全师，造价师，医师药师，护士，物业管理师，特岗，监理，英语职称，公务员，事业单位，高级卫生，同等学力，自考，兽医，秘书）

各行业在职人员（医生，教师，医师，药师，护士，电力电气，石油化工）

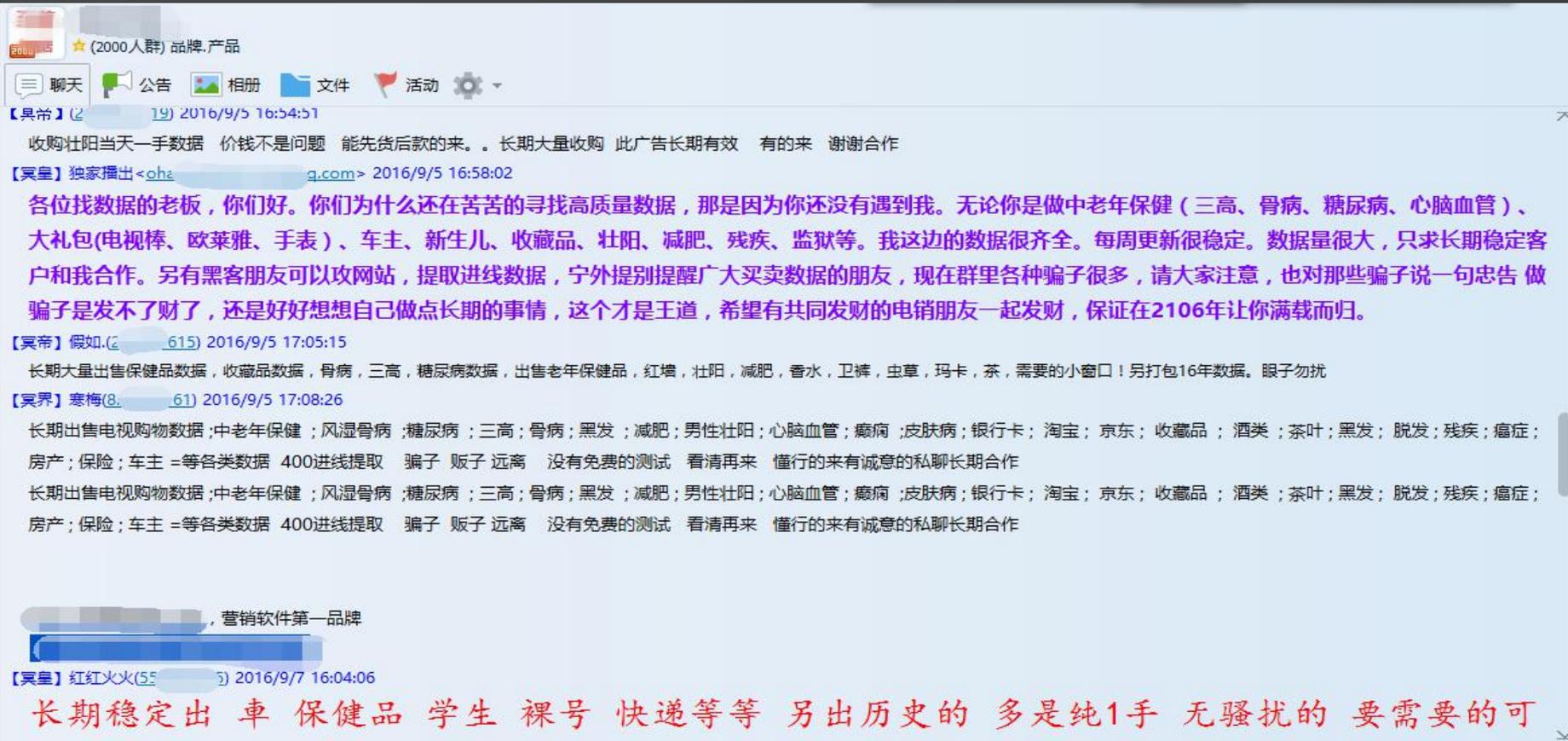
各行业内部通讯录（服装，快销，直销，广告，传媒，文化，50W全国设计院，大型企业，建筑，银行）

股民，车主，信用卡（礼品POS机），网购，等等。

实力出售，非诚勿扰，骗子和中介绕道，只和有实力的买家合作！

另外有15年全国各行各业数据低价打包需要的私聊 诚信交易群5...388

# 地下窝点的'贴靠', 卧底不是加个群那么简单!



聊天 公告 相册 文件 活动 设置

【具帝】(2000人群) 品牌.产品 19) 2016/9/5 16:54:51

收购壮阳当天一手数据 价钱不是问题 能先货后款的来。。长期大量收购 此广告长期有效 有的来 谢谢合作

【冥皇】独家播出<oh&...q.com> 2016/9/5 16:58:02

各位找数据的老板，你们好。你们为什么还在苦苦的寻找高质量数据，那是因为你还没有遇到我。无论你是做中老年保健（三高、骨病、糖尿病、心脑血管）、大礼包(电视棒、欧莱雅、手表)、车主、新生儿、收藏品、壮阳、减肥、残疾、监狱等。我这边的数据很齐全。每周更新很稳定。数据量很大，只求长期稳定客户和我合作。另有黑客朋友可以攻网站，提取进线数据，宁外提别提醒广大买卖数据的朋友，现在群里各种骗子很多，请大家注意，也对那些骗子说一句忠告 做骗子是发不了财了，还是好好想想自己做点长期的事情，这个才是王道，希望有共同发财的电销朋友一起发财，保证在2106年让你满载而归。

【冥帝】假如。(2000人群) 品牌.产品 2016/9/5 17:05:15

长期大量出售保健品数据，收藏品数据，骨病，三高，糖尿病数据，出售老年保健品，红墙，壮阳，减肥，香水，卫裤，虫草，玛卡，茶，需要的小窗口！另打包16年数据。眼子勿扰

【冥界】寒梅(8...61) 2016/9/5 17:08:26

长期出售电视购物数据；中老年保健；风湿骨病；糖尿病；三高；骨病；黑发；减肥；男性壮阳；心脑血管；癫痫；皮肤病；银行卡；淘宝；京东；收藏品；酒类；茶叶；黑发；脱发；残疾；癌症；房产；保险；车主 = 等各类数据 400进线提取 骗子 贩子 远离 没有免费的测试 看清再来 懂行的来有诚意的私聊长期合作

长期出售电视购物数据；中老年保健；风湿骨病；糖尿病；三高；骨病；黑发；减肥；男性壮阳；心脑血管；癫痫；皮肤病；银行卡；淘宝；京东；收藏品；酒类；茶叶；黑发；脱发；残疾；癌症；房产；保险；车主 = 等各类数据 400进线提取 骗子 贩子 远离 没有免费的测试 看清再来 懂行的来有诚意的私聊长期合作

...，营销软件第一品牌

【冥皇】红红火火(55...5) 2016/9/7 16:04:06

长期稳定出 车 保健品 学生 裸号 快递等等 另出历史的 多是纯1手 无骚扰的 要需要的可

# 地下窝点的'贴靠'，卧底不是加个群那么简单！

1000 (1000人群) 行业交流-其他

聊天 公告 相册 文件 活动 设置

**[经理]** 福建普用金融(913) 2016/8/28 19:02:17  
收国内一手二手国内手机数据 有的滴滴滴

**[经理]** 站住别动^\_^ (2) 2016/8/28 19:21:02  
求购卫裤和玛卡数据，日需3000条可测试联系我，骗子和钓鱼全家死完，马蛋遍地都是骗子。。。

**[经理]** 姿态(64) 2016/8/28 19:48:04  
执业医师分省全国名单都有。支持任何测试。中级会计名单全国都有。支持任何测试。价格冰点。有需要的联系。

系统消息(1000000) 2016/8/28 19:51:36  
管理员开启了全员禁言，只有群主和管理员才能发言

**[管理员]** 群总管(316) 2016/8/30 11:57:32

Seagate Expansion Drive (F:)  
115 GB 可用，共 1.36 TB

**@全体成员**

本人专注数据多年数据库已经超1000G最新2016年各类考试数据（一二建造师，会计，安全师，造价师，医师药师，护士，物业管理师，特岗，监理，英语职称，公务员，事业单位，高级卫生，同等学力，自考，兽医，秘书）

各类学生数据（大学生，研究生，小中高学生家长，GCT,MBA）

各行业在职人员（医生，教师，医师，药师，护士，电力电气，石油化工）

各行业内部通讯录（服装，快销，直销，广告，传媒，文化，50W全国设计院，大型企业，建筑，银行）

股民，车主，信用卡（礼品POS机），网购，政府本，等等。

实力出售，非诚勿扰，骗子和中介绕道，只和有实力的买家合作！

另外有15年全国各行各业数据低价打包需要的私聊

新建诚信数据群

做'黑产'不赚钱，说出去都丢人



'黑产'爱财，取之无'道'

虽无'道'德，但多的是渠'道'

钓鱼网站

中奖信息

手机木马

电话欺诈

招聘骗局

股票推荐

网银盗取

游戏盗号

电商刷单

违禁微商



# 坏人的信任危机

当我傻啊... ..

- 1.我看过《今日说法》
- 2.我没钱！
- 3.上次我就这么被你们骗的！
- 4.兄弟，同行，自己人！

发给你看看,快下载！ 猜猜我是谁！  
 你中奖了哦！ 我是法官！  
 你有法院传票！ 我是XXX警官！  
 来我办公室一趟！ 兄弟我被抓了！  
 车祸，堕胎，急救，行贿，反正急用！

你当我傻吗？！



民众



坏人

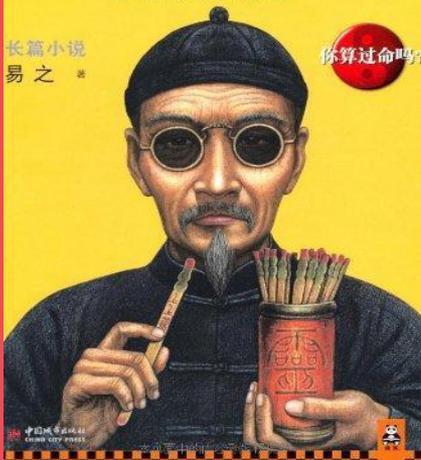


# 我是个算命先生

让一个82岁的算命老先生，带您见识算命背后的古老智慧与江湖术数。  
平租、面相、八字、八卦、周易、紫微

长篇小说  
易之 著

你算过命吗？



## '黑产'与骗局的进化

在你认为他们将没落时大显身手！

掌握足够的受害者真实信息

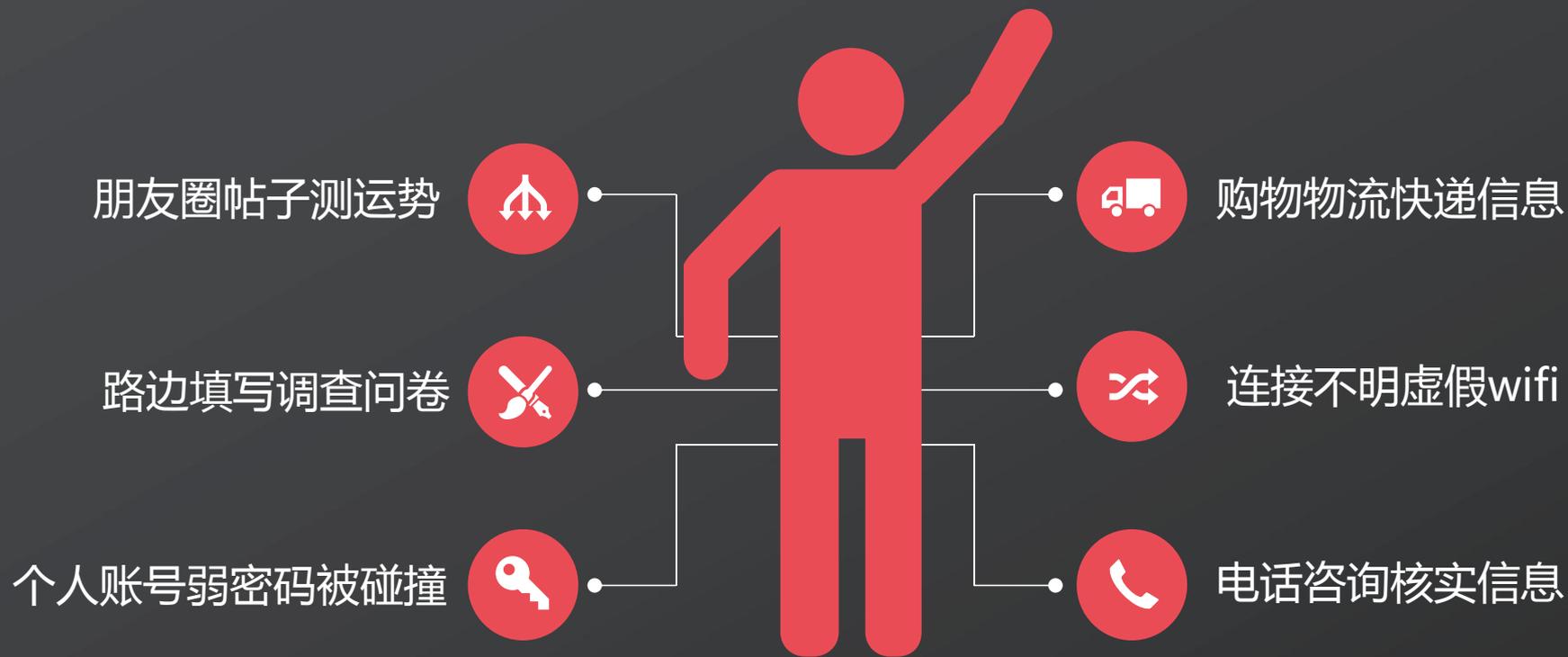
足够准确

足够隐私

罪恶的土壤是？



# 看看我们怎么把自己'贱卖'的！



 我先是信了,然后跪了,想想也是醉了!



坏人怎么知道的?



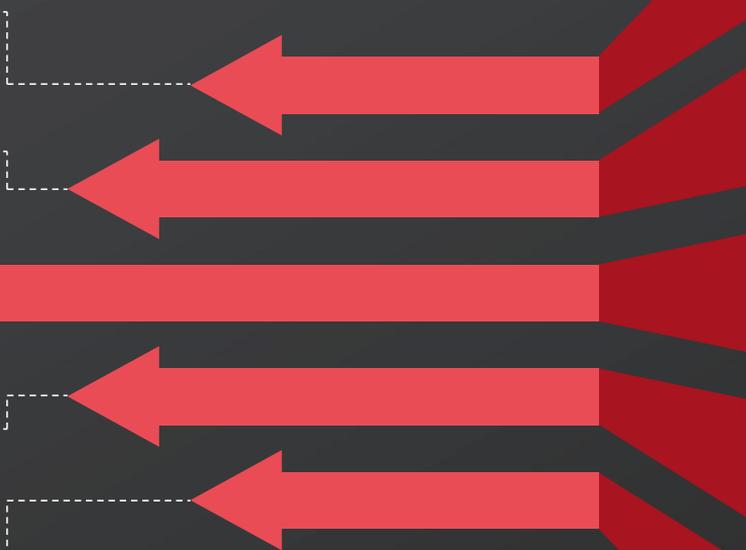
李雷是吧? 这个月工资卡更换了!

我是韩梅梅, 老同学给发个红包呗?

你车牌号京A-94170违章催缴

你幸福小区的房东换银行卡了

你银行卡6222\*\*\*\*\*888涉嫌洗钱



## 复杂的黑色产业链开始流水线了



信息猎手  
渠道商人  
分销马仔

采集

数据分类  
关联分析  
易骗人群

分析

组织人员  
分配角色  
实施攻击

布局

匿名账户  
资金扭转  
取钱分赃

分赃



# 短信蠕虫变种与集团作案介绍 (SMS-EVO)

# 安天-AVL移动安全 发布的《Curiosity病毒分析报告》



## “七夕病毒”肆虐 百万用户被感染

2014年08月05日 08:26:13 来源：新京报 分享到：



2014年第一季度手机病毒传播途径分布



数据来源：网秦 新京报制图/张妍

深圳警方8月2日晚11点在其官方微博宣布，于七夕前后泛滥的“××神器”病毒短信案件已告破。犯罪嫌疑人是一名19岁的大一新生。

“×××(机主姓名)看这个，ht://\*\*\*\*\*××shenqi.apk。”8月1日，很多人收到了一条莫名其妙的短信，并当作七夕节日祝福打开。大家却不知晓，一旦点击下载链接中的软件，手机的通讯录将在后台被自动监听。同时，手机还会自动复制这条短信并向通讯录中的名单群发。

# 短信蠕虫病毒的前世今生

为什么还能继续野蛮生长？  
为什么成了打不死的小强？  
为什么病毒的变种那么多？  
为什么还有这么多人中招？  
为什么病毒功能越来越多？

'黑产'总让安卓系统背黑锅！



安卓木马便宜

能拿短信内容

只要用户点击权限就够高

能拿通讯录

能劫持短信

木马APK容易安装

能远程控制

能群发传播



## 我们跟踪的'黑产'团伙(SMS-EVO)干了些啥？

### 准备

域名批量注册  
正规网站投毒  
绝不重复使用  
及时毁尸灭迹

### 策划

服务器全部静态  
木马链接随机化  
收费版收信邮箱  
散播收信周期快

### 执行

散播传染有渠道  
数据分析有能力  
各类信息有下家  
匿名账户有资源

### 盈利

能卖的绝不自己骗  
能骗的多少都去骗  
建立渠道分销同行  
背锅人多法不责众

# 这就是对抗中进化的SMS-EVO团伙



自己编写  
更新版本快  
加密加壳方式多  
自升级



[www.muma.com](http://www.muma.com)

批量注册  
匿名注册  
删除废弃快  
存量大



<http://muma.com/ydk3>

地址自动生成  
地址随机化  
网页静态化  
链接去除.APK



VIP收信邮箱

收费邮箱  
自动删除邮件  
客户端取信  
多邮箱抄送

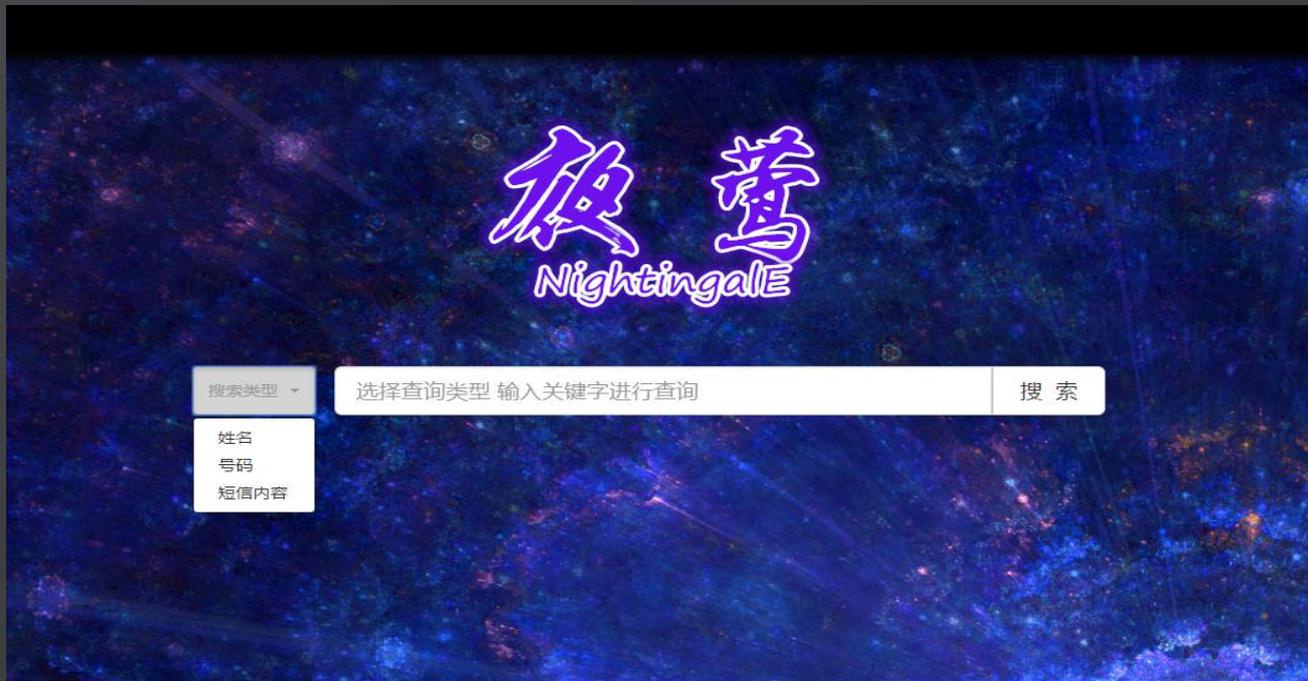


我们做了些什么

我们自己的团队做了哪些事情？



*RainRaid*  
From the people  
For the people



## 短信 & 通讯录

数据随机滚动

### 通讯录

外父	13556119049
猪肉狗	134241872
罗动庄深仔	13048125
李莹莹	13600381
百德订台	134220792
阿清	131720683
胖子强	137109380
小舅	136222216
骆健文	136101377
虫仔	139261633
阿好	139261131
嘉嘉	134341890
申通快递	137941736
么仔	158181153
丹伟	139291468
高田玲哥	139261195
大眼仔	137281721
外母	159201987
林秉在哥	139031755

### 短信

2015-03-28 15:45:39	recv	+8613685032...	收到。
2015-03-28 16:20:06	recv	106580210140...	北京市政府提示您：游北京请选择正规旅行社，详情查询 <a href="http://www.bjta.go...">http://www.bjta.go...</a>
2015-08-23 15:21:20	recv	106580210140...	北京市政府提示：游北京请选择正规旅行社（ <a href="http://www.bjta.gov.cn">www.bjta.gov.cn</a> ）或旅游集散中...
2015-04-01 08:59:11	recv	+8613599444...	请问您是哪位？
2015-04-01 09:05:14	send	+8613599444...	你好,我外公墓园每年都是你帮助打扫,今年还是麻烦你帮助打扫,本周六（...
2015-04-01 13:47:00	send	+8613960840...	柯经理,你好!我是省农行公司业务部杨凡,因上次出差错过泰康到省分行现场办...
2015-04-01 14:03:25	recv	+8613960840...	下个月我们再去服务时给我吧！
2015-04-01 14:04:00	send	+8613960840...	好的,谢谢！
2015-04-03 08:53:36	recv	+8613685032...	杨总，材料已发到您邮箱
2015-04-03 09:45:45	send	+8613685032...	好。
2015-04-03 12:33:45	recv	+8613685032...	杨总，邮件收到了
2015-04-03 12:34:26	send	+8613685032...	好,辛苦你了!
2015-04-07 11:49:45	recv	+8613685032...	杨总，我修改的材料发给您了，请查收，看一下可以吗，麻烦您了
2015-04-07 11:54:43	send	+8613685032...	已收到,我现在在外办事，下午2点半左右与你联系。
2015-04-07 11:55:32	recv	+8613685032...	知道了，麻烦您了

# 我们针对短信蠕虫病毒做了哪些事情

## 通讯录

电工	15613	5303
杨欢	18733	9330
吴	15030	3089
朱子	15830	5565
马小冬	13933	1294
胜会花	13731	1385
福利	13930	5530
李三	13292	9029
来来1	15133	7555
蛋头	13133	4413
阎海龙	15133	2160
妈	13780	9100
阎海龙1	13383	5503
占春2	15232	7666
郭是荣	13930	9459
阎海军1	18733	2522
杨宝武	13833	1743
快捷	13731	8098

## 短信

2015-09-24 19:38:30	recv	95599	【中国农业银行】您尾号2119的农行账户于09月24日19时37分完成一笔现支...
2015-09-25 18:11:10	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日18时10分完成一笔超级...
2015-09-25 18:12:09	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日18时10分完成一笔超级...
2015-09-25 18:12:43	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日18时11分完成一笔超级...
2015-09-25 18:13:29	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日18时12分完成一笔超级...
2015-09-25 19:24:55	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日19时23分完成一笔易县...
2015-09-25 19:42:28	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日19时41分完成一笔网银...
2015-09-25 19:47:52	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日19时46分完成一笔兰宝...
2015-09-25 19:52:52	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日19时51分完成一笔西平...
2015-09-25 21:05:41	recv	95599	【中国农业银行】您尾号2119的农行账户于09月25日21时04分完成一笔现支...
2015-09-26 12:14:03	recv	95599	【中国农业银行】您尾号2119的农行账户于09月26日12时12分完成一笔围场...
2015-09-26 12:21:53	recv	95599	【中国农业银行】您尾号2119的农行账户于09月26日12时20分完成一笔易县...
2015-09-26 18:35:46	recv	95599	【中国农业银行】您尾号2119的农行账户于09月26日18时35分完成一笔转支...
2015-09-26 18:47:34	recv	95599	【中国农业银行】您尾号2119的农行账户于09月26日18时46分完成一笔王飞...

# 我们针对短信蠕虫病毒做了哪些事情

## 通讯录

车队高胖子	18931044981
张裴军	1503007585
郭建	13830030300
刘师傅	1380005286
一矿索绚丽	1510008655
张路洋	1863107229
韩志远	1393100655
少波涛	1830006885
王文中	1350006903
李增田	1383005965
宋姐	1393009997
张常明老大	1370006777
张长明老二	1383002777
韩鑫	1863003055
一矿杨志强	1518000880
拉面	1393007334
总调小	13830098446
小建儿	1890008322
用拉高歌	1373004628

## 短信

2016-03-10 07:30:10	recv	95595	光大卡尾号7585还款4000元。请勿在陌生、虚假网站输入个人及卡片信息，...
2016-03-13 21:15:14	recv	95595	光大卡尾号7585还款1000元。任何人向您索要手机动态密码、支付密码均为...
2016-03-16 07:30:40	recv	95595	光大卡尾号7585还款5000元。任何人向您索要手机动态密码、支付密码均为...
2016-03-18 11:26:26	recv	95595	光大卡尾号7585还款3000元。如需办理分期还款业务，请致电4006666999[...
2016-03-20 21:14:56	recv	95595	手机查账单，还能办分期！中国光大银行全新推出移动版信用卡账单，账单详...
2016-03-02 14:56:44	recv	+8613949033...	13253000257刘岩
2016-03-09 13:02:40	send	+8615803879...	熙越妈妈，您好！我是吴晋鑫爸爸，上次宝宝的保险计划，我讲明白了吗？你...
2016-03-09 13:05:44	recv	+8615803879...	我想买有医疗报销和住院补贴那个，不过我想这几天先把孩子的居民医保建上...
2016-03-09 13:08:51	recv	+8615803879...	麻烦你抽空再出个你给我的那种有明细的单子，保额按10万，有居民医保，其...
2016-03-09 13:20:28	send	+8615803879...	好的，没问题
2016-03-15 20:13:38	send	+8615803879...	熙越妈妈，您好！我是吴晋鑫爸爸。第二次做的计划您有什么不明白的，不要...
2016-03-15 20:34:46	recv	+8615803879...	好的，周四舞蹈课我去咨询你 - 【中国移动高清语音全省率先试商用，接通无...
2016-03-15 20:35:39	send	+8615803879...	好的，早点休息。
2016-03-18 09:35:23	send	+8615803879...	熙越妈妈，今天您有时间或方便的话下午或者晚上见个面，具体解答您和熙越...
2016-03-18 09:45:45	recv	+8615803879...	我在开会，我昨晚看了看给熙越买的保险，是交10年保20年，20年后可以返...

# 坏人为什么知道你叫啥？

通讯录

短信

name	phonenum
老王	138306937
菏泽老王	138608884
潍坊老王	138308725
老王	188706007
老王	132709935
老王	137606738
老王	152002635
老王	182905532
老王	152002635
老王	182905532
南阳老王	150907882
瓦工老王哥哥	151601249
老王	138309689
老王涂料	138307122
老王	136208271
黑茶老王	139003462
老王哥哥容	150001638
装修工老王	13030292
老王舅远女士	+8610609453

# 坏人怎么那么了解你？

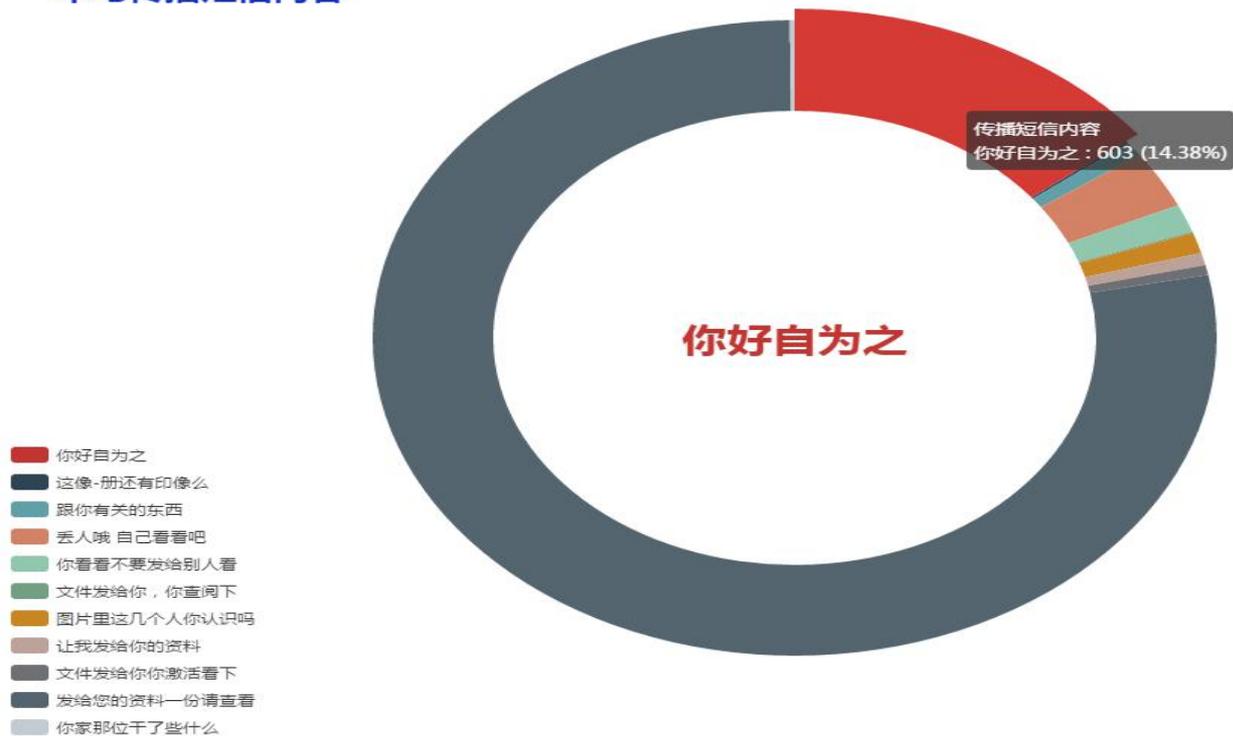
1325	95588	recv	2016-03-24 10:11:17	您尾号7035卡3月24日10:11网上银行收入(徐涵春支付宝转账)20,000元,余...
1747	95555	recv	2014-08-05 15:55:07	马丽娟于2014年08月05日 15:55向贵账户4875发起13500.00元的转账;本短...
1748	95555	recv	2014-12-16 09:00:43	马丽娟于2014年12月16日 09:00向您账户2409发起150000.00元的转账;本短信...
1749	95555	recv	2014-12-30 11:33:45	马丽娟于2014年12月30日 11:33向您账户2409发起100000.00元的转账;本短信...
1752	95555	recv	2015-06-17 15:12:21	尊敬的用户,感谢您申办招商银行一卡通,更多优惠,免费转账,专属高收益...
1757	95555	recv	2015-11-28 09:44:45	任何向您索要验证码的都是骗子,千万别给!您正在向崔涛(尾号6747)转账
1763	95555	recv	2016-01-13 15:48:49	任何向您索要验证码的都是骗子,千万别给!验证码583152,您正在向绍华...
1764	95555	recv	2016-01-13 15:53:46	任何向您索要验证码的都是骗子,千万别给!验证码694533,您正在向邵华...
1818	95511	recv	2014-09-18 10:40:16	尊敬的叶小东:您的P32*9713个人费用99保费576元经尾号5845邮储账户转账...
1819	95511	recv	2014-09-18 10:40:21	尊敬的叶小东:您的P32*9714平安康盛保费847元经尾号5845邮储账户转账成...
1832	95511	recv	2015-09-16 11:12:22	尊敬的叶小东:您的P32*9714平安康盛保费843.1元经尾号5845邮储账户转账...
1833	95511	recv	2015-09-16 11:12:24	尊敬的叶小东:您的P32*9713个人费用99保费576元经尾号5845邮储账户转账...
1931	95528	recv	2015-12-03 14:09:27	尊敬的我行客户,现诚邀您申办浦发信用卡,与您浦发借记卡关联即可完成自...
2562	9555812	recv	2016-03-19 18:02:04	【中信银行】尊敬的叶小东先生,感谢您选择中信银行,您目前享有使用我行...
3150	+8613298331...	send	2013-07-10 19:20:50	您正通过实时转账向中国平安支付9186.00元,请输入动态密码:8384459,...
3303	95588	recv	2014-08-17 12:23:46	您尾号6128卡17日12:23自助终端支出(转账)50,000元,余额1,353,013.76元...

# 坏人怎么知晓你的行踪？

id	phonenum	mms_type	mms_time	mms_body
603	12306	recv	2015-08-12 17:39:40	(2/2)可持二代身份证直接检票乘车或换取纸质车票后乘车。【铁路客服】
604	12306	recv	2015-08-12 17:39:45	(1/2)订单号E919539828,谢先生您已购08月14日G7343次06车10A号、10...
605	12306	recv	2015-08-14 18:56:44	(1/2)订单号E989385994,谢先生您已购08月15日G7639次06车1张无座。...
606	12306	recv	2015-08-14 18:56:49	(2/2)直接检票乘车或换取纸质车票后乘车。【铁路客服】
607	12306	recv	2015-08-14 19:19:00	(2/2)国强、王珏、谢锦池可持二代身份证直接检票乘车或换取纸质车票后乘...
608	12306	recv	2015-08-14 19:19:05	(1/2)订单号E968495883,谢先生您已购08月15日G1678次08车10A号、10...
609	12306	recv	2015-08-14 19:32:14	(1/2)订单号E959337620,谢先生您已购08月17日G7698次03车17A号、17...
610	12306	recv	2015-08-14 19:32:19	(2/2)国强、王珏、谢锦池可持二代身份证直接检票乘车或换取纸质车票后乘...
611	12306	recv	2015-09-03 21:30:03	(2/3)号南京南18:48开,检票口B17。王珏(G7686)、王珏(G7605)可持二...
612	12306	recv	2015-09-03 21:30:08	(3/3)车。【铁路客服】
613	12306	recv	2015-09-03 21:30:10	(1/3)订单号E950194783,谢先生您已购09月07日G7686次03车02B号溧阳0...
614	12306	recv	2015-09-26 15:07:29	(3/3)谢锦池(G7686)、谢锦池(G37)、谢国强(G37)、王珏(G37)可持...
615	12306	recv	2015-09-26 15:07:35	(2/3)7次05车09F号15车08C号、08D号南京南20:39开,检票口B3。谢国强(...
616	12306	recv	2015-09-26 15:07:37	(1/3)订单号E936108657,谢先生您已购10月06日G7686次04车01C号、01...
617	12306	send	2015-12-01 15:08:36	999
618	12306	recv	2015-12-01 15:08:44	12306用户注册或既有用户手机核验专用验证码:824030。如非本人直接访...
7362	106581391230...	recv	2016-03-10 10:26:09	中国移动提醒:请您关注当前手机【套餐/业务】,回复A开始查询详情!
7364	12306	recv	2016-03-15 16:16:14	【铁路客服】订单E672791424,伍先生您已购3月16日D2266次6车12A号恩...

# 看看我们最喜欢点哪些病毒短信的链接

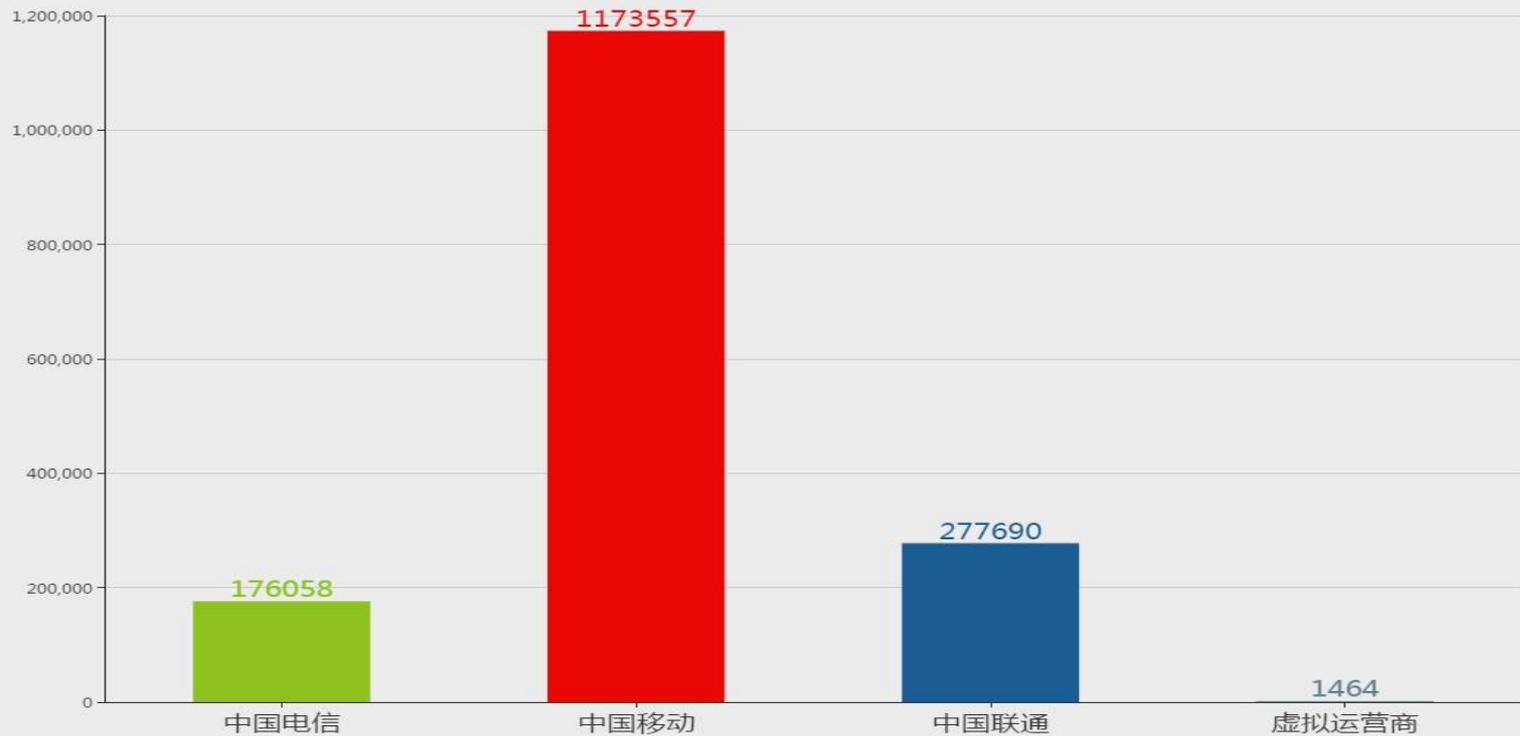
## 木马传播短信内容





# 受害者运营商统计，虚拟运营商为什么那么少？

通讯录号码运营商信息



# 受害者区域分布图

## 通讯录手机号归属地

- 中国电信
- 中国移动
- 中国联通
- 虚拟运营商





对抗本就不是一件势均力敌的事情，却必须得做！

'黑产':

多少人前赴后继甚至  
牢狱之灾换来的血淋  
淋的经验，筹码够多，  
有恃无恐，跟随互联  
网发展，见缝插针，  
无孔不入！



我们:

要防护的**攻击面太广**，  
实际筹码并不多。  
而且对面的群体庞大，  
应对和反制较为**困难**。  
需要结合**多方力量**共  
同推动。



'黑产'集团化，我们是否还孤军奋战



当民众面对越来越多的网络威胁时，  
我们如何为受害者当好神队友？

# 当下可能要练的功夫



内功  
绝对不主动送信息



马步  
抵御诱惑和诱导



双刀  
相关部门与社会力量



太极  
从数据源头抓根源





**Thanks**

