骨子里的黑客梦

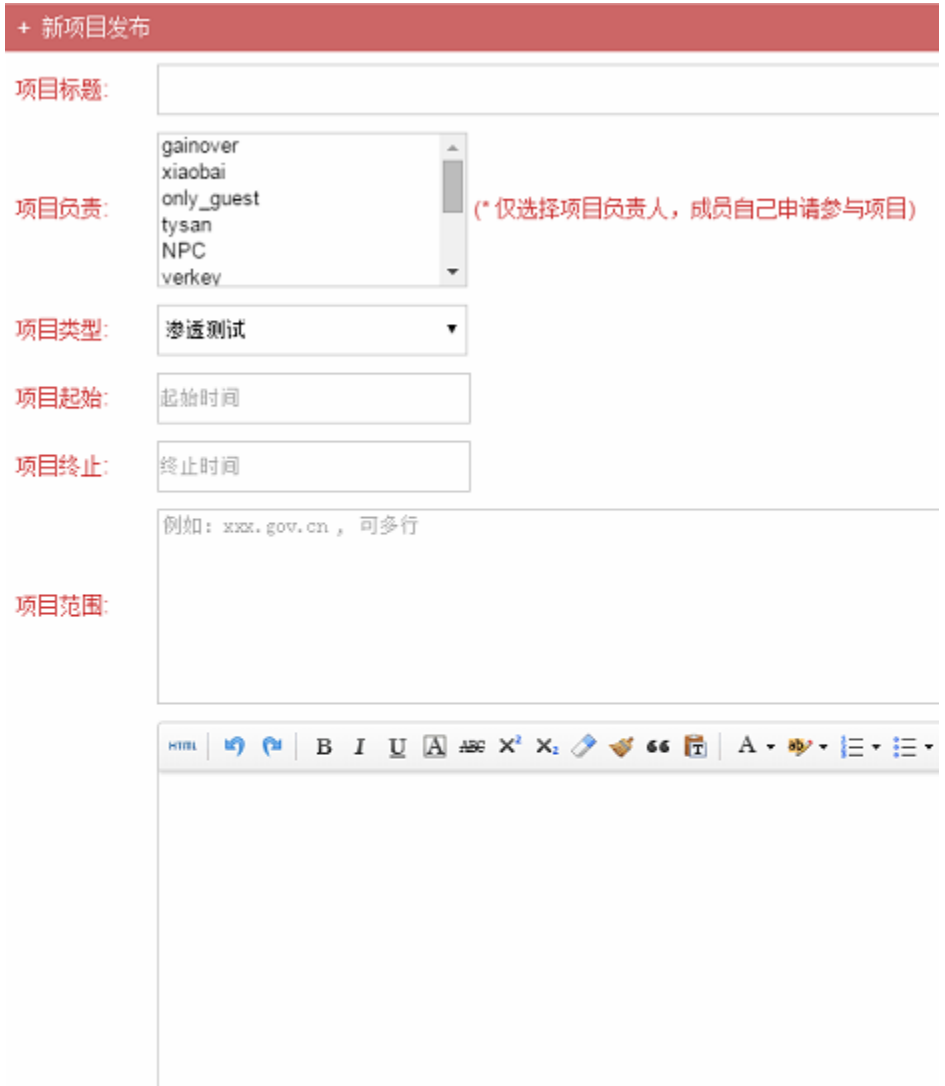
怎么组建一个黑客团队？

让工作变得像页游


双螺旋实验室工作平台
用户:
密码:
登录
重置
Powered by DoubleHelix


> 后台管理 [退出]
+ 个人事务
个人主页
个人项目
所有项目
绩效统计
密码修改
+ 项目管理
新项目发布
待评分项目
待验收项目
项目人员审核
漏洞类型管理
+ 日常安排
个人日程
每周议题
+ 人员管理
月底分数归档
员工管理
级别评定
+ 关于程序
待修改列表
程序更新日志
+ 所有项目列表
[• 进行中] [2015
[• 进行中] [2015
[• 已关闭] [2015
[• 已关闭] [2015
[• 已关闭] [2015
[• 进行中] [2015
[• 进行中] [2015
[• 已关闭] [2015
分页: 1 2 3 4 5

让工作变得像页游


+ 新项目发布
项目标题:
项目负责:
gainover
xiaobai
only_guest
tysan
NPC
verkev
(* 仅选择项目负责人，成员自己申请参与项目)
项目类型:
渗透测试
项目起始:
起始时间
项目终止:
终止时间
项目范围:
例如：xxx.gov.cn ，可多行

让工作变得像页游


+ 项目参与人
gainover
伟大娃娃
tysan
香草
xiaoL
felixk3y
only_guest
css
+ 项目报告列表
> sql注入漏洞
> 验证码重放
> 搜索引擎泄露敏感资料
> 后台地址泄露
> 敏感信息泄露
> 服务器相关信息泄漏
> 验证码重放
> 目录遍历漏洞


请输入报告标题
高危
请选择漏洞类型
x 取消
漏洞类型选择
移动APP
客户端应用
WEB应用
安全事件及情报
运营安全及风险
系统及服务运维
应用程序漏洞
应用流程/逻辑漏洞
应用配置错误
管理后台弱口令
URL Redirect（URL跳
未授权访问/权限绕过
JSON HiJacking（JS
Click Jacking（点击劫
命令执行
代码执行
文件包含
文件上传
文件读取/下载
SQL注入
敏感信息泄漏
确定
2. 危害等级
高危
3. 漏洞位置
请在此处输入漏洞所发生的位置，例如：某一个URL或者某一个功能模块名称。
4. 漏洞复现过程
请在此处输入漏洞具体情况，例如：漏洞复现过错。
5. 安全风险
暂无

让每一个任务变得有趣

- 收到一条这样的短信内容
- 13569095446
- 刘xx你快看，t.cn/sdfhrG2

- 受害者接收到短信后点击链接下载安装了一个文件

==========
15271035853
肖姗姗这你看~http://t.cn/RAD0Wcy
类型:发送 2015-12-07 07:26:13
==========
15871076275
二姐这你看~http://t.cn/RAD0Wcy
类型:发送 2015-12-07 07:26:13
==========
15288127717
徐这你看~http://t.cn/RAD0Wcy
类型:发送 2015-12-07 07:26:13
==========
13197166309
房东这你看~http://t.cn/RAD0Wcy
类型:发送 2015-12-07 07:26:13
==========
15587798226
周睿这你看~http://t.cn/RAD0Wcy
类型:发送 2015-12-07 07:26:13
==========
13527095595
刘得慧这你看~http://t.cn/RAD0Wcy
类型:发送 2015-12-07 07:26:13
==========
15196781065
张秀荣这你看~http://t.cn/RAD0Wcy
类型:发送 2015-12-07 07:26:13
==========

12306:12306
OPPO官方:4001666888
OPPO官方客服:4001666888
POS:15516964766
万三:13569095958
三舅:13937242578
上楼板:15936458221
世宏:13683723893
东亮:13937232892
中秋:15083049099
中秋媳妇:15565188061
二姑:15237209986
二姑:15514691949
二楼:13837235975
于柯:13937251160
亲老二:15514898388
任刚:13849287377
任勇强:15093968779
任强:15136533325
任永刚:18231015555
任海平:13569032329
伟:15994117902
何雪朋:18034211811
侯东风:13937229068
侯五星:13598136078
侯国有:15137256448
侯海刚:13525848035

军:15994142989
军委:15937239739
冬亮:13525848388
冬冬:18749338599
冯东亮:13193523319
冯东新:18317398898
冯保亮:18337276556
冯庆丰:13938689139
冯校长:18837269658
冯校长:18937283688

==========
95559
(1/2)您的亲友冯东亮诚邀您办理交通银行信用卡！登录交通银行信用卡网站申请办卡，新客户核卡即赠100元刷卡金,最快当日领卡！申【交通银行】
类型:接收 2015-05-08 10:07:48
==========
95559
(2/2)请时别忘在推荐码栏位填写亲友的手机号哦！ 详情参见信用卡网站。【交通银行】
类型:接收 2015-05-08 10:07:51
==========
1069043604
亲~表孝心很简单：妈妈舍不得买的，我送她！5.10母亲节，分期管家精选最值得买的礼物送母亲：http://dwz.cn/Jbnzm 退订回T【分期管家】
类型:接收 2015-05-08 12:26:46
==========
10655020061860707
【趣分期】999白条免费借，苹果6免利息，速抢 http://t.im/lzvr 回复TD退订
类型:接收 2015-05-08 01:03:26
==========
95595
您正在通过网络渠道申请光大银行信用卡，您申请“福”信用卡的动态密码为：643034[光大银行]

- 我监控了这个邮箱3天

文件夹	邮件数量	所占容量
收件箱	11633	268.69MB
垃圾邮件	712	1.05MB
已删除邮件	0	0.00MB
已发送邮件	0	0.00MB
草稿箱	0	0.00MB

獲取到同 訓 路,機 器 碼:865521014828189	2015-05	13 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:354337061267785	**2015-05**	**56 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:867523019257453	**2015-05**	**18 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:A000002FD6F431	**2015-05**	**28 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:358584054139010	**2015-05**	**5 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:864791026943919	**2015-05**	**5 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:null	**2015-05**	**13 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:865924016343878	**2015-05**	**3 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:865924016343878	2015-05	3 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:865737023857999	2015-05	25 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:356205051650526	**2015-05**	**14 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:866174020345894	2015-05	7 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:352156053113522	**2015-05**	**13 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:864103020720725	**2015-05**	**8 KB**	**sina(1502137...**
獲取到同 訓 路,機 器 碼:null	2015-05	5 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:862084020656188	2015-05	17 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:862084020656188	2015-05	17 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:862084020656188	2015-05	17 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:865206022429986	2015-05	113 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:865347011763207	2015-05	7 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:356131051208505	2015-05	52 KB	sina(15021371...
獲取到同 訓 路,機 器 碼:866089025219391	2015-05	10 KB	sina(15021371...

15021371481m0

发给 15021371481m0

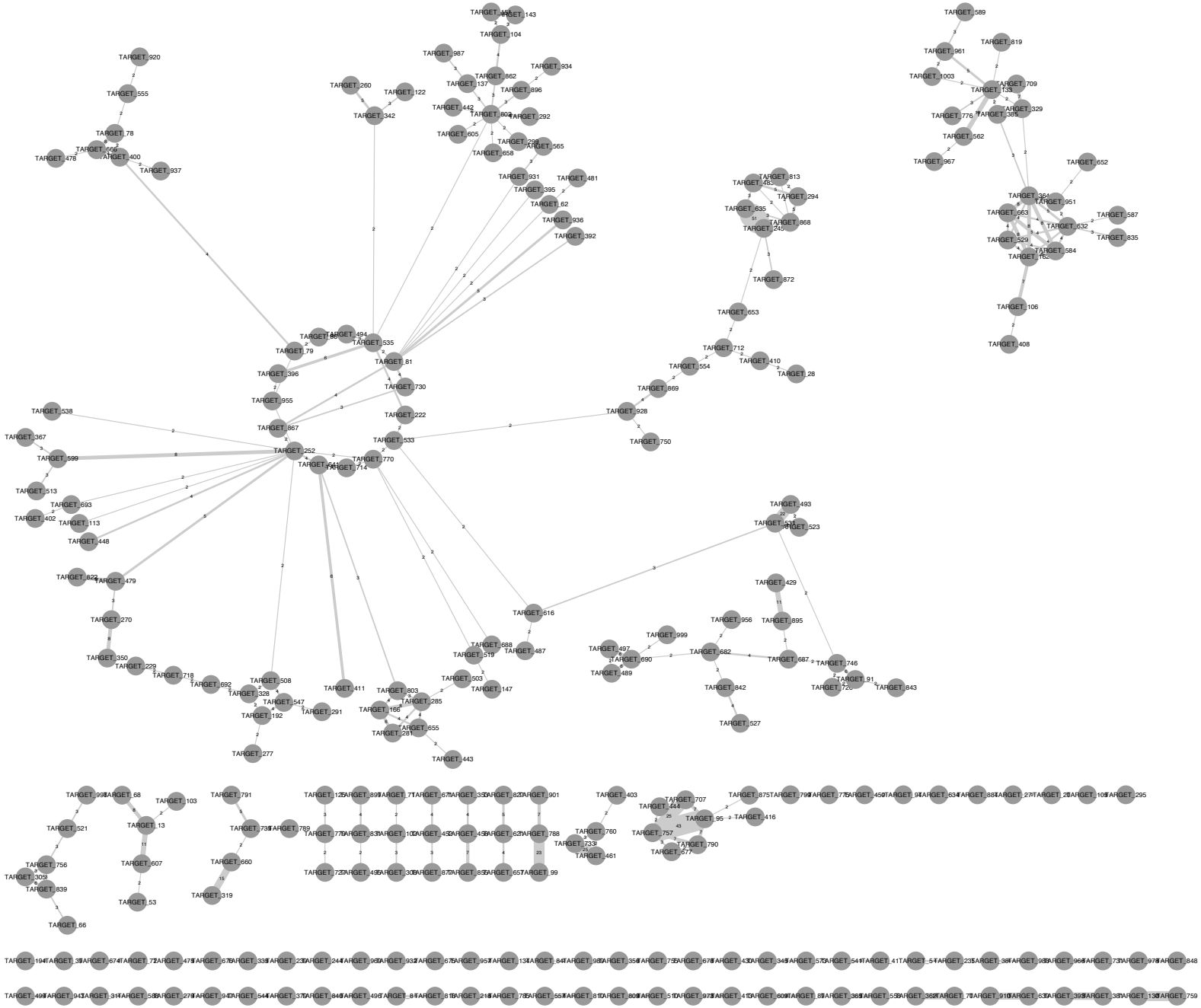
发件人: 15021371481m0<15021

收件人: 15021371481m0<15021

时间: 2016年5月5日 (周四) 16:38

大小: 6 KB

成都检察院:12309
细辛脑，:125
宋表姐:13037715363
杨通海:13037736960
杨坤友:13084391963
杨坤华:13094568833
陈四:13096031638
杨青刚:13154917383
陈思明:13198619566
张，，鸣绿村:13219786008
蒋代强:13219793327
赵敏:13281193452
刘小琴:13408293095
赵光军:13408298962
杨孟林:13419320942
黄心明:13440021653
老样:13440137140



KCon West 2016

一条来自95533的手机短信

- 尊敬的建行用户：您账户已满10000积分可兑换5%的现金，请登录手机网 wap.ccbvos.cc 查询兑换，逾期失效【建设银行】

中国建设银行
China Construction Bank
建行手机网

简洁版 完整版

客户服务热线：95533

导航 动态 查询 行情 微博

欢迎登录建行手机网
1、建行积分兑换现金活动正式举办中，使用建行账户的客户都可参与积分兑换现金活动。
2、兑换现金是按照积分的百分之五进行兑换。
3、例：积分10000分可以兑换500元现金，也就是积分的百分之五。现在可登录手机银行（积分兑换）进行兑换。
4、活动截止时间：今日截止

手机银行（积分兑换）

信用卡用户 储蓄卡用户

优惠与服务 | 最新公告 | 新闻中心

生日一起过，礼物你来拿——建行网银15周年主题…
微创新让网银页面“活”起来
建行微信狂欢季 缤纷豪礼乐翻天

更多 >>

金融服务

理财产品 基金投资 贵金属 外汇牌价 利率查询

1	银行卡号	密码	证件号码	手机号码	姓名
2	[redacted]0050950091	930127	50[redacted]99301052428	18580[redacted]72	
3	[redacted]0032780202	444888	51[redacted]97303222423	18423[redacted]08	王明芳
4	[redacted]0031234292			18302[redacted]11	
5	[redacted]0031592434	985165	50[redacted]99911143062	18725[redacted]31	陈小英
6	[redacted]0048280882	132456	50[redacted]99309132814	13452[redacted]32	杨飞
7	[redacted]0003180245	421888	51[redacted]96304213734	18502[redacted]29	张世彬
8	[redacted]46660076	200311		18875[redacted]16	
9	[redacted]0081094851	123454	50[redacted]99210144925	18723[redacted]75	
10	[redacted]49790474	199762	50[redacted]99707267743	15736[redacted]67	
11	[redacted]0017773909	951003	50[redacted]99511246410	15123[redacted]21	万睿
12	[redacted]9002806991	827625	52[redacted]99503064931	15117[redacted]14	
13	[redacted]0013600635	168668	51[redacted]97404105011	18223[redacted]35	刘小波
14	[redacted]66115291	369258		13511[redacted]44	
15	[redacted]0042086723	240514		18580[redacted]34	
16	[redacted]0065461035	312514	50[redacted]98909293719	18875[redacted]08	
17	[redacted]0036451883	100530	50[redacted]99306110025	18896[redacted]97	曹杨
18	[redacted]0086914434	960820	622[redacted]00086914434	13508[redacted]17	
19	[redacted]2022168898	921209	52[redacted]99201210615	18786[redacted]24	
20	[redacted]0004512787	741206		15310[redacted]02	
21	[redacted]0031390078	520814	50[redacted]99508141115	13527[redacted]00	赵昌伟
22	[redacted]0007266047	962464	50[redacted]99202157443	18875[redacted]23	
23	[redacted]0022890000	023321	50[redacted]98704273000	15123[redacted]50	
24	[redacted]0005620000	584484	50[redacted]99705258346	15696[redacted]60	孙维维
25	[redacted]0015282549	555666	50[redacted]99804235429	13896[redacted]14	张俊
26	[redacted]0022756725	199612	50[redacted]99612157704	15025[redacted]20	敖美
27	[redacted]0070650838	937016	50[redacted]99307161000	15215[redacted]99	汪黎黎
28	[redacted]0029310000	000619	51[redacted]97206198846	13594[redacted]33	雷先玲
29	[redacted]0004572595	177495	51[redacted]00002111000	15215[redacted]95	罗小芳
30	[redacted]0024755097	888999	50[redacted]98505241973	15823[redacted]38	廖强
31	[redacted]0005852380	675743	50[redacted]9951130252X	15025[redacted]24	郭青晶
32	[redacted]0007685213	987654	50[redacted]98501028000	13983[redacted]45	邬宗尉
33	[redacted]0089243021	199637	50[redacted]99603072303	15723[redacted]04	刘丹
34	[redacted]0101997687	199315		18384[redacted]22	
35	[redacted]0061074121	198203	51[redacted]98203248876	13996[redacted]32	杨世中
36	[redacted]0025142709	909090	51[redacted]99010065000	14708[redacted]18	邹红蓮

继续深挖

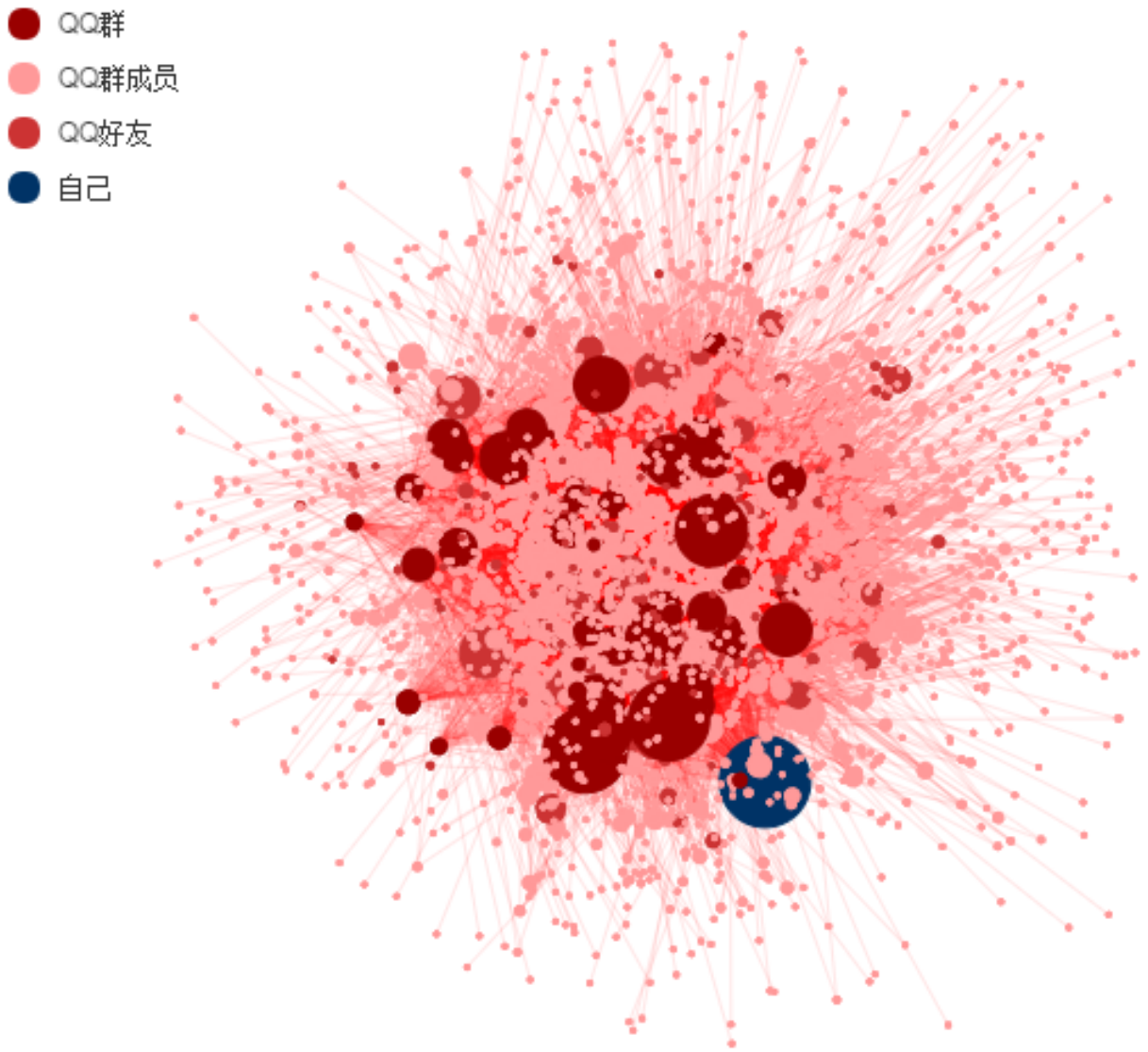
两个IP

- 183.41.0.113----广东省广州市 电信
- 183.41.31.11----广东省广州市 电信

几个QQ

- 2********
- 1********
- 2********

QQ: 2 马赛克



QQ群关系数据分析

志趣相投 TOP 100：（排名越高，说明该成员与当前人员的行业相似度越高）

排名	QQ昵称（QQ号码）	权重
1	狼牙(103376	311
2	坎坎坷坷(202 80)	271
3	鸡飞蛋打(197 82)	261
4	更新中(25472)	241
5	温馨提示(322 66)	231
6	咿呀咿呀(174 05)	211
7	坦克(308008	211
8	钱 途(333950	201
9	真老师(29946)	191
10	寻求给力机(1 398)	191
11	亿百万@诚信 1572016240)	181
12	牛塘村委(134 23)	171
13	马到成功(162 15)	161
14	美好未来(318 27)	161
15	从头开始(331 64)	161
16	财神出(33422)	161
17	辉昂(980769	151
18	好运来(27935)	151

马赛克马赛克马赛克马赛克马赛克马赛

支付密码都是159753　　格式：支付宝|登录密码|支付密码|姓名|身份证号

mimu036824195qe@163.com　|hangou8989|159753|王勇　|422421195012227218

kuijiao277029hzy@163.com　|hangou8989|159753|王勇　|140211195101062715

ld7ieda@163.com　|hangou8989|159753|王文　|410326196512084222

ld638mlm79@163.com　|hangou8989|159753|王文　|410621196406152054

wengji02743612zr@163.com　|hangou8989|159753|陈小华|362421197607274139

分类	创建时间	名称 | 对方 | 交易号	金额 | 明细
	2016-04-19 16:49	alipaynew 合肥飞梅商贸有限公司 | 流水号 2016...602	4750.00
	2016-04-19 16:47	alipaynew 合肥飞梅商贸有限公司 | 流水号 2016...871	4750.00
	2016-04-19 14:03	alipaynew 合肥浮光网络科技有限公司 | 流水号 2016...436	4810.00
	2016-04-19 12:44	alipaynew 合肥浮光网络科技有限公司 | 流水号 2016...658	4810.00
	2016-04-19 12:37	alipaynew 合肥浮光网络科技有限公司 | 流水号 2016...949	4810.00
	2016-04-19 11:31	alipaynew 合肥浮光网络科技有限公司 | 流水号 2016...052	1800.00

2016-03-12 20:39	携程礼品卡（任我行）	携程旅行网 | 流水号 2016...583	5000.00
2016-03-12 10:51	携程礼品卡（任我行）	携程旅行网 | 流水号 2016...773	5000.00
2016-03-12 10:50	携程礼品卡（任我行）	携程旅行网 | 流水号 2016...739	5000.00
2016-03-11 20:07	1号店订单，只为更好的生活(7793612929754)	纽海电子商务（上海）有限公司 | 流水号 2016...943	5000.00
2016-03-11 18:32	1号店订单，只为更好的生活(7792799396754)	纽海电子商务（上海）有限公司 | 流水号 2016...956	5000.00
2016-03-11 18:22	订单号:BJ16031142060098内部编号:43401097	中粮海优（北京）有限公司 | 流水号 2016...872	4900.00
2016-03-11 18:10	携程礼品卡（任我行）	携程旅行网 | 流水号 2016...739	5000.00

单号：2016010410198100 | 2016年01月04日 17:23:42 实际可得：¥ 3500.00

卖卡提交	等待受理	验证卡券	交易成功		
2016-01-04 17:23:42	2016-01-05 00:30:39	2016-01-05 00:30:39	2016-01-05 11:46:40	¥ 3500.00	查看详情

单号：2016010448101102 | 2016年01月04日 14:59:28 实际可得：¥ 3500.00

卖卡提交	等待受理	验证卡券	交易成功		
2016-01-04 14:59:28	2016-01-05 11:41:21	2016-01-05 11:41:21	2016-01-06 09:31:15	¥ 3500.00	查看详情

单号：2016010453515755 | 2016年01月04日 14:59:01 实际可得：¥ 3500.00

卖卡提交	等待受理	验证卡券	交易成功		
2016-01-04 14:59:01	2016-01-05 11:41:20	2016-01-05 11:41:20	2016-01-06 09:31:11	¥ 3500.00	查看详情

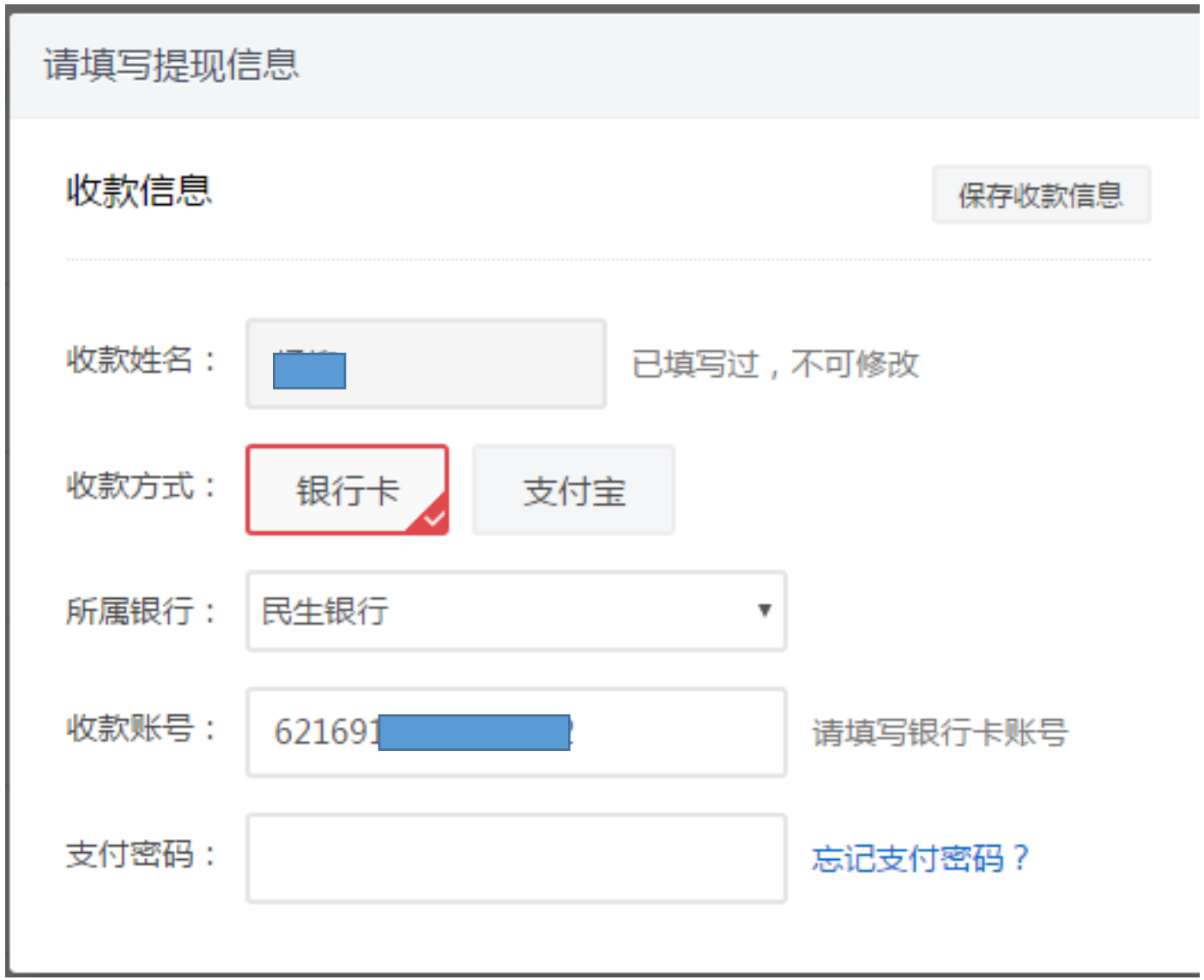
单号：2016010451504899 | 2016年01月04日 14:58:27 实际可得：¥ 3500.

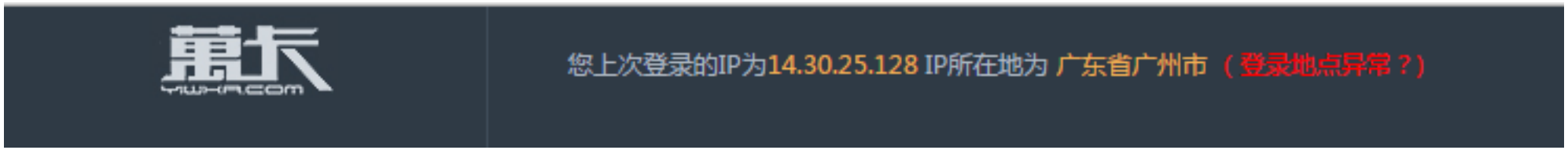
卖卡提交	等待受理	验证卡券	交易成功		
2016-01-04 14:58:27	2016-01-05 11:41:20	2016-01-05 11:41:20	2016-01-06 09:31:01	¥ 3500.00	查看详情

单号：2016010451999952 | 2016年01月04日 14:57:23 实际可得：¥ 3500.

卖卡提交	等待受理	验证卡券	交易成功		
2016-01-04 14:57:23	2016-01-05 11:41:16	2016-01-05 11:41:16	2016-01-06 09:30:57	¥ 3500.00	查看详情

4:25	-14000.00	-	14000.00	转账完成
9:56	-83.00	-	83.00	转账完成
3:16	-3500.00	-	3500.00	转账完成
4:18	-6317.43	-	6317.43	转账完成
3:22	-3500.00	-	3500.00	转账完成
5:16	-1072.00	-	1072.00	转账完成


请填写提现信息
收款信息
保存收款信息
收款姓名：
已填写过，不可修改
收款方式：
银行卡
支付宝
所属银行：
民生银行
收款账号：
621691
请填写银行卡账号
支付密码：
忘记支付密码？


您上次登录的IP为14.30.25.128 IP所在地为 广东省广州市 （登录地点异常？）

提现流水	申请金额	交易金额	账户余额	银行名称	银行账号	开户姓名
T160415113700846	1200元	1200元	99.25元	中国建设银行	**********5058	李瑞栋
T160324112928866	23700元	23700元	15.25元	中国建设银行	**********5058	李瑞栋
T160320112797208	3000元	3000元	33.25元	中国建设银行	**********5058	李瑞栋
T160315112658033	3900元	3900元	96.25元	中国建设银行	**********5058	李瑞栋
T160307112406309	1700元	1700元	4元	中国建设银行	**********5058	李瑞栋
T160305112334067	2500元	2500元	66.75元	中国建设银行	**********5058	李瑞栋
T160116111586288	922元	922元	.25元	中国建设银行	**********5058	李瑞栋
T160113111541688	700元	700元	37.25元	中国建设银行	**********5058	李瑞栋
T160104111402845	600元	600元	73.5元	中国建设银行	**********5058	李瑞栋
T160103111379283	300元	300元	54元	中国建设银行	**********5058	李瑞栋

订单号：001070159 预订日期：2016-01-04 删除订单

携程礼品卡(任我行)	1	常规礼品卡	电子卡	¥5000

订单号：001070085 预订日期：2016-01-04 删除订单

携程礼品卡(任我行)	1	常规礼品卡	电子卡	¥824

订单号：001069927 预订日期：2016-01-04 删除订单

携程礼品卡(任我行)	1	常规礼品卡	电子卡	¥5000

订单号：001069909 预订日期：2016-01-04 删除订单

携程礼品卡(任我行)	1	常规礼品卡	电子卡	¥5000

订单号：001064997 预订日期：2016-01-02 删除订单

携程礼品卡(任我行)	1	常规礼品卡	电子卡	¥5000

您购买的卡密信息如下：

订 单 号:160323210236785019039 20

商品名称:盛付通100元卡

商品单价:100

商品数量:50

订单金额:5000.00

卡密信息:

8013389007909857 92836929

8013389007909858 65145873

8013389007909859 40895462

8013389007909860 10813877

8013389007909861 54719269

8013389007909862 17414361

8013389007909863 71489035

8013389007909864 58255528

8013389007909865 38860261

8013389007909866 90370650

8013389007909867 83822152

8013389007909868 46105490

8013389007909869 20612132

8013389007909870 60563613

8013389007909871 90250892

- 得到了伪基站后台人员的所有信息
- 得到了犯罪链条上下游的所有信息
- 得到了犯罪链条资金的完整流向

事情是不是变的有趣起来？

我想我们是这样的

用领先3年的技术
花4年的时间
做5年后的产品

谢谢大家
微信:Guestt