

基于社交网络的大规模网 络攻击自动对抗技术

成杰峰

geoffcheng@tencent.com

腾讯社交网络BG



QCon 全球软件开发大会
INTERNATIONAL SOFTWARE
DEVELOPMENT CONFERENCE

BEIJING 2017

- 1 互联网安全第一环：恶意帐号
- 3 腾讯恶意帐号智能识别系统
- 3 全量社交网络规模的图计算内幕
- 4 从恶意帐号识别到大规模网络攻击的自动对抗
- 5 恶意库在互联网安全的应用

QCon
全球软件开发大会

主办方 Geekbang > InfoQ
极客邦科技



我是“**网络信息安全建设最佳实践**”专题讲师

腾讯社交网络运营部专家工程师

成杰峰

安全第一环： 恶意帐号

51.8%的全网流量来自于自动机，28.9%为大规模攻击产生的恶意网络流量¹

- 中国是最大的攻击目标/发源国
- 攻击主要受影响的行业：电游,娱乐和社交
- 通过帐号发起的恶意威胁互联网信息安全
- 养号和盗号[fake(sybil)/compromised account]

针对账号的安全制本之道

- 恶意帐号的操控人五花八门
- 恶意帐号的目的各异
- 养号行为无规则和统计特性
- 自动分类无法在大盘准确识别

地区	网络名称	经纬度 (lat)	在网率	LAT
浙江省杭州市电信-1001	Sk	30°	支持	
浙江省宁波市电信-1002	Sk	29°	支持	
中国网通联合网络-1003	Sk	10°	支持	
山东省潍坊市联通-1005	Sk	31°	支持	
浙江省嘉兴市电信-1006	Sk	空网	支持	
山东省滨州市电信-1009	Sk	34°	支持	
河北省石家庄市联通-1010	Sk	26°	支持	
浙江省丽水市电信-1011	Sk	空网	支持	
辽宁省盘锦市电信-1015	Sk	30°	支持	
浙江省杭州市电信-1015	Sk	30°	支持	
浙江省杭州市-1016	Sk	30°	支持	
四川省资阳市电信-1017	Sk	27°	支持	
四川省电信1002成都-1024	Sk	16°	支持	
上海市电信-1025	Sk	29°	支持	
四川省绵阳市-1027	Sk	12°	支持	
北京网通-1029	Sk	32°	支持	
黑龙江省大庆市联通-1031	Sk	32°	支持	
黑龙江省哈尔滨市-1033	Sk	空网	支持	

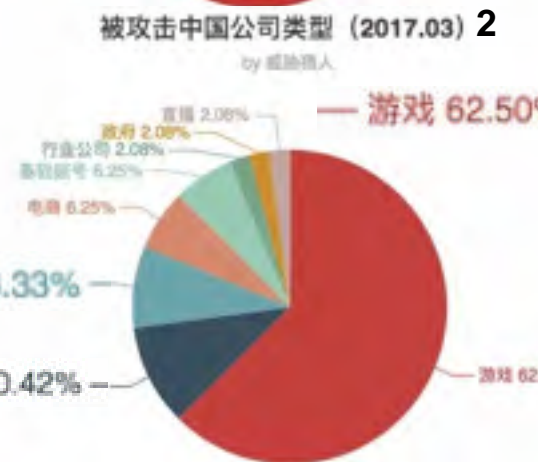
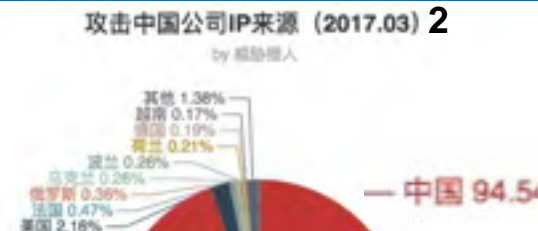
小黑科技代刷价格表
招收代理66/一位绑定QQ号

- 说说赞 : 8 /一千赞【代理价:5.5】
- QQ名片赞: 10/一万赞【代理价:8/】
- 空间访客: 20/十万访客【代理价:1】
- 快手粉丝: 20/一千粉丝【代理价:】
- QQ购物号: 15/一个【代理10/一个】

小黑秒赞平台价格
招收代理20/一位

秒赞平台地址: [http://www.kp.cn](#)

- 月卡.4块【代理价:2块】
- 季卡.12块【代理价:8块】



- 四川省绵阳市-1027
- 北京网通-1029
- 黑龙江省大庆市联通-1031
- 黑龙江省哈尔滨市-1033

1 Bot Traffic Report 2016
2 <http://www.cebnet.com.cn/20170407/102380792.html>

腾讯恶意帐号智能识别和安全服务



祝融安全系统



静态养号做种在海量请求流水数据中聚类扩展
计算大盘中的活跃养号



基于团伙标签的
安全服务策略

按业务逻辑定制
打击和监控策略



恶意、可疑和温和的
团伙类别

机器学习分类模型
自动分类识别

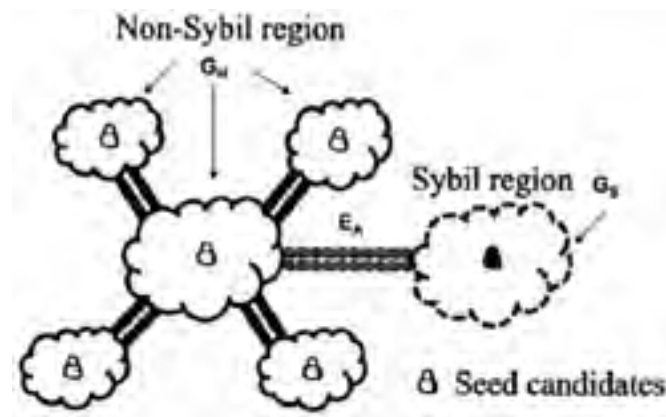


大批活跃养号团伙

挖掘静态养号账户：基于网络SybilRank打分¹的图挖掘方案：I-图聚类；II-算打分；III-选养号

- 关系链图有18亿个顶点,495亿条边，目前最先进的可扩展图聚类pSCAN²也仅能处理4千万个顶点，12亿条边的大图
- SybilRank使用的是基于社区模度的图聚类方法³，其最好扩展版本⁴能处理1亿个顶点，37亿条边

高可扩展性图处理



1 Xiaowei Yang, and Tiago Pogueiro: Aiding the detection of fake accounts in large scale social online services, In NSDI, 2012.

2 Lijun Chang et al.: pSCAN: Fast and exact structural graph clustering, In ICDE, 2016.

3 Vincent D. Blondel et al.: Fast unfolding of communities in large networks, In J. Stat. Mech., 2008.

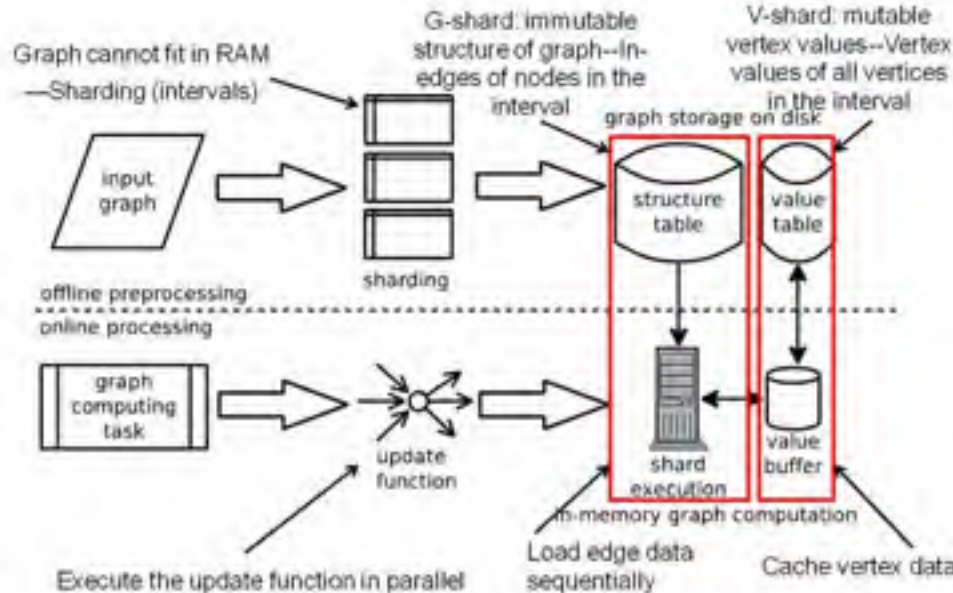
4 Hiroaki Shiokawa et al.: Fast algorithm for modularity-based graph clustering, In AAAI., 2013.

图数据之间彼此互连，依赖性强；平台专业性强

- MapReduce和Spark等主流大数据平台并不适合
- 图计算平台成为了图挖掘和相关机器学习算法的新方法
- 用顶点程序 (equiv. Map/Reduce)达到自动化分布并行平台独立
- 分布式内存图计算 vs 磁盘图计算
- **Jiefeng Cheng**, Qin Liu, Zhenguo Li, et al. VENUS: Vertex-Centric Streamlined Graph Computation on a Single PC. In ICDE, 2015.



磁盘图计算系统VENUS



分布式 vs 磁盘

VENUS vs Spark: PageRank on Twitter (41M 顶点, 1.4B 边)

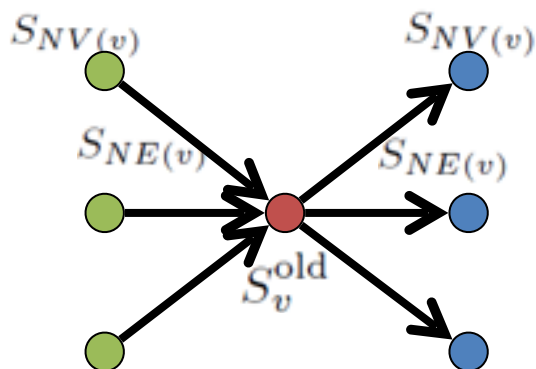
system	resource	speed
Spark	50 servers, 100 CPU	8.1minutes
VENUS	1 PC, 8CPU, hard disk	5minutes

VENUS vs GraphChi: PageRank on clue-web (1B 顶点, 43B 边)

GraphChi	X-Stream	VENUS
4.3hours	7.4hours	1.8hours

顶点程序

$$S_v^{new} = \text{VertexUpdate}(S_v^{old}, S_{NV}(v), S_{NE}(v)).$$



高可扩展性图聚类

Fast unfolding算法的图计算实现

- 以模块度最大化的目标把社交网络分成多个社区
- 模块度 = 各社区内总边数 - 各社区内随机应有的边数

$$Q = \frac{1}{2m} \sum_{i,j} [A_{ij} - \frac{k_i k_j}{2m}] \delta(c_i, c_j)$$
$$\delta(c_i, c_j) = \begin{cases} 1 & \text{when } c_i = c_j \\ 0 & \text{else} \end{cases}$$

所有边的权重之和

顶点i和j之间边的权重

与顶点j相连的边的权重之和

- (i)初始化(ii)按模块度增益调整每个顶点v至相邻社区，重复直到所有顶点的所属社区不再变化(iii)压缩同一个社区所有顶点成一个顶点并重复前一步直到模块度收敛

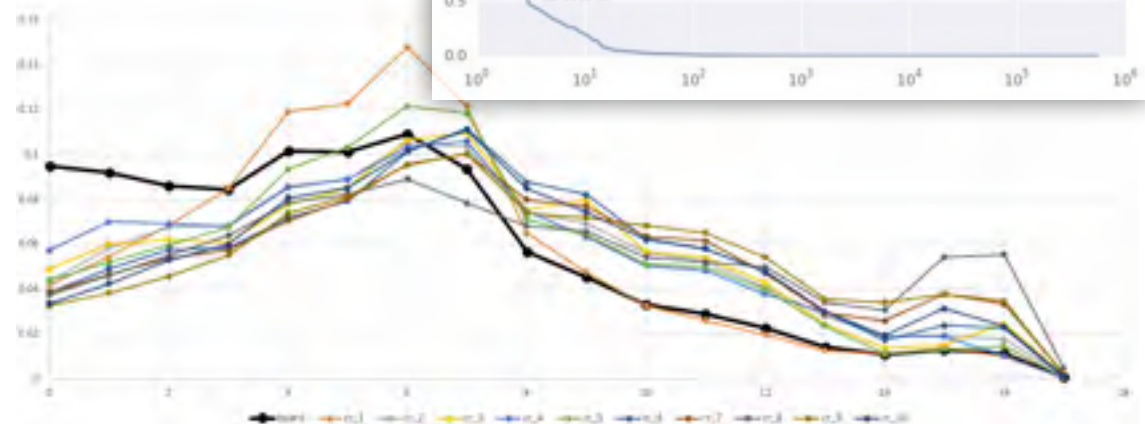
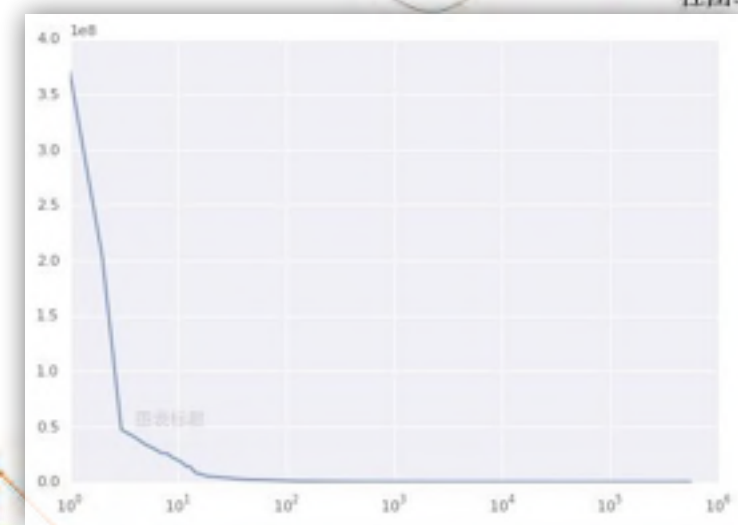
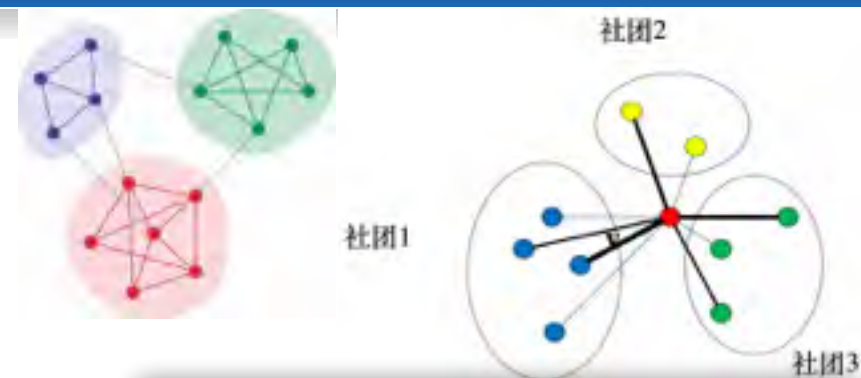
模块度增益

$$\Delta Q = \frac{k_v [C]}{2m} - \frac{k_v \sum_{tot}^C}{2m^2}$$

社区C与顶点v相连的边的权重之和

社区C的边的权重之和

- 图计算中的顶点状态是每个顶点所属社区，维护一个全局字典 \sum_{tot}^C
- 顶点程序收集 $k_v [C]$ ，并对每个相邻社区计算模块度增益
- 耗时119小时，3.1千万个社区，前3大社区大小分别为3.7亿、2亿、4.7千万，两大社区30%的顶点，2万个连通分量，最大18.8亿，3.9万微连通分量孤立号码
- 社区大小和对应的社区满足power-law分布



高可扩展性SybilRank计算

对图聚类发现的每个社区选出一个白种子（好人）

- 基于业务数据：投诉、异常登录、打击历史等

SybilRank 算法图计算实现

- 图计算中的顶点状态是每个顶点的SybilRank打分

$$T^{(0)}(v) = \begin{cases} \frac{T_G}{S} & v \text{ 是白种子} \\ 0 & v \text{ 不是白种子} \end{cases}$$

$$T^{(i)}(v) = \sum_{(u,v) \in E} w_{(u,v)} \frac{T^{(i-1)}(u)}{k_u}$$

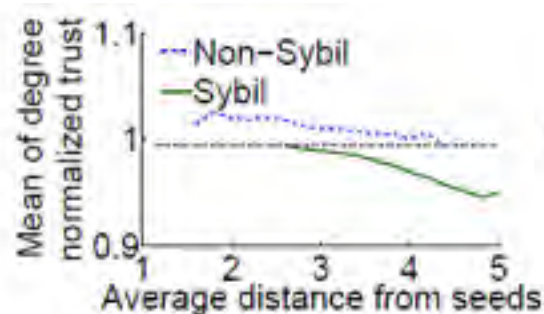
给定图中分值的总和
 图中白种子的个数
 第*i-1*次迭代中u的打分
u的邻边的权重之和
v和u间的边的权

- (i)初始化(ii)根据顶点状态和边的权值更新状态(iii)计算 $O(\log(|V|))$ 次迭代
- 需时62.65个小时

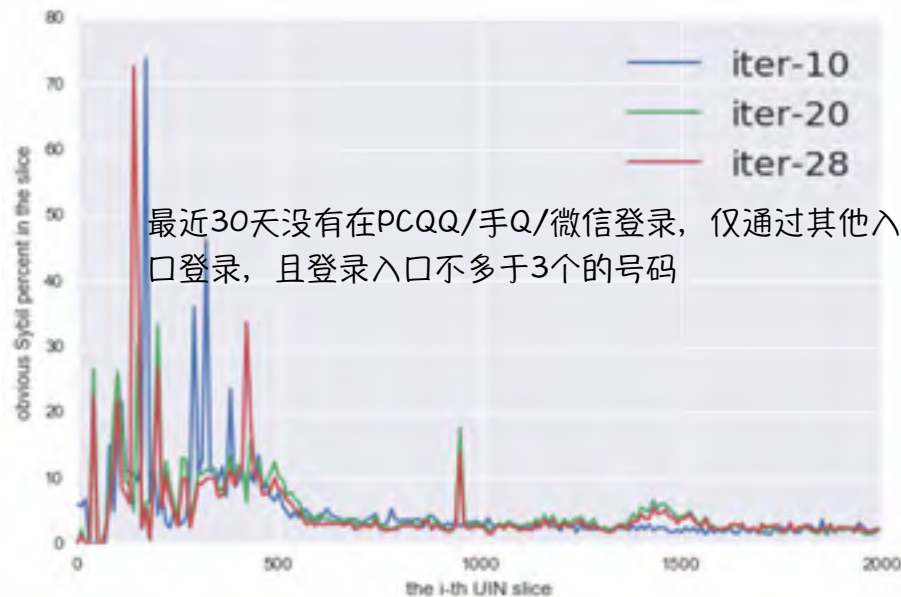
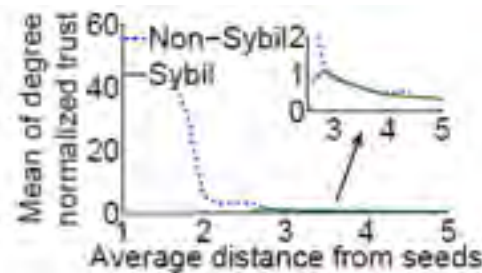
用打分排名划分出的高可信养号区

- 分析排名靠前的号码，使用登录入口行为异常，设备聚集等几个条件辅助判断出高可信养号区，号码量在1千万左右
- 静态养号：针对在线活跃攻击的覆盖率很低

理想



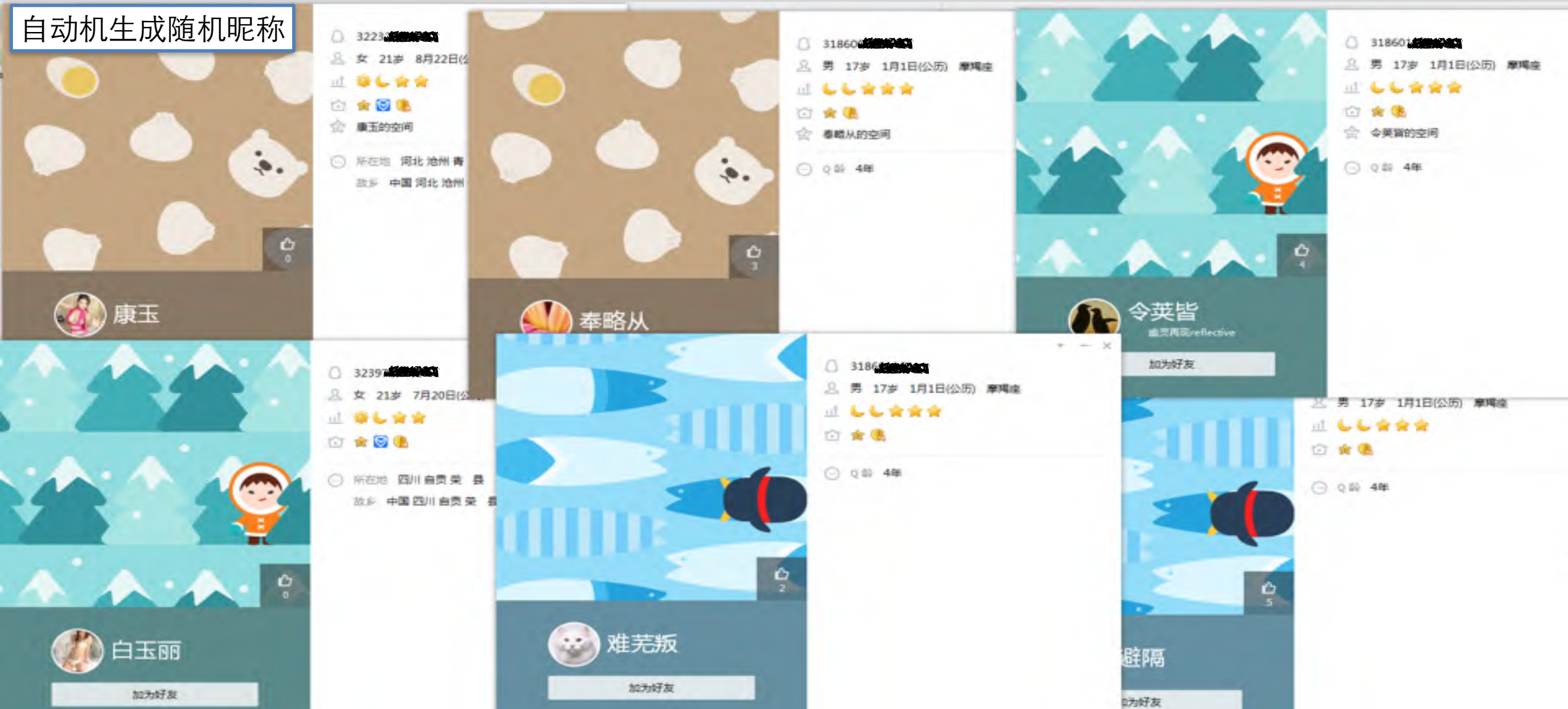
实际



最近30天没有在PCQQ/手Q/微信登录，仅通过其他入口登录，且登录入口不多于3个的号码

静态养号典型案例

自动机生成随机昵称



静态养号典型案例

登录IP上有聚集

A23	底片	1502339626						
	A	B	C	D	E	F	G	H
15	1283368567	0.006914	1.32E+08	17	167 6790, 330	0eaa, 1	16	[21125111, 12, 13
16	1286209741	0.005974	2.2E+08	15	167 743f, 1		16	[21000111, 12, 13
17	1463391430	0.006806	2.43E+08	12	167 6d01, 444	e5f5, 1	16	[21125111, 12, 13
					167 e618, 438	0522, 1	16	[21125111, 12, 13,
					167 4db3, 358	c993, 1	16	[21125111, 12, 13,
					167 e618, 438	45c9, 1	16	[21125111, 12, 13,
					167 4db3, 358	d358, 1	16	[21125111, 12, 13,
					167 e94b, 380	2674, 1	16	[21125111, 12, 13,
					167 2a11, 488	16f4, 1	16	[21125111, 12, 13,
					167 d4af, 385	8eb3, 1	16	[21125111, 12, 13,
					167 1f32, 257	884e, 1	16	[21125111, 12, 13,
					167 b6f6, 433	a4af, 1	16	[21125111, 12, 13,
					167 3f7e, 470	ac25, 1	16	[21125111, 12, 13,
					167 e3de, 379	98b6, 1	16	[21125111, 12, 13,
					167 b7fe, 337	2bda, 1	16	[21125111, 12, 13,
					167 38d4, 443	1249, 1	16	[21125111, 12, 13,
					167 5efc, 401	7352, 1	16	[21125111, 12, 13,
					167 d4af, 385	fc57, 1	16	[21125111, 12, 13,
					167 7992, 341	8d71, 1	16	[21125111, 12, 13,
					167 10fe, 232	d0a7, 1	16	[21125111, 12, 13,
					167 5c8d, 430	1267, 1	16	[21125111, 12, 13,
					167 0fef, 439	cb3d, 1	16	[21125111, 12, 13,
					167 0fef, 439	f7f9, 1	16	[21125111, 12, 13,
					167 b6f6, 433	c028, 1	16	[21125111, 12, 13,
					167 3a37, 462	e2fa, 1	16	[21125111, 12, 13,
					167 21f9, 371	bf4b, 1	16	[21125111, 12, 13,
					167 2ea2, 468	2019, 1	16	[21125111, 12, 13,
					167 9406, 381	8da7, 1	16	[21125111, 12, 13,
					167 44c2, 443	b936, 1	16	[21125111, 12, 13,
					167 85be, 339	3b1d, 1	16	[21125111, 12, 13,
					167 4eb3, 342	61d5, 1	16	[21125111, 12, 13,
					167 5c8d, 430	dede, 1	16	[21125111, 12, 13,
					167 c7a2, 402	f7e0, 1	16	[21125111, 12, 13,
					167 e618, 438	d1ce, 1	16	[21125111, 12, 13,
					167 44c2, 443	1f16, 1	16	[21125111, 12, 13,
					167 e94b, 380	9543, 1	16	[21125111, 12, 13,
49	1970517089	0.00682	1.03E+08	14			-1	-1
50	1972048661	0.006891	3.25E+08	12			1	4
							1	4
							1	4
							-1	-1
							-1	-1
							1	4
							-1	-1

nil
6790, 330 | 0eaa, 1
7d3f, 1
6d01, 444 | e5f5, 1
e618, 438 | 0522, 1
4db3, 358 | c993, 1
e618, 438 | 45c9, 1
4db3, 358 | d358, 1
e94b, 380 | 2674, 1
2a11, 488 | 16f4, 1

The screenshot shows a search interface with a search bar containing the ID '1502339626'. Below the search bar, there are filters for location (广东, 深圳) and gender (女). The search results show a profile for a user named 'qh' (1502339626) with a profile picture of a bird. The profile information includes '女 41岁 8月8日(农历) 狮子座'. There are several social media icons and a '加好友' (Add Friend) button.

静态养号典型案例

大量不同虚假公司名

uin	score	vid	degree	城市	登录入口	hashes
227331	0.41774	52361367	33	366 367	3f2d, 5	16
10574	0.417713	198522283	603	358	8a77, 3 00b5, 2 be9c, 3	1 16
27212	0.417739	297731159	144	354	1007, 5	1
12198	0.417712	161454275	607	353	96c4, 2 5b88, 3	1 16
28485	0.417733	164152638	311	353	f4f2, 4	1
3769	0.417747	97666292	446	353	76d4, 10	1
7050	0.417725	46638621	487	353	d8dc, 6	16

查找

找人 | 找群 | 找主播 | 找课程

227331

所在地: 中国, 广东, 深圳 | 故乡: 中国 | 性别 | 年龄 | 摄像头

返回 搜索: 2273317662

找到 1 个人

新疆金桥旅游2 (227331)

新疆 乌鲁木齐

+ 好友

新疆金桥旅游2

新疆金桥旅游2的空间

所在地 新疆 乌鲁木齐

邮箱 xjcui@xia@sina.com

Q龄 5年

学校 新疆职业大学旅游系

所在地 新疆 乌鲁木齐

邮箱 xjcui@xia@sina.com

Q龄 5年

学校 新疆职业大学旅游系

静态养号典型案例

利用已经失效的公司的号码



+色群【589054527】倒国飞嫉显咽您 (3001089259)

+ 好友



3001089259

习惯了曾经
公司职员 | 铂域网络

静态养号典型案例

不再活跃的商业号码



健康在线咨询 (3001769751)
福建 福州
+ 好友



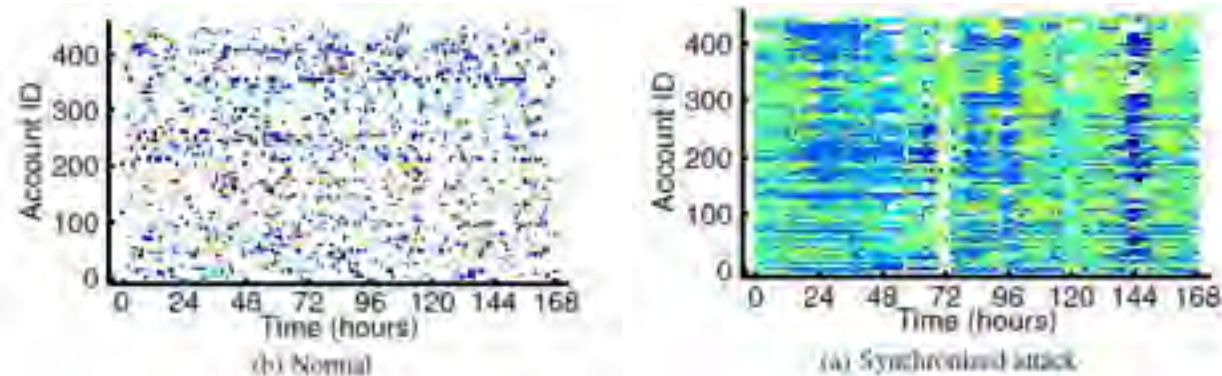
3001769751

健康在线咨询
公司职员 | 金麦网络

从静态养号到活跃养号团伙

恶意批量行为和养号团伙识别

- 批量协同的大规模恶意通常具有爆发和分布特征
- 具有反复批量相似行为的养号群组形成团伙
- 帐号两两相似度计算：密集/反复性请求产生的噪音和有效时间窗产生的重复



静态养号做种在海量请求流水数据中聚类

- 可计算性：

$$O(|V|^2) \rightarrow O(|V|)$$
- 健壮性：仅养号容易具有长时间反复批量相似行为 (含盗养号)
- 可运营性：一天业务总请求量~500亿，用1个入口5天的登录请求(~2亿)可匹配出700亿对相似养号用户

基于登录请求可自动识别~2000万的活跃养号

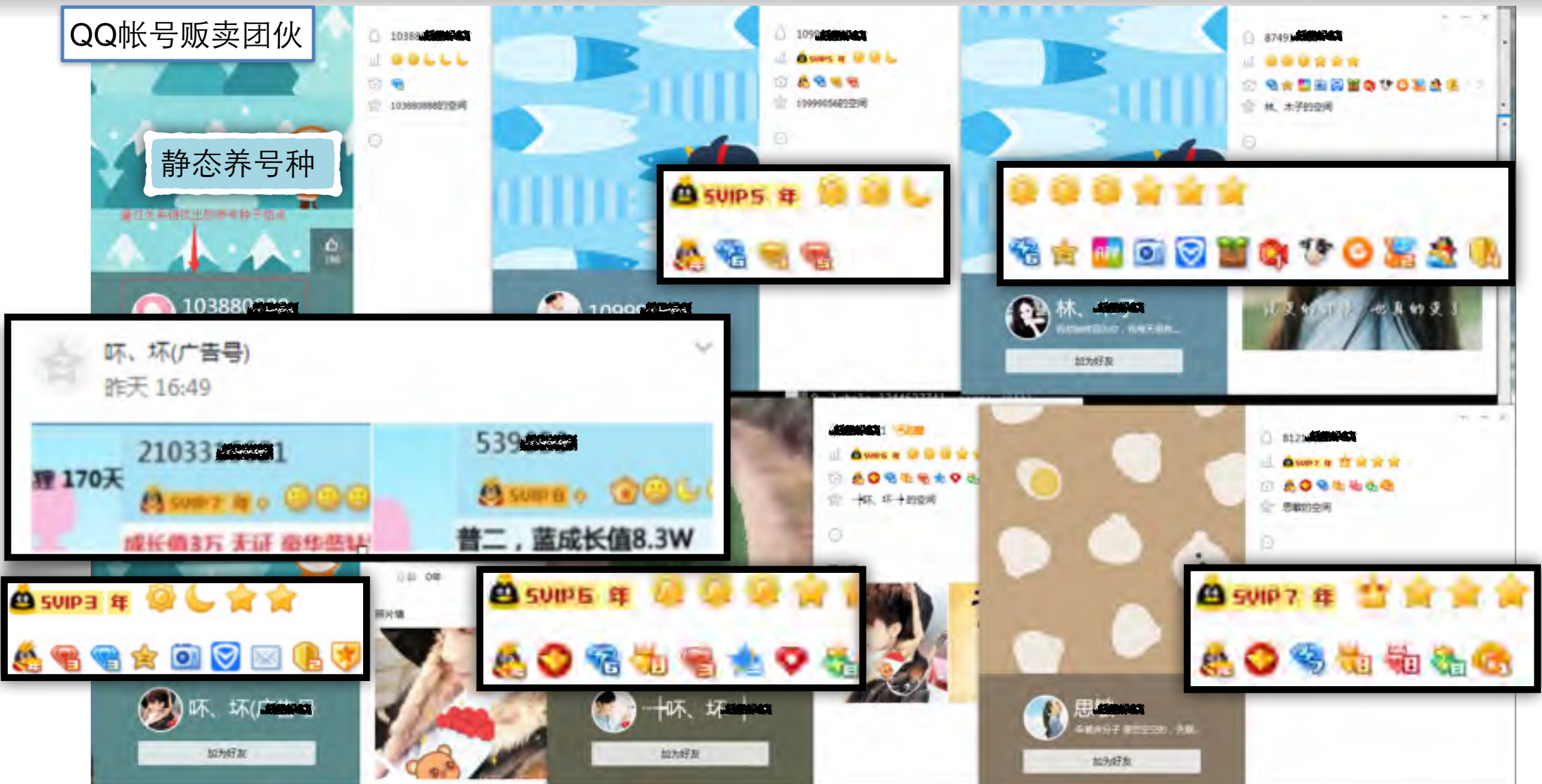
- 团伙大小大致分布：
 >1000 ~40%
 >500 ~30%
 其余 ~30%

login_apid	uin	inp_detc
21000501	0164	20170207143805
21000501	0065	20170207143857
21000501	00119	20170207143430
21000501	03513	20170207144850
21000501	02740	20170207145428
21000501	02388	20170207144542
21000501	01206	20170207143130
21000501	00521	20170207140967
21000501	02000	20170207143704
21000501	04075	20170207140224
21000501	00738	20170207144213
21000501	00702	20170207144220
21000501	00731	20170207142011
21000501	03744	20170207145530
21000501	03521	20170207145020
21000501	02656	20170207140124
21000501	00126	20170207143809
21000501	01580	20170207144443
21000501	03436	20170207145046
21000501	03543	20170207150056
21000501	04143	20170207151270

活跃养号团伙典型案例

QQ帐号贩卖团伙

静态养号种

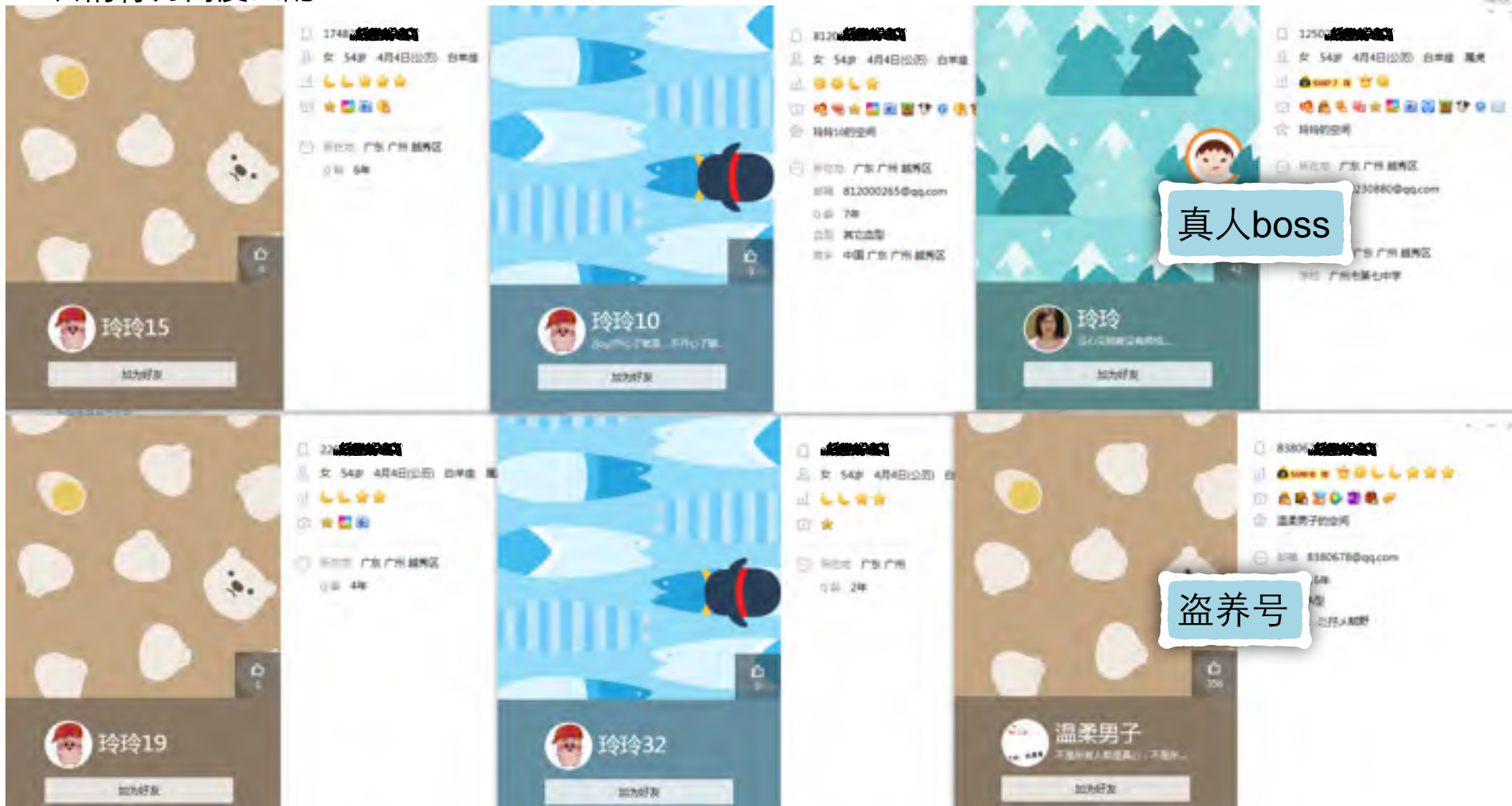


活跃养号团伙典型案例

玲玲 + 数字 只在同一IP登录，无其它请求

每个团伙通常有真人boss

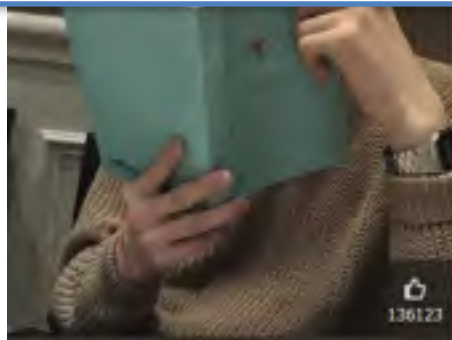
包含盗养号（标黄），有加群、群消息、好友消息产生，但是在该登录入口的行为高度匹配



10	549000912	18190
11	549000912	25440
12	549000912	10130
13	549000912	33214
14	549000912	17395
15	549000912	25039
16	549000912	29417
17	549000912	12533
18	549000912	9067
19	549000912	16935
20	549000912	26467
21	549000912	4
22	549000912	781
23	549000912	1
24	549000912	17479
25	549000912	83
26	549000912	8120
27	549000912	10656
28	549000912	14294
29	549000912	17520
30	549000912	15820
31	549000912	26539
32	549000912	17482
33	549000912	22699
34	549000912	32327
35	549000912	24717
36	549000912	22891

活跃养号团伙典型案例

一群会说故事的nice养号团伙？



故事君
得之我幸 失之我命



微故事
宝贝们请设置我力 特别关心...

加为好友

20岁 9月26日(农历) 天秤座
故事君 的空间
所在地 台湾 台北市
Q龄 17年

407724
男 19岁 1月1日(农历) 摩羯座
微故事的空间
所在地 奥地利
Q龄 16年

照片墙

"该玩的年纪 却动了情"



微故事 女孩大学毕业了，要到很远的一座城市去，四个同时暗恋她的男生一起送她。女孩知道，这一去恐怕再也与他们无缘了。
火车就要启动的时候，四个男孩似乎都想说什么，女孩笑着问：“你们是不是舍不得我离开啊？真舍不得就跟我走呀！”
四个男孩神情茫然，一时都不知如何是好。
就在车门快要关闭的时候，其中一位男孩飞奔跃上了火车，冲到女孩的座位上，把她紧紧地抱在怀里。
女孩没有拒绝，她靠在男孩的肩头，泪水滴湿了她的衣领。
站台上的三个男生一下子愣愣得目瞪口呆，还没有他们做出任何反应，火车就“咔嚓咔嚓”地驶出了站台。
一年后，另一座城市，在女孩的婚礼上，其他的三个男孩问女孩：“你是什么时候决定嫁给他？”
女孩说：“就在他奋不顾身跃上火车的那一刻。”
女孩问：“那时候，你们怎么不想我走呀？”
“我还以为你在开玩笑呢！”一个男孩说。

撩妹成癮

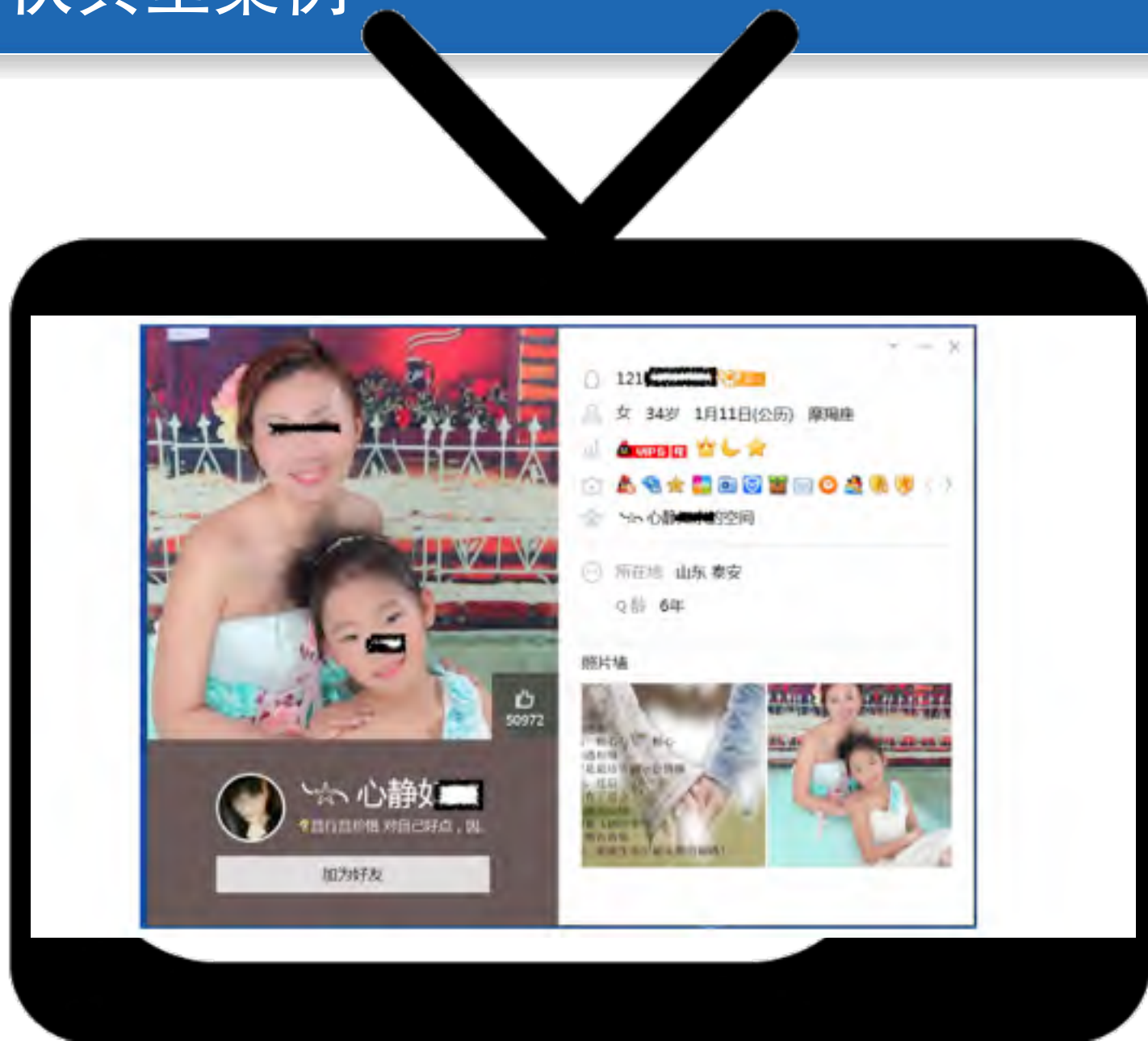
45511
男 1岁 1月6日(农历) 摩羯座
套路王的空间
Q龄 16年

套路王
自古深情解不住，总是套路得...

加为好友

活跃养号团伙典型案例

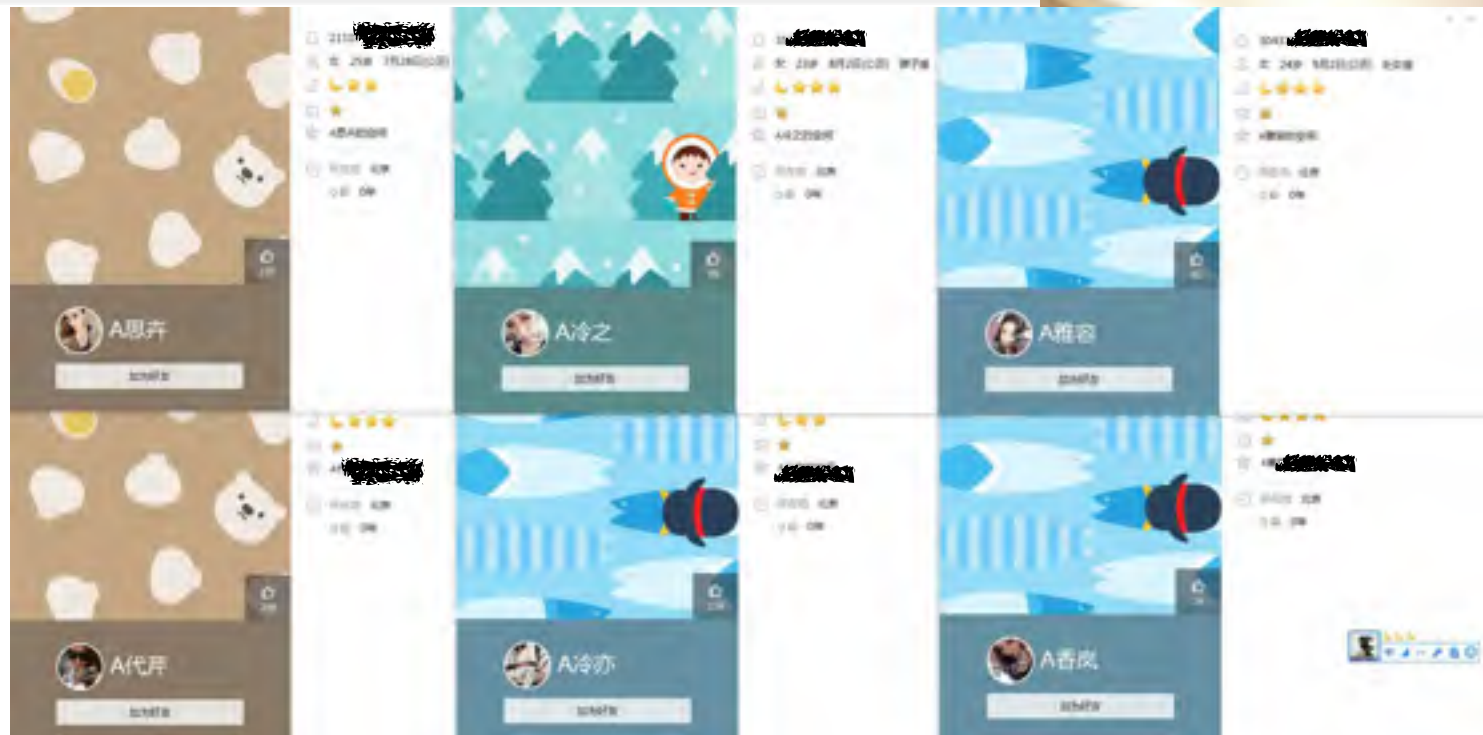
盗养号团伙



基于恶意帐号识别的恶意自动对抗

从养号作恶分类到团伙标签

- 柔性治理：好人偶然违例 vs 坏人严肃处理
- 养号作恶种类
- 安全中机器学习难题的解决方案
 - ☉ 业务中的发现的养号：样本自动提取
 - ☉ OCR图像识别难题的化解
 - ☉ 恶意URL识别难题的化解



按业务逻辑定制
打击和监控策略

基于团伙类别的各
类安全策略

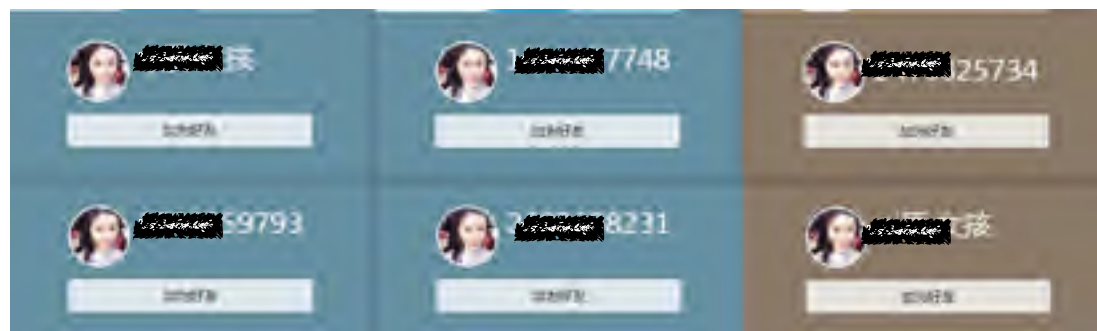


恶意、可疑和温和的
团伙类别

机器学习分类
模型自动分类



大批活跃养号团伙





天御系统



END