业务安全 之防守者说

Aboutr Me

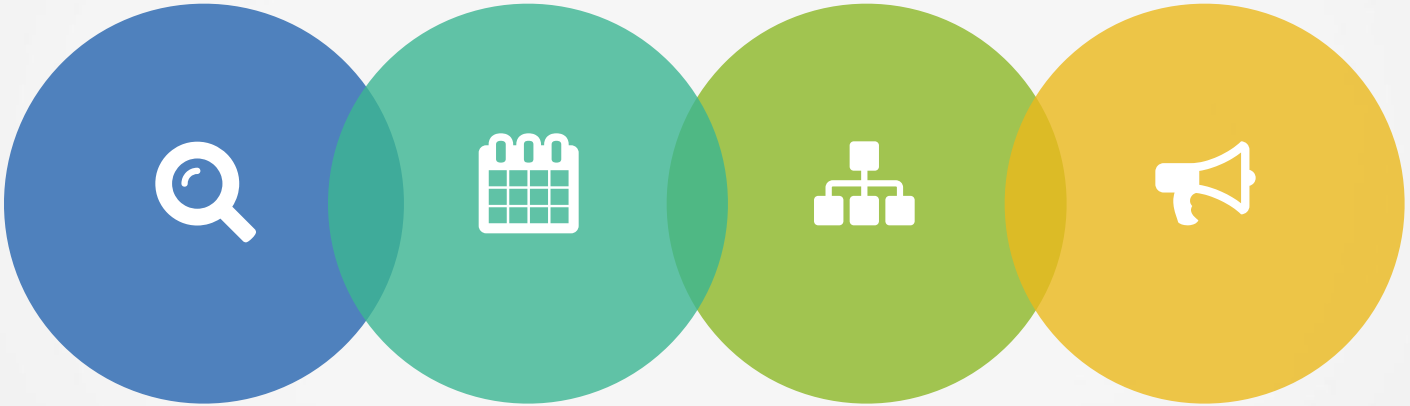
网络安全

咨询服务
产品

数据安全
反欺诈

信息安全
反欺诈

风险点



账户　交易　支付　信用

帐户安全：垃圾注册/盗帐户/撞库

百度帐号批量注册软件

金兰知道账号注册机

美丽说账号注册工具

小米账号全自动注册机

4399注册机下载(4399账号注册软件)

京东账号注册软件

这是一门生意：

骚扰其他用户/广告/虚假交易/套利/贩卖。。。

垃圾注册对抗之路

防御手段	对抗技术	深度技术
IP限制	代理	代理IP库、高危IP库、各种云服务器、爬虫、IDC、反向探测
验证码	打码平台	低层次防御
手机验证码	收码平台、阿里小号	爬与反爬、授权验证、数据合作验证、电话验证
设备指纹	模拟器、虚机、一键变换	模拟器特征识别、虚机特征识别、算法与规则
人机识别	分布式人工	速度、轨迹、轻重
账号算法	？	账号名好坏算法

IP识别

爬取代理IP

国内高匿代理IP

国家	代理IP地址	端口	代理位置	是否匿名	类型	验证时间
	61.130.97.212	8099	浙江宁波	高匿	HTTP	14分钟前
	202.103.190.102	80	广东深圳	高匿	HTTPS	14分钟前
	58.30.233.198	8080	北京	高匿	HTTPS	15分钟前
	119.187.148.35	80	山东东营	高匿	HTTP	15分钟前
	183.218.63.179	8118	江西上饶	高匿	HTTP	15分钟前
	117.136.234.1	80	移动	高匿	HTTP	16分钟前
	117.136.234.8	80	移动	高匿	HTTP	1小时前
	218.89.170.114	8888	四川攀枝花	高匿	HTTP	1小时前
	124.240.187.89	80	河南濮阳	高匿	HTTP	1小时前
	183.218.63.174	8118	江西上饶	高匿	HTTP	1小时前
	117.136.234.3	80	移动	高匿	HTTP	1小时前
	120.198.245.36	8080	移动	高匿	HTTP	1小时前
	182.254.153.54	80	广东深圳	高匿	HTTP	1小时前
	183.207.228.11	86	移动	高匿	HTTP	1小时前
	222.39.112.12	8118	内蒙古兴安盟乌兰浩特	高匿	HTTP	1小时前
	123.56.134.65	8080	河北石家庄	高匿	HTTP	1小时前
	113.215.0.130	80		高匿	HTTP	1小时前
	117.136.234.5	80	移动	高匿	HTTP	1小时前
	117.136.234.12	80	移动	高匿	HTTP	1小时前
	183.207.128.47	80	移动	高匿	HTTPS	1小时前

爬不全

高危IP

业务数据：实时业务产生；

高危地区：泉州、广西部分地区、儋（dan）州、东南亚巴西俄罗斯

数据不适用
恶化速度快

IDC类收集

服务器段IP注册

典型各类云

僵尸IP，从广告欺诈延伸到羊毛党

反向探测

对端是否开启80等服务端口 100%

X-Forwarded-For 100%

HTTP源端口>10000 匿名代理或大型机构出口 50%

Keep-alive 可能为代理或HTTP1.0 50%

准、覆盖面不够

手机验证码抗之路

爬取收码平台手机号

爬不全
不定期换

授权验证

运营商不统一
时间慢、隐私
对抗与合作

合作数据验证

隐私
费用

电话验证

+电话回拨，通告验证码

费用
大规模电话通告

人脸识别

费用
公安部
识别率
重

设备指纹

基站定位[20487,21978,-1]
ISO标准国家码cn
电话状态1
移动网络码CMCC
设备软件版本号01
SIM串号序列号898600
IMSI460026600748623
电话号码-
国际身份码359092052927724
UDID
设备名称ha3g
ROM编号名称JSS15J.N900XXUCMK2
手机型号SM-N900
销往地ha3gxx
CPU类型3
CPU速度1590.88
CPU硬件UNIVERSAL5420
CPU序列号476980ef4d00b906
屏幕分辨率1080x1920
存储空间17.17 GB
设备配置ConfigurationInfo{4363f
音乐哈希15273db1383ea08a52b9713
wifi mac地址D0:22:BE:5D:6F:21

dd73724f9010781a5b0e66f62abe4018

同一设备不同账号登录
同一账号不同设备登陆
设备与注册手机号不符
同设备多帐户
同设备高频率注册
历史作案记录
....

安卓模拟器

安卓模拟器软件排行榜 太平洋下载

软件名
1 靠谱助手(安卓模拟器) 3.6.2289 官方版
2 BlueStacks(安卓模拟器) 0.9.31.4259 ...
3 Droid4X(海马玩模拟器) 0.8.4 官方版
4 夜神安卓模拟器 2.2.0.0
5 天天安卓模拟器 1.2.1025

特征匹配

设备指纹

设备信息修改软件

虚拟机对抗

虚拟机网卡 000569 000c29 005056开头

USB和声卡

时钟异常

IP包编号自动随机并存

VM特征 内存 进程 服务 注册表

。。。

算法与规则

GPS与IP不匹配
移动距离异常
黑名单命中
设备环境无法获取
....

1、没有绕不过的算法
2、犯罪分子地域化，更换设备零部件

人机识别与坏帐户

人机识别

键盘敲击频率

鼠标移动速度及轨迹

点击位置偏好

屏幕触摸压力

屏幕签名

心理技术识别

。。。

坏帐户

GOOD：

重帐户

帐户名有意义

存活周期长

账户有关联朋友

实名且具备相关个人信息

BAD：

新帐户

轻帐户

无关系圈

个人信息虚假

邮箱账号是否真实存在

是否有过网络痕迹

是否活跃

机器学习

比如；

Fraud001@126.com被标记为欺诈

那么

Fraud002@126.com

Fraud003@126.com

交易安全

实名

订单泄露

刷单

实名

实名身份

身份证号码与姓名

身份证图片

银行绑卡

人脸识别

1、收购身份证办银行卡、手机卡
2、边缘地区小银行有内外勾结嫌疑

- 行业黑名单共享
- 地下情报收集

实名


新闻 网页 贴吧 知道 音乐 图片 视频 地图 百科 文库
Bai图片
身份证
百度一下
图片筛选
相关搜索： 身份证大全号码 身份证正反面清晰照 身份证大全号 静静身份证 身份证号码 身份证号 身份证正反面清晰 身份证正反面 身份证样本
韩呈祥
男 汉
1988 年 3 月 15 日
山东省淄博市张店区中埠镇铁冶村1组65号
公民身份号码 370303198803156013
金海
1981 年 11 月 27 日
公民身份号码 511225198111274834
中华人民共和国
居民身份证
孔令宇
男 汉
1985 年 12 月 11 日
江苏省江都市扬南路25号501
公民身份号码 321088198301304871
姜璐
男 汉
1982 年 12 月 18 日
辽宁省大连市甘井子区海
滨路607号1-4-4
公民身份号码 210211198212181 41X
张正韬
1977 年 9 月 11 日

订单泄露

订单泄露是个综合治理工程，每个泄漏点都是一个大课题

信用

盗卡

贷款

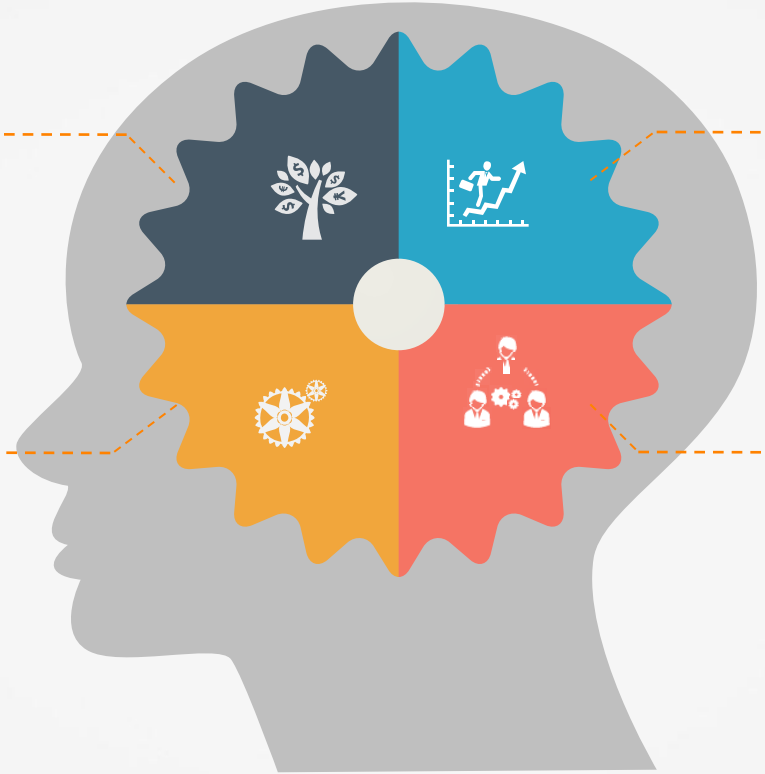
盗刷前一笔在干吗？

时差分布

- **小结论：**
- **坏人呈现出上班时段，偏向职业化，周末有小幅下降；**
- **交易后几小时内发生诈骗；**
- **盗刷基本在24小时内完成；**

信息泄露是罪魁祸首！

对抗



订单

订单金额
注册邮箱
注册地址
物流地址
...

卡信息

卡号
开卡日期
发卡日期
账单地址
风险值
...

设备信息

IP
浏览轨迹
手机
可信设备
关系网络
...

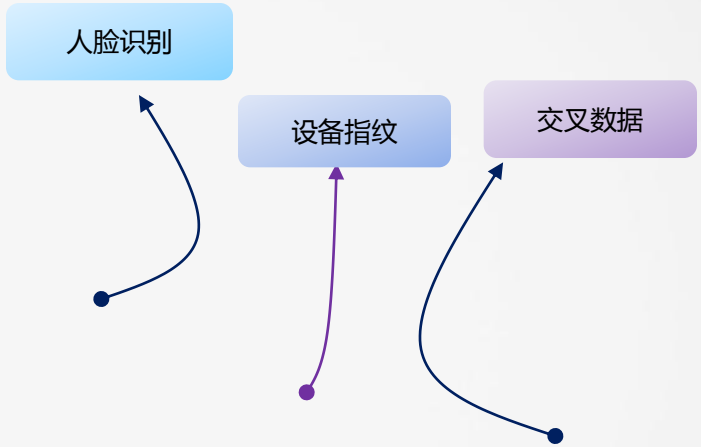
数据验证

各类黑名单库
风险模型
风险系数
信用记录
人工review
....

贷款

欺诈风险

- 虚假借款
- 异常提现
- 黑中介
- 洗钱



总结

- 内忧
  - 攻防成本
  - 大公司的内部合作
  - 内外勾结，尤其是外包

- 外患
  - 游击队VS合成旅
  - NO DATA NO BB，貌合神离的各类合作组织

- OTHER
  - 情报组、爬虫组、重案组、政委下连队、联席作战
  - 数据狂：宽表、关系网络
  - 联防：黑手机、高危身份证、黑名单、多头贷款、黑卡

THANK U