

唯品会
vip.com



唯品会安全应急响应中心
VIP Security Response Center

2016唯品会互联网电商安全峰会

电商安全的闭环

电商安全体系建设的血与泪

REVEALING

Road to User Analysis System Construction



电商安全

撞库

马甲

信息泄漏

刷购物车

刷单

刷券

入侵

爬虫



第一次 尝试



日志

NGINX

消息源

kafka

处理计算

APACHE
STORM™
Distributed · Resilient · Real-time

结果存储

cassandra

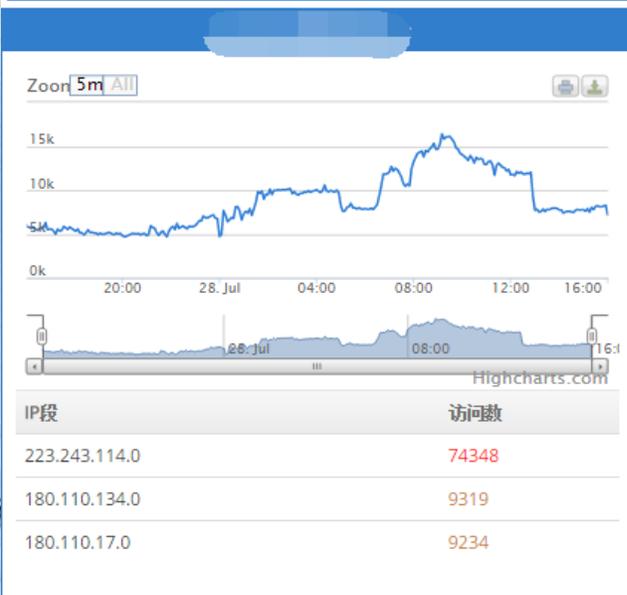
MySQL™



IP_ABC段	次数
115.220.2.0	13668
115.203.77.0	12584
115.203.69.0	12542
115.216.193.0	12538
115.202.176.0	12480
115.203.85.0	12425
115.203.93.0	11311
115.202.162.0	11299
115.203.87.0	11273
60.162.157.0	10583

IP段	次数
115.220.2.235	10086
115.203.74.22	10060
183.153.8.40	10053
115.202.176.24	10042
115.203.69.205	10037
115.203.87.199	10036
183.153.1.3	10036
115.203.93.32	10027
115.202.162.252	10025

全部 我的关注 异常规则 登录相关 注册相关 订单相关 短信相关 领券相关 购物车相关 域名监控 多APP登录 多APP注册



安全日志警报[公共邮箱] 0
SOC-alert: WAP端订单列表查看 15:11
 Thu Jul 28 15:08:54 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: mlogin登录监控/WAP端订单详情 13:54
 Thu Jul 28 13:51:34 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: WAP加购物车/WAP端订单详情查 13:44
 Thu Jul 28 13:41:48 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: 临时购物车 13:14
 Thu Jul 28 13:11:52 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: WAP加购物车/wap检查手机是否 12:32
 Thu Jul 28 12:28:49 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: WAP加购物车 12:03
 Thu Jul 28 12:00:44 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: WAP加购物车/App登录测试/API 12:00
 Thu Jul 28 11:57:20 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: WAP加购物车/app登录 11:58
 Thu Jul 28 11:55:27 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: WAP加购物车/监控扫描器黑客/A 11:18
 Thu Jul 28 11:15:44 2016 您所关注的接口出现以下...

安全日志警报[公共邮箱] 0
SOC-alert: App登录监控2 11:02
 Thu Jul 28 11:00:26 2016 您所关注的接口出现以下...

与账户有关

电商安全

与账户无关

撞库

马甲

信息泄漏

刷购物车

刷单

刷券

入侵

爬虫



	以IP为主线索	以账户为主线索
信息完整性	无法得知IP详细信息	理论上可以拥有账户活动的所有信息
可追踪性	IP使用者可能经常更换	账户使用者固定
打击精确度	正常用户与非常正常用户可能使用同一IP	极少有正常用户与非常用户共用一个账号
打击力度	封锁IP更换容易	冻结账户短时间内难以再重新注册大量帐号



第二次 尝试

❶ 缺乏信息

没有一个系统可获得用户所有的信息。

有用户日志被零散的存储在公司各个系统的各个角落

日志的格式不统一

❷ 缺乏算法

每种不同的行为需要有具有针对性的不同的分析算法

不同的算法最终需要汇总到同一个纬度

不缺乏的是我们改变的决心



用户ID: 62437456 用户名: 18616547259 非马甲用户 | 非被盗用户

帐户详情>>>>>>

用户行为>>>>>>

壕评分:

博士评分: 0

绑定手机: 18616547259

注册IP: 58.246.181.94

注册来源: web

下单数量: 7

总计花费: 7077.2

会员积分: 3747

已使用积分: 3747

注册日期: 20140513

注册时间: 2014-05-13 14:05:16

首单ID: 256401276

首单时间: 0

登录信息>>>>>>

订单信息>>>>>>

购物车信息>>>>>>

注册信息

登录信息

账户操作记录

虚拟订单信息

订单信息

优惠券信息



购物车信息



撞库分析



Coin Flip



1. 判断登录是否异地

2. 将登录按维度聚合

3. 聚合后，总计有n次登录，其中有m次不一致。

事件概率：
$$\sum_{k=m}^n \binom{n}{k} x^k (1-x)^{n-k}$$

- n为按纬度聚合后的总登录数
- m为异地登录数
- x为正常情况下异地登录的概率



聚合后，总计6次登录，其中有5次归属地不一致，
当正常情况下登录不一致的概率为0.25。

$$\binom{6}{5}0.25^5(1-0.25)^1 + \binom{6}{6}0.25^6(1-0.25)^0$$

$$= 0.00439$$

用户系统下的 一种问题**解决**之道



电商安全

撞库

马甲

信息泄漏

刷购物车

刷单

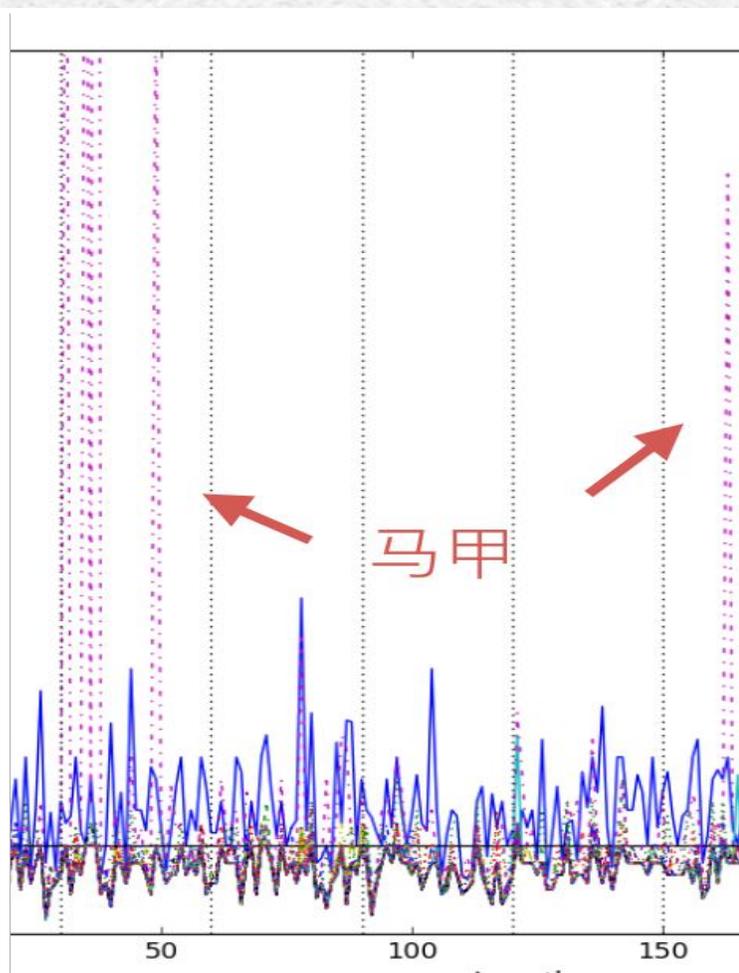
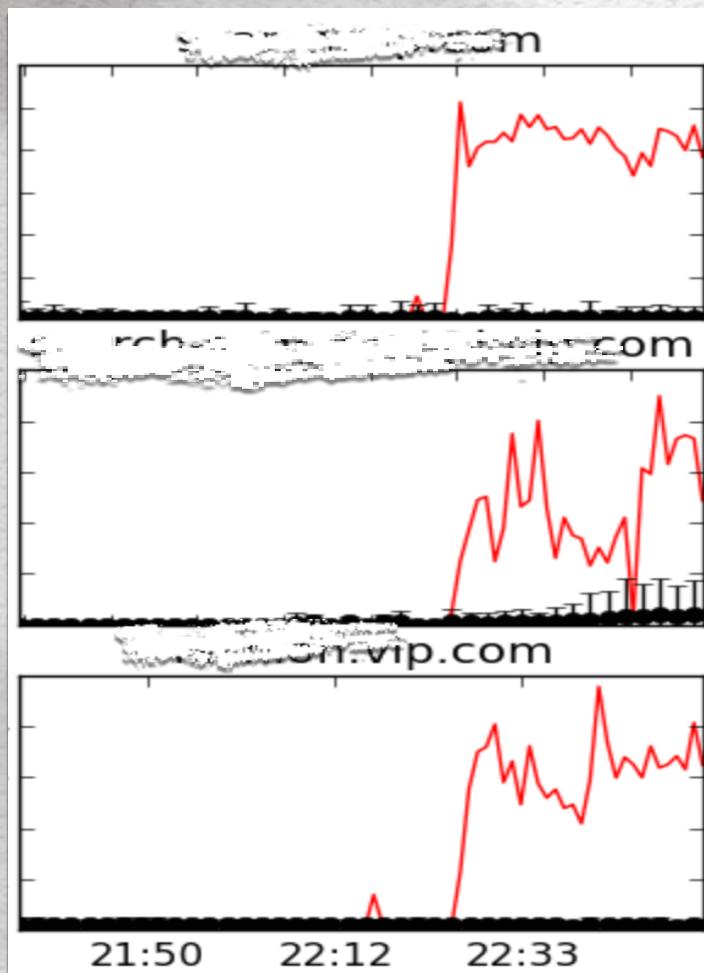
刷券

入侵

爬虫



发现和处理异常行为



吴川市.黄坡镇	三江村	"梅录自提"	林贵
吴川市.黄坡镇	里屋村	"梅录自提"	吴光
吴川市.黄坡镇	岭博村	"梅录自提"	何林
吴川市.覃巴镇	南山塘村	"梅录自提"	刘敏
吴川市.大山江街道	那贞村	"梅录自提"	张扬
吴川市.吴阳镇	高杨村	"梅录自提"	郭权
吴川市.覃巴镇	山懒村	"梅录自提"	周锦
吴川市.覃巴镇	那林村	"梅录自提"	林平
吴川市.覃巴镇	新村	"梅录自提"	梁博
吴川市.吴阳镇	海山村	"梅录自提"	何柄
吴川市.覃巴镇	新屋村	"梅录自提"	何生
吴川市.覃巴镇	新华村	"梅录自提"	陈贵
吴川市.覃巴镇	文屋村	"梅录自提"	曾建
吴川市.黄坡镇	平城村	"梅录自提"	古井
吴川市.王村港镇	林河村	"梅录自提"	周晚
吴川市.振文镇	大桥村	"梅录自提"	刘际

扫描、马甲、异常订单...

预测 VS 发现

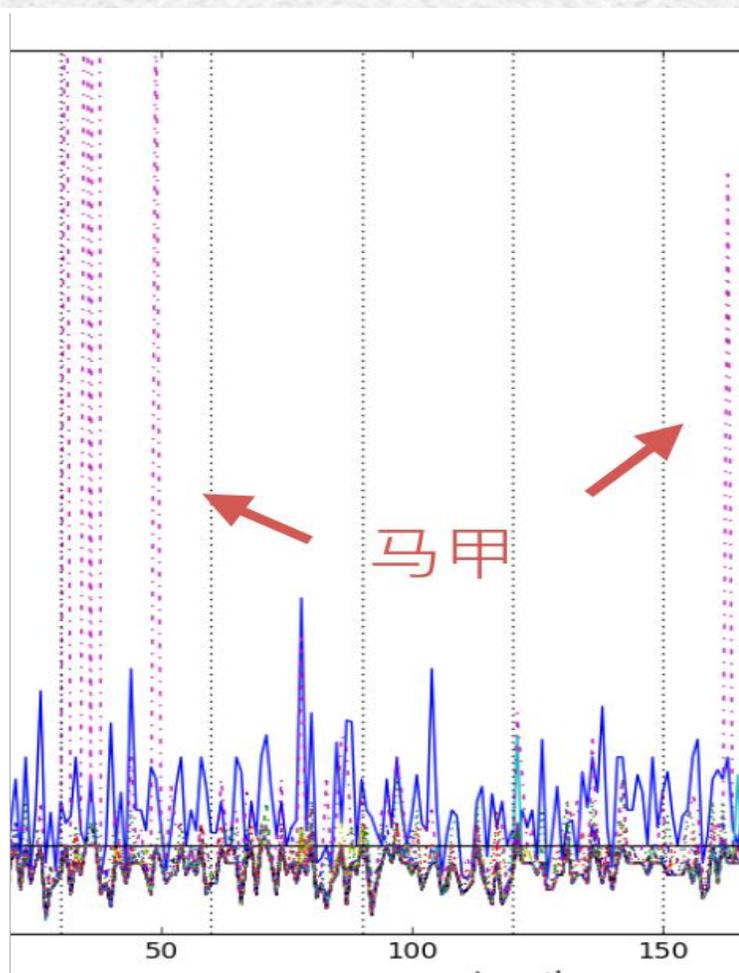
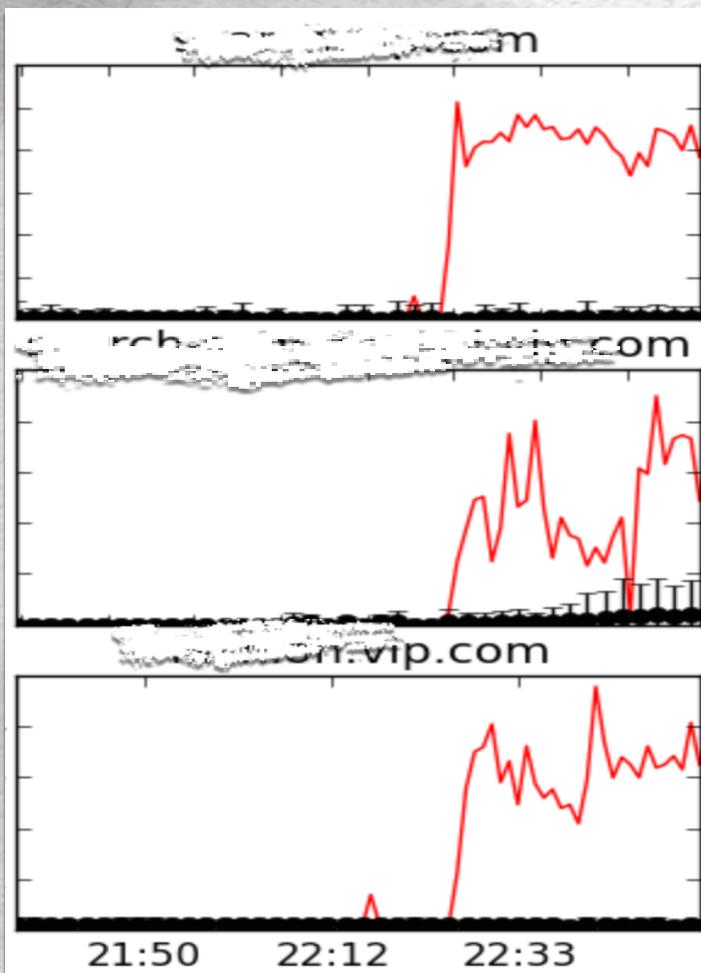
—机器学习，学什么？



预测 VS 发现

— “无监督” , 学 “分布”



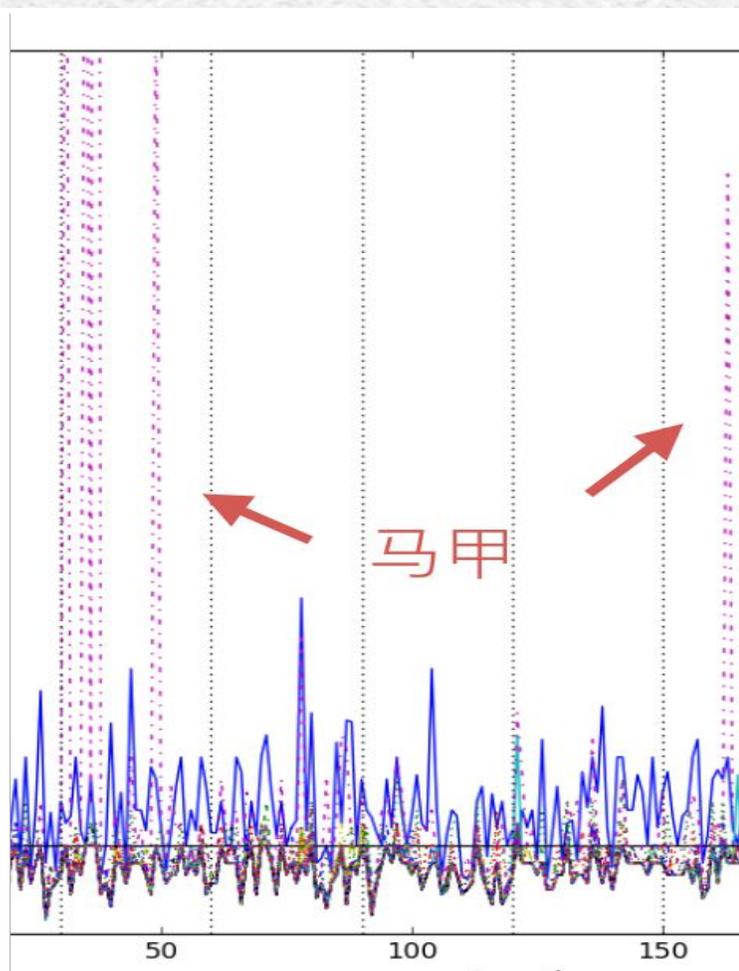
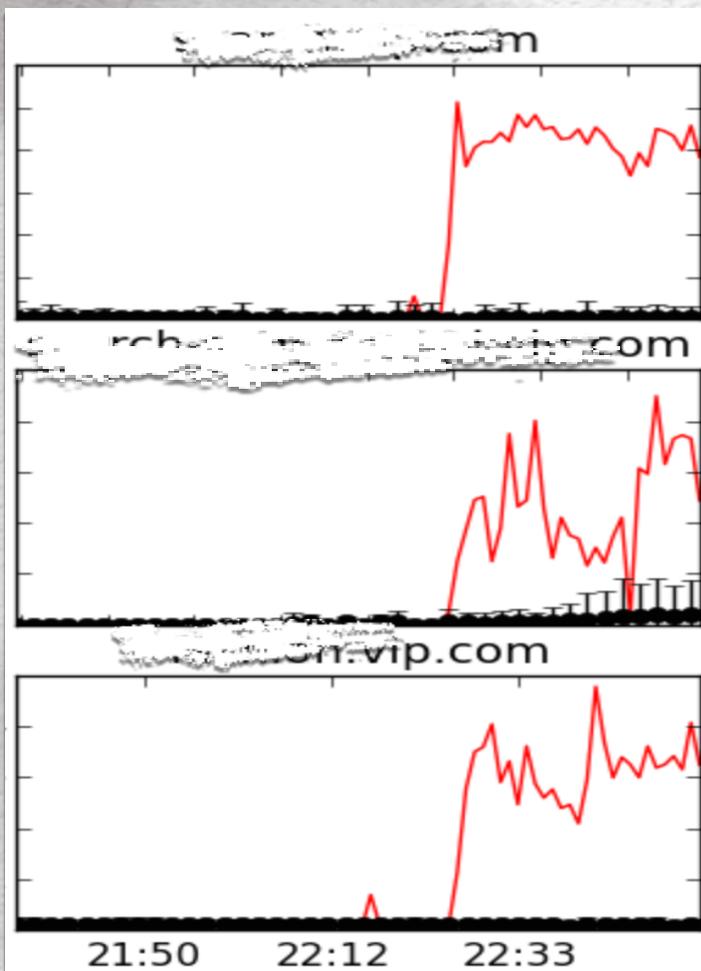


吴川市.黄坡镇	三江村	"梅录自提"	林贵
吴川市.黄坡镇	里屋村	"梅录自提"	吴光
吴川市.黄坡镇	岭博村	"梅录自提"	何林
吴川市.覃巴镇	南山塘村	"梅录自提"	刘敏
吴川市.大山江街道	那贞村	"梅录自提"	张扬
吴川市.吴阳镇	高杨村	"梅录自提"	郭权
吴川市.覃巴镇	山懒村	"梅录自提"	周锦
吴川市.覃巴镇	那林村	"梅录自提"	林平
吴川市.覃巴镇	新村	"梅录自提"	梁博
吴川市.吴阳镇	海山村	"梅录自提"	何柄
吴川市.覃巴镇	新屋村	"梅录自提"	何生
吴川市.覃巴镇	新华村	"梅录自提"	陈贵
吴川市.覃巴镇	文屋村	"梅录自提"	曾建
吴川市.黄坡镇	平城村	"梅录自提"	古井
吴川市.王村港镇	林河村	"梅录自提"	周晚
吴川市.振文镇	大桥村	"梅录自提"	刘际

时间、空间、设备

用户系统：
更多维度，更多选择





吴川市.黄坡镇	三江村 "梅录自提"	林贵
吴川市.黄坡镇	里屋村 "梅录自提"	吴光
吴川市.黄坡镇	岭博村 "梅录自提"	何林
吴川市.覃巴镇	南山塘村 "梅录自提"	刘敏
吴川市.大山江街道	那贞村 "梅录自提"	张扬
吴川市.吴阳镇	高杨村 "梅录自提"	郭权
吴川市.覃巴镇	山懒村 "梅录自提"	周锦
吴川市.覃巴镇	那林村 "梅录自提"	林平
吴川市.覃巴镇	新村 "梅录自提"	梁博
吴川市.吴阳镇	海山村 "梅录自提"	何柄
吴川市.覃巴镇	新屋村 "梅录自提"	何生
吴川市.覃巴镇	新华村 "梅录自提"	陈贵
吴川市.覃巴镇	文屋村 "梅录自提"	曾建
吴川市.黄坡镇	平城村 "梅录自提"	古井
吴川市.王村港镇	林河村 "梅录自提"	周晚
吴川市.振文镇	大桥村 "梅录自提"	刘际



开发时长

半年

团队

2人

异常账户检出率¹

94 %

误判率²

<0.1 %

- 
- 1、该数字由两种完全独立的检测算法互相对比得出
 - 2、基于用户投诉与异常账号的比值
- 

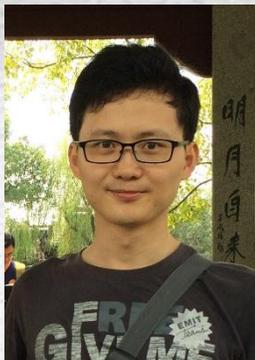
坐享其成





孟诚 | 汪浩





上海交通大学天体物理学博士后

唯品会信息安全部工程师



Georgia Tech 电子与计算机硕士
上海交通大学电子与计算机学士

唯品会信息安全部工程师