



2016 杭州·云栖大会  
THE COMPUTING CONFERENCE

云栖社区  
yq.aliyun.com

# 互联网企业 通用业务安全防控体系建设

2016  
The Computing Conference

李升华  
2016年10月

主办单位： 杭州

 Alibaba Group  
阿里巴巴集团

战略合作伙伴：



扫码观看大会视频

目录

CATALOG

□ 业务常见安全问题

□ 解决方案和实践

□ Q&A



## 业务常见安全问题

### 绑架P2P平台？解密疯狂的“羊毛党”

第一财经日报 安卓 2015-04-21 06:00:00

“羊毛党越来越普遍，我们2010年平台成立的时候，全国P2P平台还不是那么多，所以羊毛党未成气候，这两年，随着P2P平台的大量涌现，为了吸引眼球，P2P平台只能通过各种优惠活动获客，羊毛党随之而生，可以说，羊毛党是P2P行业竞争加剧过程中衍生的一个群体。”



评论 0

赞 0

近日，广州一小型P2P平台的投资者向媒体爆料称，该平台目前已经出现提现困难，平台的法人代表失联，其位于广州珠江新城的办公室已经被搬空。

《第一财经日报》记者发现，这家名为“民间财富”的平台已经无法注册新会员，其最后一次发标是在3月30日。平台公告显示，该平台成立于2014年中旬，目前注册会员534人，待收总金额59.24万元。

可以说，这是一家上线不久，且交易金额很小的平台，然而，就在这个小平台处于瘫痪状态的背后，一个独特的投资人群体浮出水面，业内称之为“羊毛党”。在广州一网贷业内人士看来，这个平台目前出现的问题与“羊毛党”有很大关系。



## 业务常见安全问题

	优惠券249-50 149-40 优惠券 券 抵价券 现金券/卷/券	¥ 2.00 已售	7469人付款 2681条评论
	优惠券19-10元 新号账号现金 券【微博登录】带随机红包	¥ 0.88 已售	3817人付款 513条评论
	优惠券80-10 149-40 249-50 抵价券 优惠券现金券券卷	¥ 1.00 已售	4059人付款 2205条评论
	优惠券19-10元/ 抵用券 不带 红包【 微博】	¥ 0.99 已售	1177人付款 1133条评论
	优惠券 聚美优品10元现金券 19-10优惠 带0.6~1.88	¥ 0.88 已售	1759人付款 553条评论
	10元现金券优惠券满19-10 抵价券优惠券 带0.6~1.88	¥ 0.88 已售	661人付款 294条评论

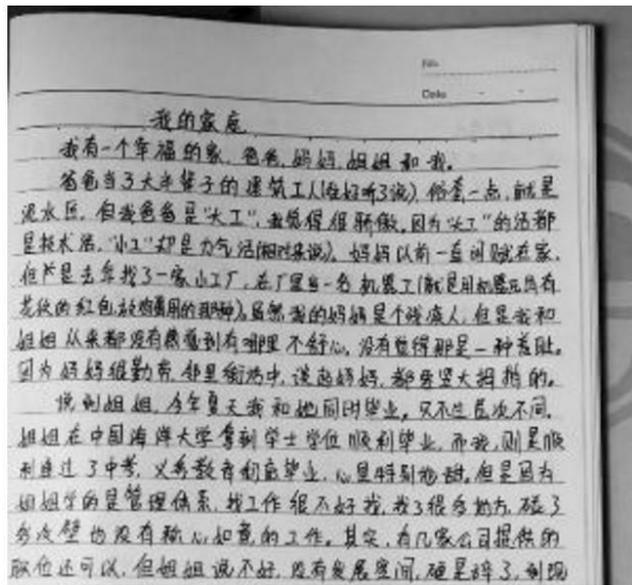


## 又一山东大学生遭电信诈骗猝死，谁害死了“徐玉玉们”

2016-08-26 12:13:40 来源: 东方早报(上海)

▲ 举报

(原标题: 又一山东大学生遭电信诈骗猝死，谁害死了“徐玉玉们”)



“18岁准大学生徐玉玉被骗学费  
心脏骤停”后续

“冰山一角”

据江阴市公安局统计，2016年1月份以来，该市共285名在校学生遭遇电信网络诈骗，被骗总金额116万余元，受害人平均年龄18岁。



扫码观看大会视频

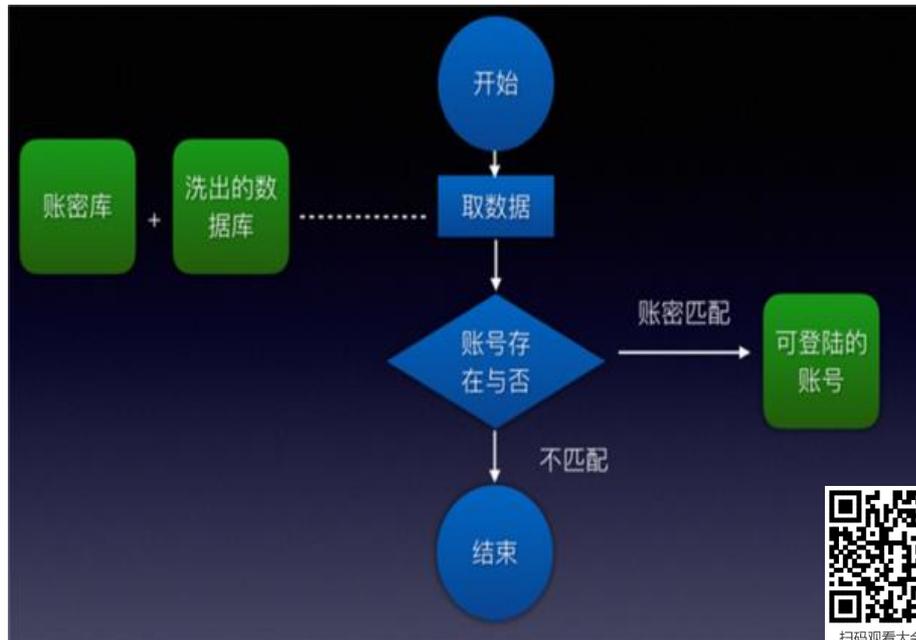


# 刷库撞库

## 第一步：洗库



## 第二步：撞库



## 业务黑灰产

- 产业链的上游是一个基础性的行业；
- 中游是网络账号提供商及信息交易交流平台；
- 下游主要是利用非正常渠道的网络账号进行欺诈、盗窃、刷单等犯罪和不道德行为的团伙。



国内黑产从业人员 **150万+**



黑产市场规模 **1000亿+**



扫码观看大会视频

目录

CATALOG

□ 业务常见安全问题

□ 解决方案和实践

□ Q&A



## 通用架构



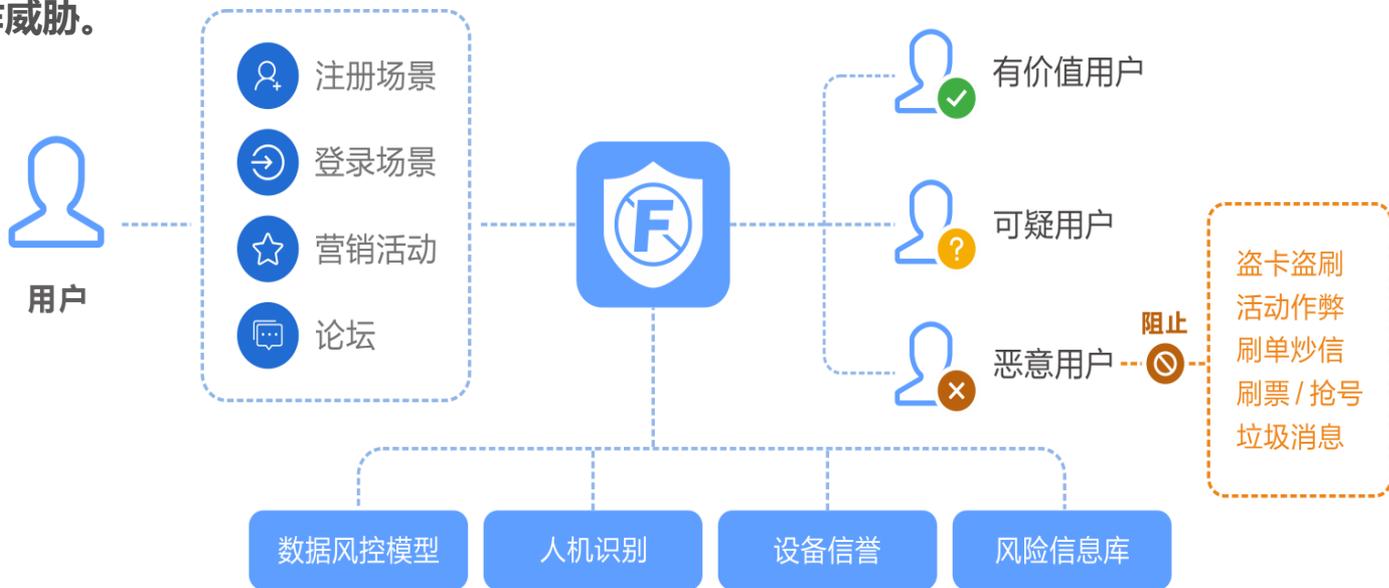
## 布点防护

常见风险	注册	登陆	密码找回	信息修改	活动/交易
反垃圾注册 ( 虚假, 垃圾 )					
防账号盗用 ( 撞库, 盗用 )					
反活动作弊 ( 黄牛, 羊毛 )					



## 阿里聚安全数据风控

基于阿里大数据计算能力，通过业内领先的风险决策引擎，解决企业账号、活动、交易等关键环节存在的欺诈威胁。



# 滑动验证

## Pc web版

请输入您需要开通账户的帐户名

会员名：

验证：



拖动滑块验证>>



了解新功能

确定



## 滑动验证

### HTML5 版

为了你的账户安全请填写一个手机号完成验证

国家/地区 中国大陆 (+86) ▾

手机号



向右滑动验证

继续操作即视为同意[淘宝服务协议](#)、[法律声明](#)及  
[隐私政策](#)和[支付宝协议](#)



### Native 版

中国移动

4:21 PM

100%

< 返回

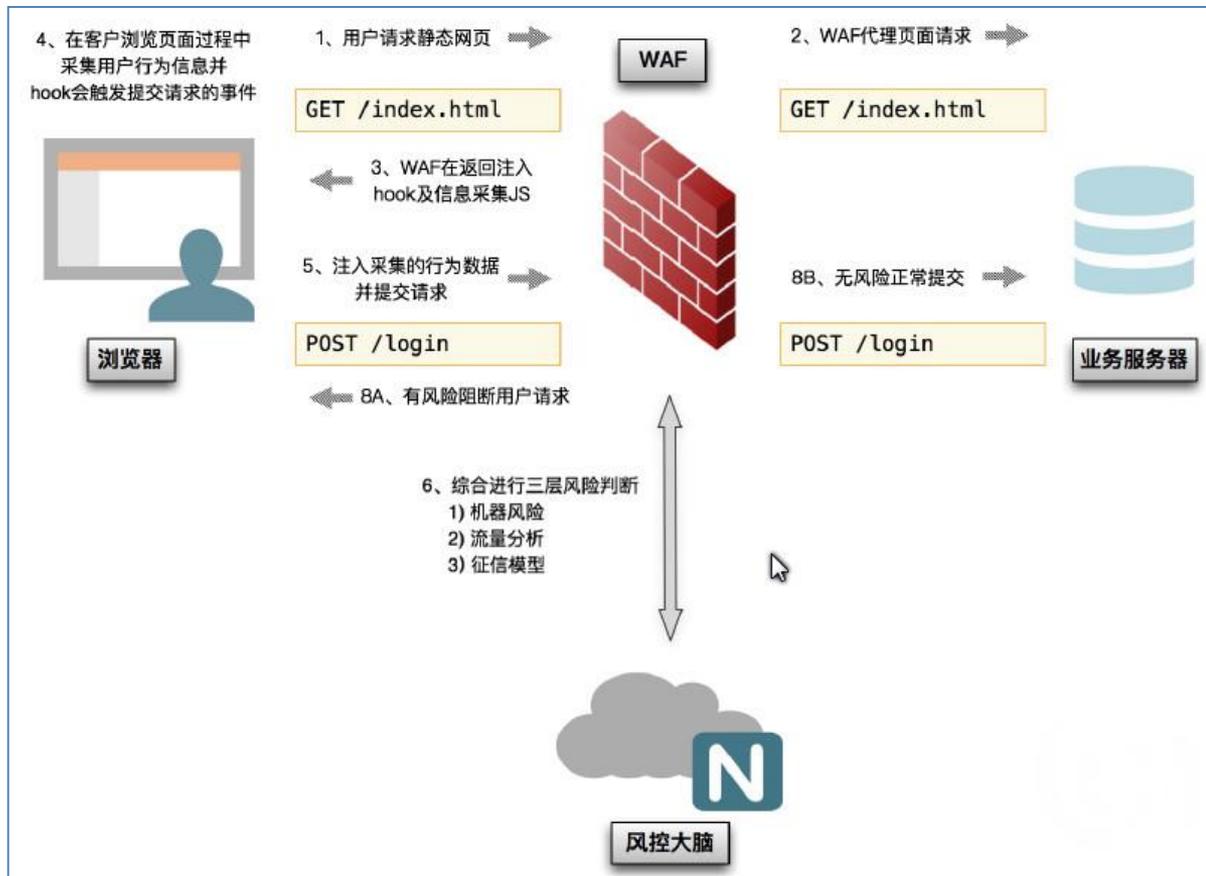
### 安全验证



为了你的账号安全，本次登录需要进行验证  
请将下方的Logo移动到圆形区域内



# 阿里云WAF数据风控





< 返回首页



您已经完成注册!

完成



扫码观看大会视频

虚假认证指认证自然人身份信息无效、虚假、或者归属人与实际操作人或账号使用人不一致，存在身份造假或者身份冒用风险。

## 产业上游

黑身份证（主要是  
电子身份证件）  
交易平台



黑银行卡  
交易平台



恶意注册账号  
交易平台



## 产业中游

虚假认证团伙



账号分销团伙

## 产业下游

信息类犯罪：发布危及国家安全的言论、虚假广告

商品类犯罪：销售国家禁售商品，销售侵权产品以及假冒伪劣商品

扰乱市场秩序类犯罪：诈骗、盗窃、损害商业信誉、寻衅滋事

...



实人认证是根据用户提交的身份材料和网络行为，经过生物特征识别和大数据动态风控模型来判定个人用户身份真实性的一套网络自然人核身服务。

## 身份存在



### 实名校验

姓名、身份证号验证



### 语音验证

电话直拨，一键验证



### OCR证件识别

假证冒用，无处可藏



### 风险名单

风险用户，名单累积

## 真实有效



### 人脸检测

人像捕获，准确定位



### 人脸比对

特征提取，快速比对



### 活体认证

活体校验，真人鉴别



### 人脸检索

人脸建模，快速搜索



### 声纹认证

声音识别，听微决疑

## 持续一致



### 扫脸验证

高危应用，扫脸核实



### 动态风险跟踪

风险用户，实时复核



### 团伙识别

关联行为，群体分析



### 风险决策

大数据模型，综合决策



目录

CATALOG

□ 业务常见安全问题

□ 解决方案和实践

□ Q&A



Q & A



 阿里聚安全  
官方微博



 阿里聚安全  
微信公众号



扫码观看大会视频

20 The  
16 Computing  
Conference  
**THANKS**

