

日知录

IT大咖说  
不止于技术

# 知道创宇网络反欺诈经验分享

---

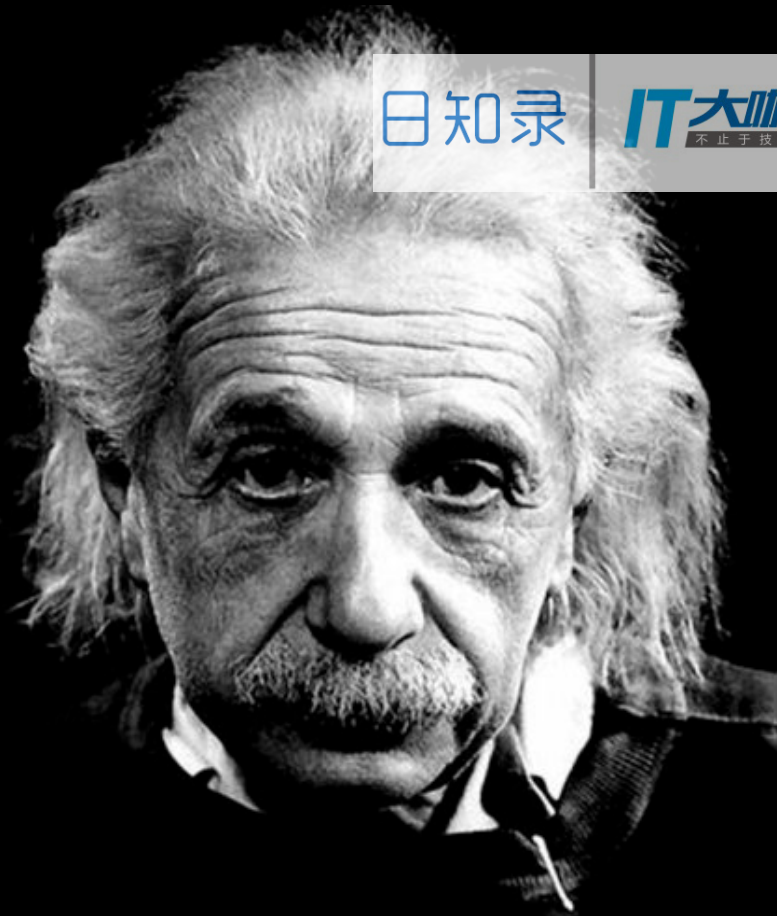
潘少华

知道创宇反欺诈产品线总监

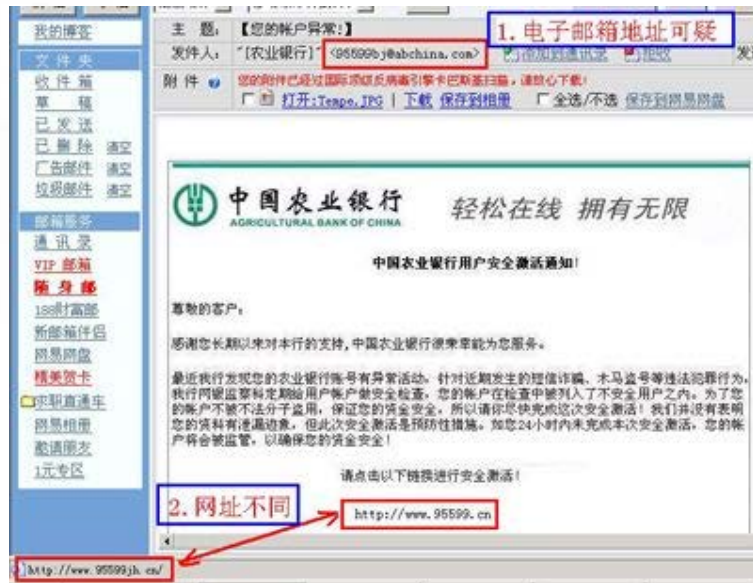
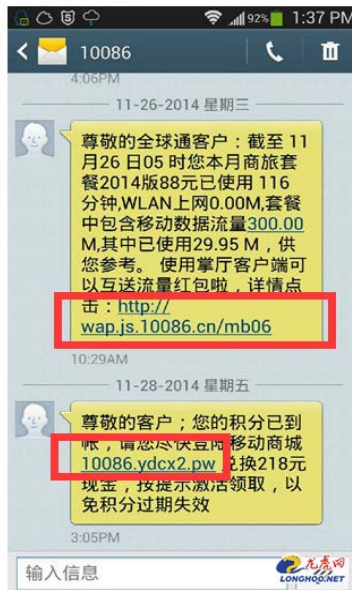
日知录

IT大咖说  
不止于技术

这个世界很危险  
不是因为那些邪恶的人  
而是因为那些无动于衷的人



随着移动互联网的高速发展，用户浏览网站信息的途径已经从单一的PC端越来越多转变为移动端设备，与此同时移动端的安全问题也日益凸显，特别是“钓鱼、手机木马网址”。



日知录

IT大咖说  
不止于技术

# 全民进入移动时代，诈骗横行

## 冒充公检法人员诈骗120万元

2015-05-08 01:24:06 来源: 郑州日报(郑州)

## 广州一天3宗电信诈骗 冒充公检法骗走731万元

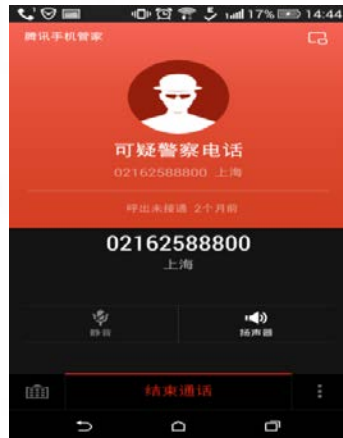
广州资讯 2015年5月6日 来源: 信息时报

## 冒充公检法，老套骗术 骗走她805万

2015-04-30 17:09 来源: 晶报

## 工程师40天被骗1127万 骗子冒充公检法人员骗钱

发布时间: 2015-06-03 10:31:23 编辑: xuzia



你在干嘛? 新年快乐, 这是过年时候大家聚会的照片, 好珍贵的留影, 你快看看吧, 地址: <http://url.cn/eZs4uT>

< 信息 日知录 +852 9516 1321

IT大咖说 不止于技术

短信/彩信  
4月15日 周三 13:24

尊敬的旅客: [redacted] 您好!我们很抱歉的通知:您预订2015年04月16日09:40起飞的MU2325航班(西安—深圳)由于机械故障已取消,请收到短信后及时联系客服办理退改签业务,以免耽误您的行程,给您带来不便我们深表歉意!(注:改签乘客需要先支付20元改签手续费,无需承担差价,并且每位乘客将额外获得航班延误补偿金300元)客服热线: [400-6911-787](tel:400-6911-787) 【东方航空】

XX,谁上传了你的视频啊? 恶心你下看 <http://caiyun.feixin.10086.cn/sh/1ctG1ENfCjvHtDZr>

尊敬的招商银行用户: 您的信用积分已满兑换699.68元现金条件, 手机访问 [cmbcnzm.cc](http://cmbcnzm.cc) 即可兑换-招商银行

你好! 我是房东请把房租打到这张卡上, 工行: 6212 264 0 0002 7619 168李友军

## 电话诈骗盛行，运营商成众矢之的

日知录

IT大咖说  
不止于技术

- 电信诈骗成为社会顽疾，电话及短信成为诈骗核心渠道，运营商成为众矢之的
- 治理电话诈骗任重道远，非运营商一己之力可解决，处于反信息诈骗的舆论漩涡
- 运营商往往成为电话诈骗的受害者，用户责备、政策及舆论利空



### 电信诈骗应追究银行运营商责任

来源：佛山日报 日期：2015-03-13 编辑：孔德钦 字号：T T

分享到： 0

长期关注电信诈骗问题的全国人大代表、珠海格力集团副总裁陈伟才昨日（3月12日）在广东代表

新浪河南

[新浪河南](#) > [数码频道](#) > [运营商专区](#) >

### 央视315晚会三大运营商无一幸免

2015年3月16日08:35 [新浪科技](#)

新浪科技讯 3月15日晚间消息，在刚刚结束的央视315晚会上，科技类企业中三大电信运营商无一幸免，分别涉及诈骗电话和手机实名制等问题。而此前传说中的P2P企业和电商类网站均逃过一劫。

据节目报道，中国移动、中国铁通在为骚扰电话提供各种支持，甚至给“10086、110”之类的诈骗电话一路开绿灯，即使发现诈骗电话显示虚假主叫号码，仍然允许骗子将虚假电话号码显示在用户手机上。

## 黑色产业链走精细分工模式，形成规模经济

日知录

IT大咖说  
不止于技术

- 黑产的开发、传播、运营、洗钱每个步骤都有精细的分工模式
- 黑产模式上有改号诈骗、伪基站、钓鱼网站、恶意病毒等组合变换的方式



- 病毒开发
- 恶意网站制作
- 黑卡、改号线路

- 电话拨打
- 伪基站
- 短信群发

- 洗钱

# 知道创宇联合腾讯、百度发起安全联盟公益组织打击网络犯罪

## 日知录

## IT大咖说

不止于技术

成员单位及合作伙伴

[查看更](#)

Tencent 腾讯

Baidu 百度

金山网络

KNOWSEC  
知道创宇

腾讯电脑管家

腾讯手机管家

微信

QQ

百度卫士

百度杀毒

百度浏览器

搜狗浏览器

搜狗号码通

搜狗搜索

猎豹浏览器

金山毒霸

中呼  
ZHONGHU

WooYun

加速乐

火狐浏览器

新浪微博

多玩游戏  
duowan.com

YY浏览器

YY语音

瑞星

湖南卫视

芒果TV

浙江卫视

风行网

168

黑龙江卫视

CHOISKYCN  
韩+艺

GREE 格力

电话帮

中国工商银行

平安银行  
PING AN BANK

中国银行  
BANK OF CHINA

交通银行  
BANK OF COMMUNICATIONS

中国建设银行  
CHINA CONSTRUCTION BANK

中国农业银行  
AGRICULTURAL BANK OF CHINA

招商银行  
CHINA MERCHANTS BANK

期待您的加入



8亿条

共享恶意网址  
数据库

150+个

厂商正在共享和  
交换数据

5000万次

每天交换恶意  
网址数据

180万次

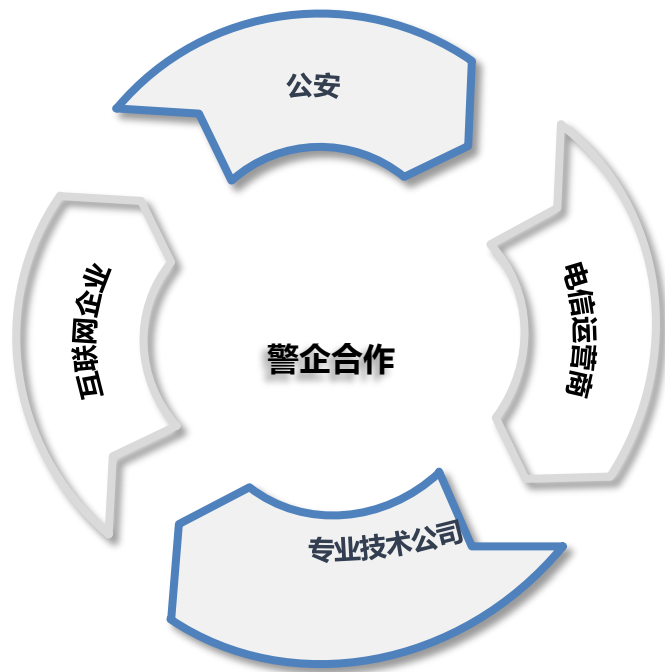
年受理网友举报



# 反诈骗资源整合

日知录

IT大咖说  
不止于技术



## 诈骗号码的合作方案：事中提醒+阻断

日知录

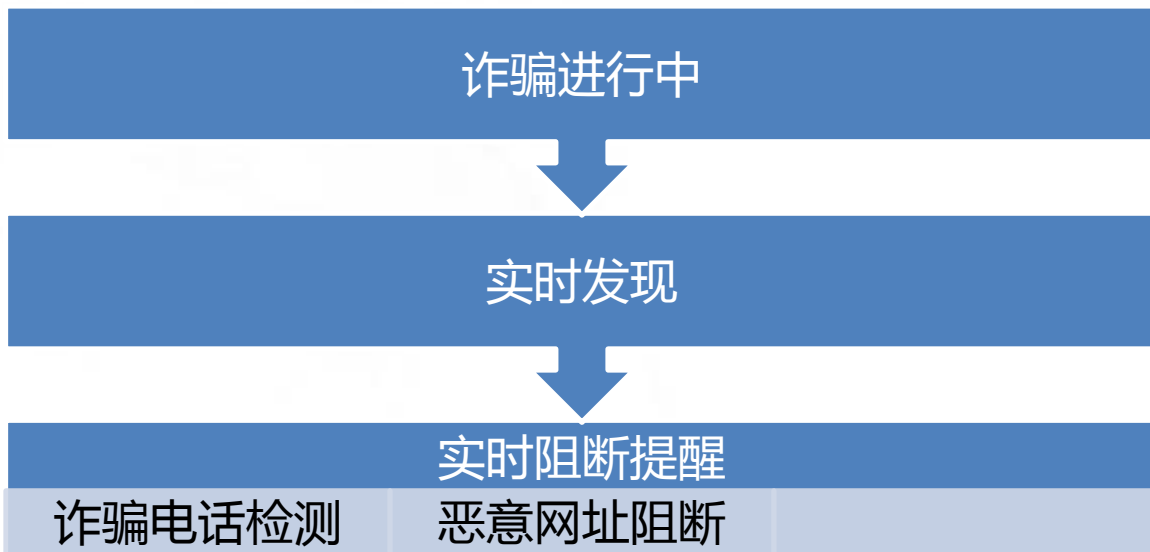
IT大咖说  
不止于技术

- 传统方法——事后：



- 我们的解决办法——事中：

- 发现，提醒，阻断



# 目录

contents

1 面临的安全挑战

2

诈骗电话检测技术

3

反网址诈骗系统



# 诈骗技术和方法更新，导致原有拦截手段失效

日知录

IT大咖说  
不止于技术

本地落地

对抗国际端局封堵

## 呼叫地来源检测

1. 拦截不规范的主叫和号首，例如0002-0009的国际主叫；
2. 拦截尾号为10086、95588、12333等国际来话

网间诈骗

对抗呼叫地来源检测

## 国际端局封堵

1. 拦截0002-0009、00010-00018开头的不规范国际主叫；
2. 拦截0057、0058开头位长小于10位的主叫
3. 拦截00191/2/4/8/9等电信网编号规划中未定义国际局标示码

仿冒真实号码

对抗黑名单拦截

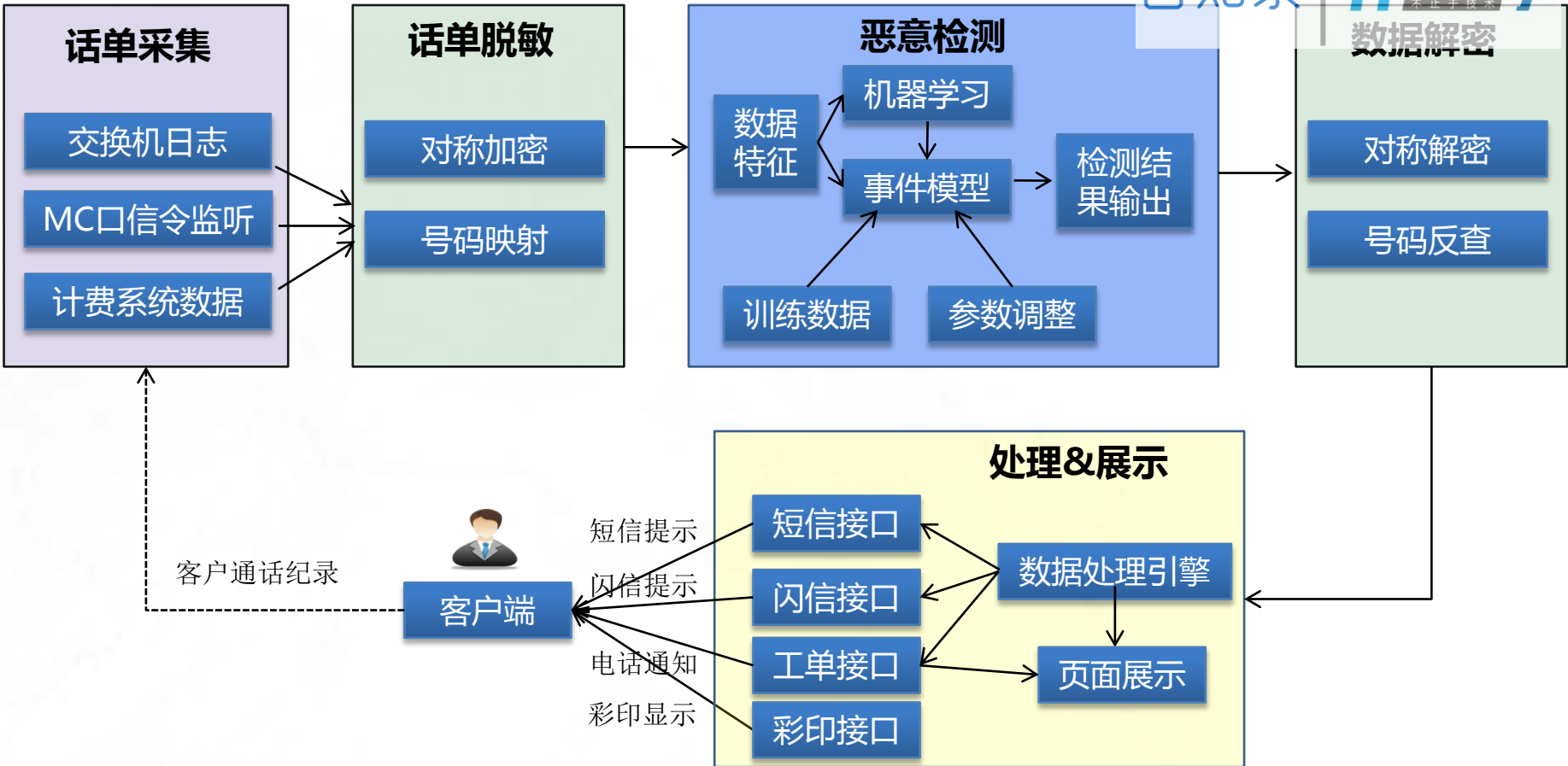
## 黑名单拦截

1. 骚扰电话黑名单
2. 诈骗电话黑名单

# 基于大数据机器学习的诈骗电话检测管控系统

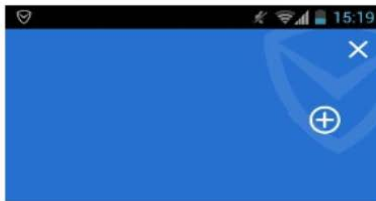
日知录

IT大咖说  
不止于技术  
数据解密



### ➤ 基础数据：250W的活跃诈骗号码库

1. 用户接到陌生电话，弹出标记框引导用户标记号码



标记陌生来电，识别骚扰号码：



2. 后台服务接收标记上报，使用一定策略拉黑号码

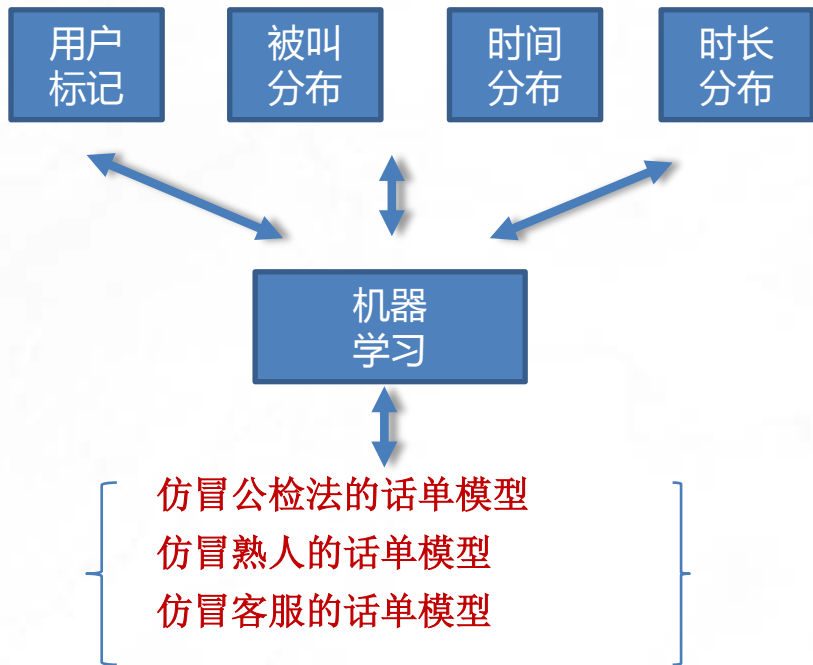


3. 用户接到诈骗电话时，后台服务提醒用户，并显示标记人数

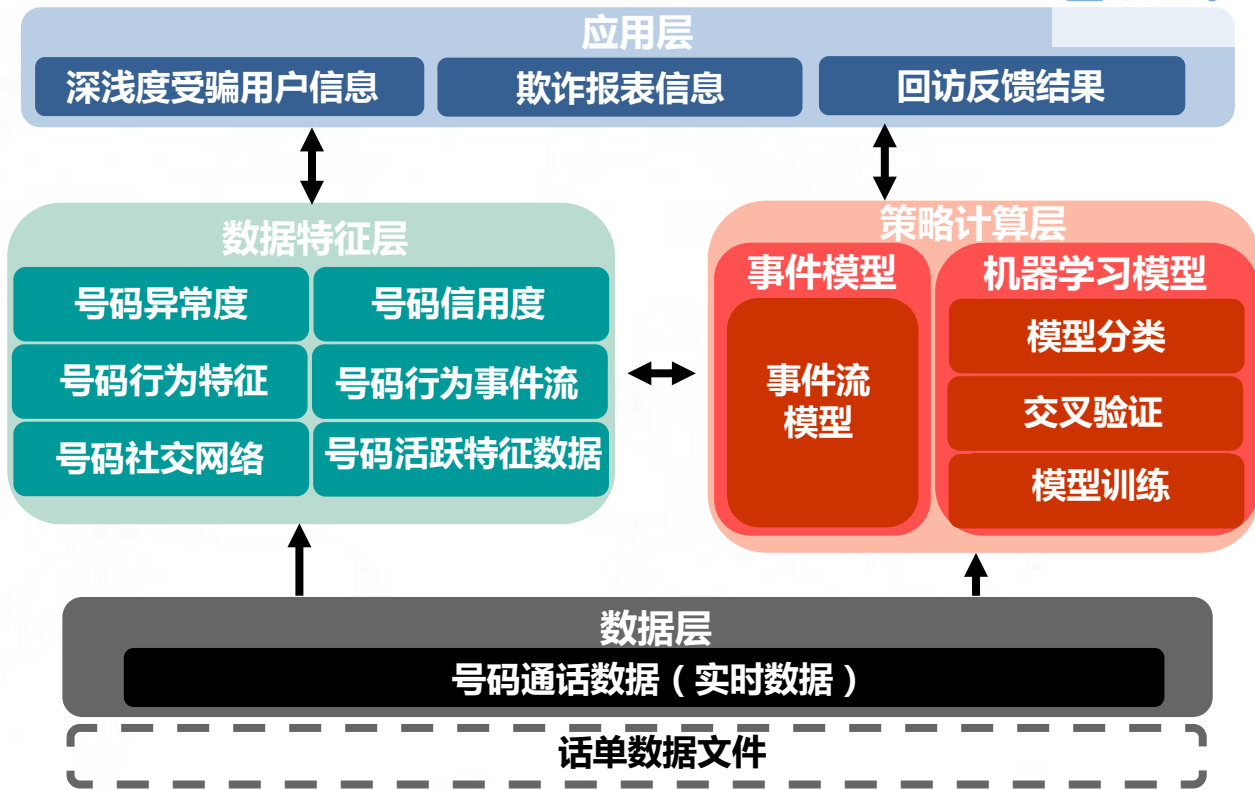


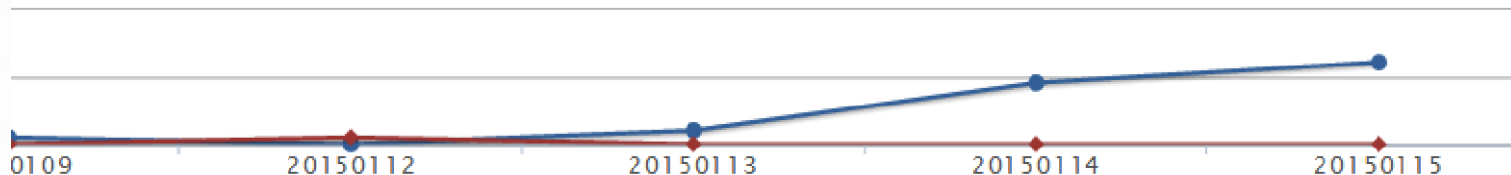
# 核心技术：大数据机器学习

- 基于话单行为机器学习模型
- 内置超过50种类型语音诈骗话单模型







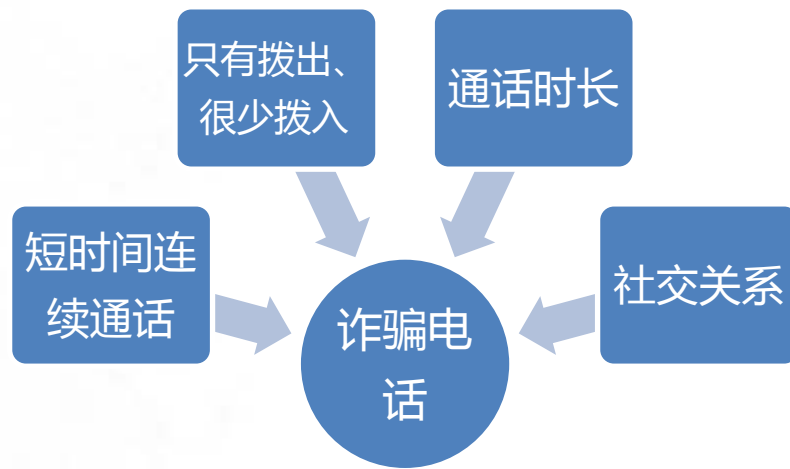
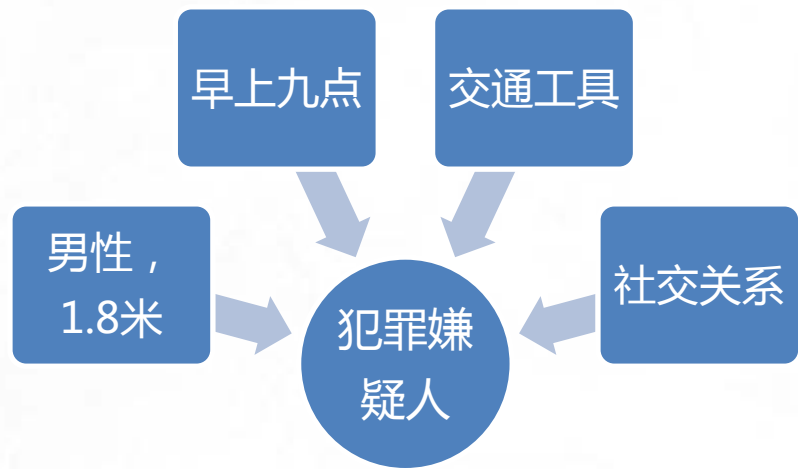


对于诈骗号码，往往使用周期都很短，所以对于该号码，往往有通话量突增的特点，根据此特点，再结合地域、好友关系链，号码历史评价等维度的数据，能检出这种特点明显的诈骗电话。

- |       |              |                                  |
|-------|--------------|----------------------------------|
| 10:12 | +18588567356 | 自动语音，说有个文件投递没有成功，按9转人工。          |
| 10:23 | +0195852211  | “公安局刘警官”打过来                      |
| 11:38 | 02156608111  | 仿冒“上海市公安局宝山分局”的电话打过来             |
| 12:02 | 021114       | 用户拨打了021114，确认检察院电话是02124024000。 |
| 12:16 | 02124024000  | 检察院电话打过来。                        |

不法分子要进行诈骗，往往都有一定套路，基于大数据分析的方法，可以建设事件模型，检测到这样的号码序列。同样一串这样的号码，打给了多个用户，那这样一串号码序列是可疑的。

因此本技术就可以对异常事件进行拦截，而不像传统技术受限于号码拦截。



会从各种用户的举报中收集到类似的大量400的恶意电话。

针对话单里面主被叫号码一段时间的通话情况分析：

- A. 该号码作为主叫给人拨打的概率是多少？ A概率
- B. 该号码作为被叫被人拨打的概率是多少？ B概率
- C. 该号码联系的人的地域散列量有多少？ C数量
- D. 该号码被叫时通话时长分段特征有多少？ D数量 (0~60S概率,60~120S概率,120S~300S概率)

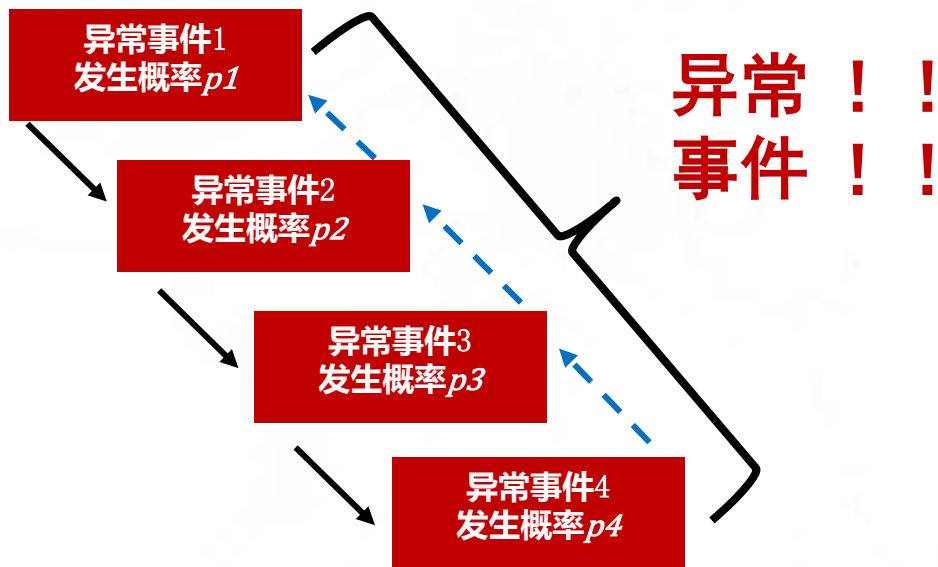
正常的号码 主被叫概率相当，联系用户的省份相对较少，常规联系人的省份数大多是一个，通话时长波动会比较大

针对此类仿冒客户的诈骗号码，有明显的特征：

- A概率比较低 而且
- B概率比较高 而且
- A概率小于B概率 而且
- C联系用户的省份比较多 而且
- D数量很少（一般要么被骗，要么很快识别出来诈骗）

诈骗分子会经常调整策略！

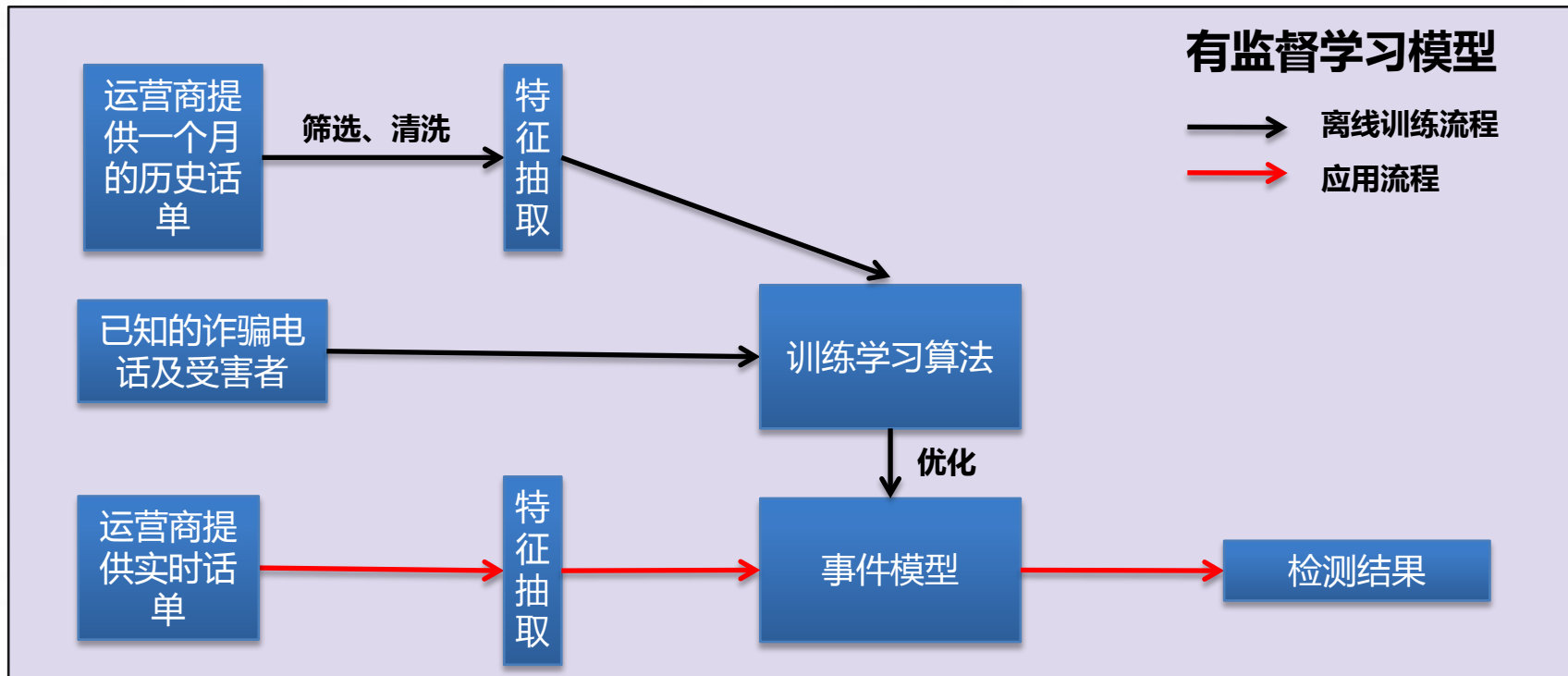
以一个常规的电话仿冒公检法案情发生过程为例，它的发生过程伴随着一系列可能异常的话单通话情况，比如海外广撒网通话和仿冒公检法机构的通话，他们之间的通话可能存在多次且连续发生。那么这样的一系列通话行为则是异常行为事件流，会被特征模型提取出来，最终被事件模型的逻辑所捕获。



## 基于通话行为模式智能分析——机器学习算法

目知录 IT大咖说

采用有监督学习的算法模型，模型共包括二个流程，一个是离线训练流程（黑色箭头），包含数据筛选和清洗、特征抽取、模型训练和优化模型等环节；另一个流程则是应用流程（红色箭头），对需要预估的数据，抽取特征，应用离线训练得到的模型进行预估，获得预估值作用在实际数据中。



# 反电话诈骗检测系统的流程说明



## 1. 话单采集系统

从交换机上采集前N月的通话话单，本地识别引擎使用话单分析模型以及同步云端黑白名单库，形成本地黑白名单库。而后采集实时通话话单。

## 2. 话单脱敏系统

将话单进行脱敏并输送给识别引擎。

云端

## 3. 知道创宇恶意号码识别引擎

针对同步的准实时话单，通过同样加密的黑白名单以及话单模型识别里面的恶意号码和受害用户（均在加密形态中）。

## 4. 工单系统

根据知道创宇提供的受害用户的话单（加密形式），解密里面的原先加密的电话号码数据，发短信或者电话提醒受害用户

将完整的诈骗电话号码发回云端，更新云库数据

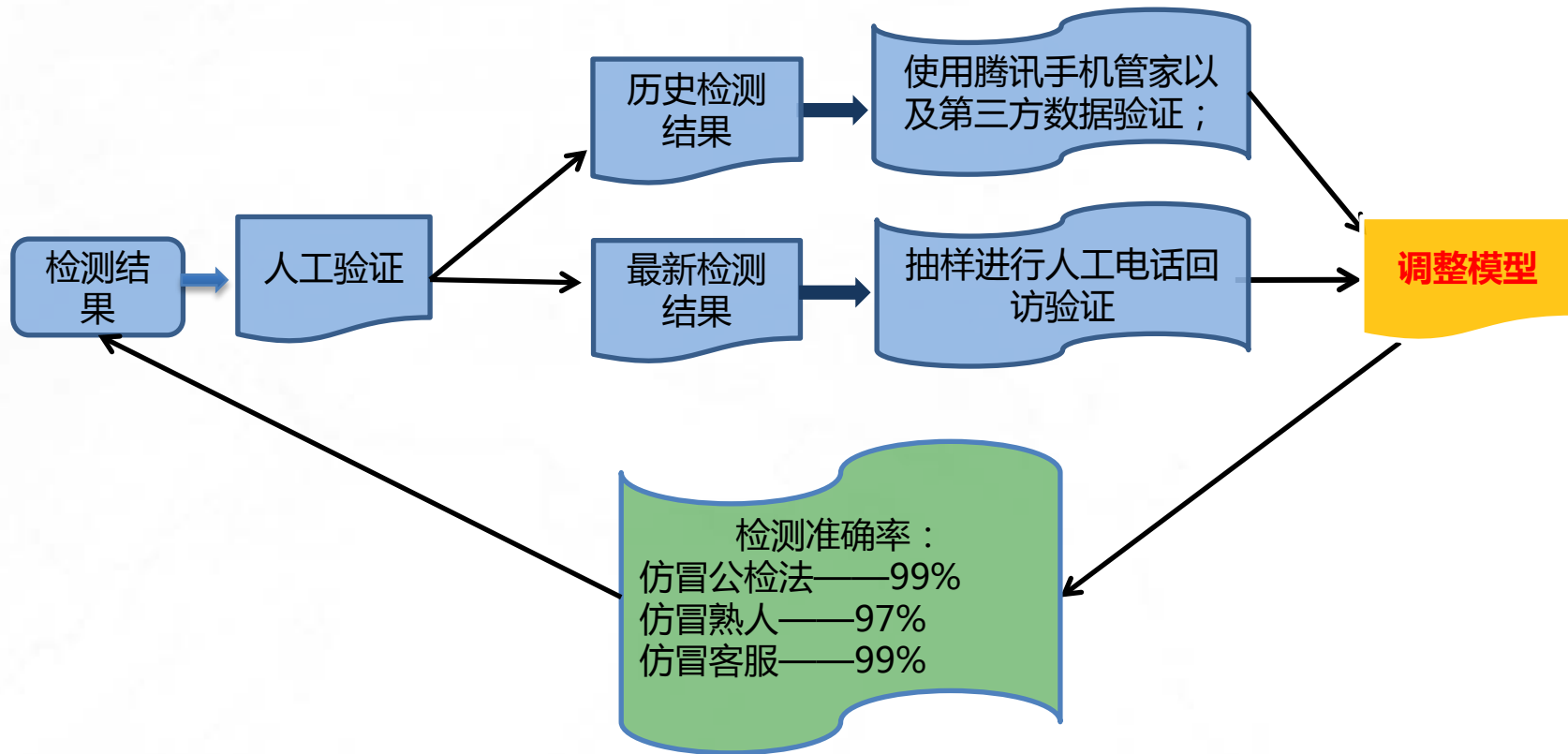


## 提供的诈骗电话字段

| 字段     | 字段含义说明               |
|--------|----------------------|
| 诈骗电话   | 诈骗电话（加密的号码串）         |
| 电话类型   | 海外电话，固话，手机号码等        |
| 运营商    | 联通，移动，联通             |
| 省份     | 号码对应省份               |
| 城市     | 号码对应城市               |
| 诈骗类型   | 仿冒公检法，仿冒领导等          |
| 操作类型   | 对号码的操作是封号，还是提醒对应通话用户 |
| 天热度    | 号码最近一天主叫和被叫总的次数      |
| 周热度    | 号码最近一周主叫和被叫总的次数      |
| 月热度    | 号码最近一月主叫和被叫总的次数      |
| 首次出现日期 | 号码首次出现日期             |

## 提供的被骗用户字段

| 字段     | 字段含义说明                  |
|--------|-------------------------|
| 被骗用户   | 被骗用户的号码（加密的号码串）         |
| 诈骗电话   | 做恶的号码（加密的号码串）           |
| 主被叫标识  | 标识受害用户是主叫号码还是被叫号码       |
| 接通时间   | 通话时间                    |
| 通话时长   | 通话时长                    |
| 诈骗类型   | 诈骗属于哪种类型，比如仿冒公检法，仿冒领导等。 |
| 恶意发现时间 | 系统什么时间发现本次通话涉嫌诈骗        |
| 提醒类型   | 需要语音提醒还是短信提醒            |



- 短信提醒内容
  - 公安授权
  - 反诈骗举报电话
  - 因举报而提醒



- 闪信提醒内容
  - 公安授权
  - 反诈骗举报电话
  - 因举报而提醒



- 彩印提醒内容
  - 诈骗标记
  - 反诈骗举报电话



- 工单系统接口
- 自动回拨功能
- 回访内容回传至页面展示
- 回访数据回传至检测引擎



- 用户隐私保护：只使用脱敏后的电话话单即可检测，不需要语音内容，也不需要真实完整的用户电话号码，所需硬件较少，对用户的隐私也能最大限度的保护。
- 检测引擎：基于机器学习，输入话单，输出恶意电话及目标用户
- 准确率：恶意号码识别准确率保证99%，检出率达到90%以上，并且能够区分浅层诈骗和深层诈骗。
- 覆盖率：基于诈骗通话模型和大数据机器学习技术，能够准确识别最新主流的电话诈骗类型，如仿冒公检法、仿冒电商客服、仿冒银行、仿冒运营商、仿冒社保部门、仿冒银行、仿冒航空公司、仿冒领导熟人等，仿冒公检法 / 仿冒客服的诈骗电话，能够规避无法使用黑名单拦截的问题。
- 及时打击：本系统能够与短信、客服等系统联动，自动给受害者做提醒，或者通过客服系统工单，由客服人员打电话通知受害者，从而第一时间提醒用户，避免损失。

- 某地市级运营商
  - 浅层诈骗：日均短信提醒 1000次
  - 深度诈骗：日均电话提醒40次
  - 上线半年多，一共只收到两起误报反馈
- 用户被骗金额下降70%以上
- 预计一年为用户挽回损失5000W
- 对冒充公检法全覆盖
  - 还有被骗，因为电话一直占线
- 其它可识别诈骗模式
  - 冒充熟人，航空公司，信用卡中心，电商客服...

| 通话次数 | 总通话时长（秒） | 诈骗电话            | 通话时间            | 诈骗类型类型 | 说明                      |
|------|----------|-----------------|-----------------|--------|-------------------------|
| 1    | 3057     | 0002162906290   | 2015/10/9 8:44  | 仿冒公检法  | 02162906290是上海长宁公安分局    |
| 3    | 4557     | 00138020413800  | 2015/10/9 8:17  | 仿冒公检法  |                         |
| 1    | 2727     | 0002160498684   | 2015/10/9 9:12  | 仿冒公检法  |                         |
| 1    | 1829     | 0002164868911   | 2015/10/9 9:36  | 仿冒公检法  | 02164868911是上海徐汇公安分局    |
| 1    | 2150     | 00059187621305  | 2015/10/9 9:36  | 仿冒公检法  | 手管标记诈骗电话                |
| 1    | 2944     | 0001085225050   | 2015/10/9 9:24  | 仿冒公检法  | 01085225050是北京市公安局      |
| 1    | 2708     | 00452162906290  | 2015/10/9 9:45  | 仿冒公检法  | 02162906290是上海长宁公安分局    |
| 1    | 3684     | 0002162906290   | 2015/10/9 9:25  | 仿冒公检法  | 02162906290是上海长宁公安分局    |
| 1    | 3863     | 0002131134991   | 2015/10/9 9:26  | 仿冒公检法  |                         |
| 1    | 2220     | 0002162906290   | 2015/10/9 9:57  | 仿冒公检法  | 02162906290是上海长宁公安分局    |
| 1    | 4833     | 00059187621305  | 2015/10/9 9:17  | 仿冒公检法  | 手管标记诈骗电话                |
| 1    | 1954     | 0002134074800   | 2015/10/9 10:23 | 仿冒公检法  | 02134074800是上海闵行公安分局    |
| 1    | 4313     | 0002157823618   | 2015/10/9 9:47  | 仿冒公检法  | 02157823618是上海松江公安分局    |
| 1    | 3942     | 0002131134991   | 2015/10/9 9:56  | 仿冒公检法  |                         |
| 1    | 4154     | 0002163280123   | 2015/10/9 9:52  | 仿冒公检法  | 02163280123是上海南京东路派出所   |
| 2    | 3974     | 07975564128     | 2015/10/9 10:29 | 仿冒公检法  |                         |
| 2    | 8522     | 009902767122288 | 2015/10/9 9:08  | 仿冒公检法  |                         |
| 1    | 2957     | 0002227393016   | 2015/10/9 10:23 | 仿冒公检法  | 02227393016是天津西青公安分局    |
| 1    | 5347     | 0002156608111   | 2015/10/9 9:44  | 仿冒公检法  | 02156608111是上海宝山公安分局    |
| 3    | 656      | 0002165431000   | 2015/10/9 10:59 | 仿冒公检法  | 02165431000是出入境管理局      |
| 2    | 2242     | 0002110010      | 2015/10/9 9:56  | 仿冒公检法  | 10010是联通客服              |
| 1    | 2878     | 00075584468178  | 2015/10/9 10:36 | 仿冒公检法  | 075584468178是深圳龙岗经济稽查大队 |
| 1    | 4184     | 0002162906290   | 2015/10/9 10:13 | 仿冒公检法  | 02162906290是上海长宁公安分局    |
| 1    | 5234     | 0001085225050   | 2015/10/9 10:00 | 仿冒公检法  | 01085225050是北京市公安局      |
| 1    | 3315     | 0002157823618   | 2015/10/9 10:38 | 仿冒公检法  | 02157823618是上海松江公安分局    |
| 1    | 2051     | 0002195588      | 2015/10/9 11:06 | 仿冒公检法  | 95588是工商银行客服            |
| 1    | 4912     | 0002134074800   | 2015/10/9 10:25 | 仿冒公检法  | 02134074800是上海闵行公安分局    |
| 1    | 6752     | 0002162906290   | 2015/10/9 9:54  | 仿冒公检法  | 02162906290是上海长宁公安分局    |
| 1    | 7144     | 00059187621305  | 2015/10/9 9:42  | 仿冒公检法  | 手管标记诈骗电话                |

| 诈骗类型     | 备注信息                                                                    |
|----------|-------------------------------------------------------------------------|
| 仿冒公检法    | 客户被吓坏了，差点上当。后来收到我司发的信息才避免了损失。                                           |
| 仿冒公检法    | 无人接听                                                                    |
| 仿冒公检法    | 多次打此电话，都在通话中                                                            |
| 仿冒公检法    | 客户说对方先说要停他机，后来约他去谈怎么处理，客户去了。损失了100多                                     |
| 仿冒公检法    | 对方以公安局的人打的电话，收集了资料，还没提到转钱的事。客户收到我司的信息知道是骗人的了。                           |
| 仿冒公检法    | 客户表示没接这个电话                                                              |
| 仿冒领导熟人诈骗 | 客户表示对方以领导的身份给他打过电话，让他转钱过去，客户没转。                                         |
| 仿冒领导熟人诈骗 | 语音提示忙，不方便接听                                                             |
| 仿冒领导熟人诈骗 | 客户刚开始想信对方是他的领导了，后来转钱时，客户和他领导核实了一下。才知道是骗人的。                              |
| 仿冒领导熟人诈骗 | 客户表示对方以领导的方式打给他的，让帮忙打点钱过去。客户知道是骗人的就报警了，警方说这个号已经被拉黑，客户问已经拉黑了为什么还能打电话骗人？  |
| 仿冒领导熟人诈骗 | 客户表示已经转了2800过去。我们收到信息再打过去中间有了时间差，客户说打得太晚了已经被骗。                          |
| 仿冒领导熟人诈骗 | 客户表示对方以领导的身份给他打电话，他差点上当。因为收到我们公司发给他的信息他才知道是骗人的。                         |
| 仿冒领导熟人诈骗 | 客户刚好近期在面试工作，对方正好也是以领导的身份给他打电话，说要进公司要送2000的红包，客户正在犹豫要不要转钱，接到我司电话才知道是骗人的。 |
| 仿冒领导熟人诈骗 | 语音提示不方便接听                                                               |
| 仿冒领导熟人诈骗 | 客户刚好近期在面试工作，对方正好也是以领导的身份给他打电话，让他转钱过去。客户没转钱                              |
| 仿冒领导熟人诈骗 | 客户表示对方以领导的方式打给他的，让帮忙打点钱过去。客户知道是骗人的就没理                                   |
| 仿冒领导熟人诈骗 | 客户表示对方说是他领导，让帮忙转钱过去。客户没转。                                               |
| 仿冒领导熟人诈骗 | 客户表示对方约他谈业务，去到门面时有很多人。都说那人是他们老板。之后老板说他领导来了要送红包自己走不开，让他帮忙转钱过去才有时间和他谈业务。  |
| 仿冒领导熟人诈骗 | 客户说是他的朋友，我司提示他是骗人的电话，让他核实。客户还是表示是他朋友的电话。                                |
| 仿冒银行诈骗   | 客户表示对方打电话说他信用卡消费时签错单了，如果不去处理每月会扣他500元。客户一听知道是骗人的，就没上当。                  |
| 仿冒银行诈骗   | 客户表示对方是招商银行的，说有项业务出错了，要求去处理。客户没理会。                                      |
| 虚假客服电话   | 无人接听                                                                    |
| 虚假客服电话   | 客户要买机票，已经把钱转过去5000了。现在客户正在报警                                            |
| 虚假客服电话   | 对方说让他去银行操作，客户操作了，但账上没钱，所以没操作成功。之后接到我司电话才知道是骗人的。                         |
| 虚假客服电话   | 客户表示打过去是订机票，对方要转钱过去，-客户还没转。我司已经提示是诈骗电话来的。                               |

- 某直辖市运营商
  - 每日1.5亿话单
  - 上线测试2周，
  - 组织20个民警进行回访，每天深度电话回访300次
  
- 效果评估
  - 测试前此运营商用户受害者占总受害者的80%
  - 测试后统计，此运营商用户受害者降到23%



# 目录

contents

1 面临的安全挑战

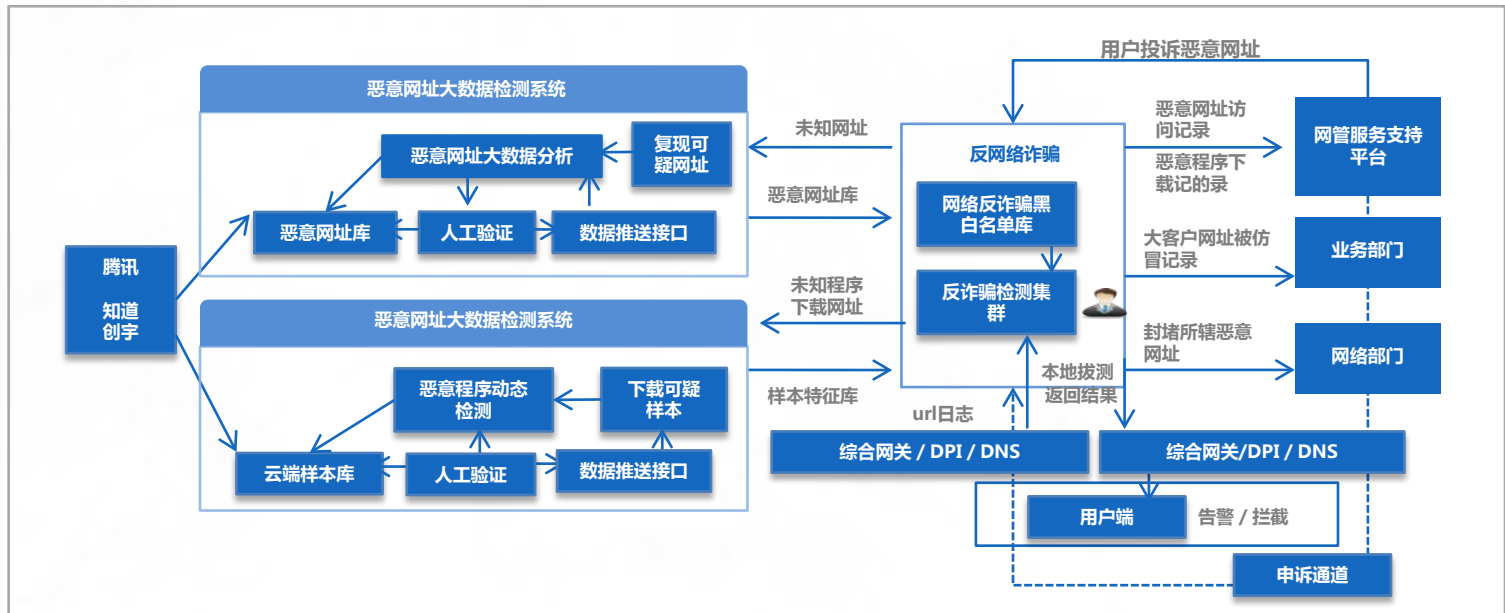
2 诈骗电话检测技术

3 反网址诈骗系统

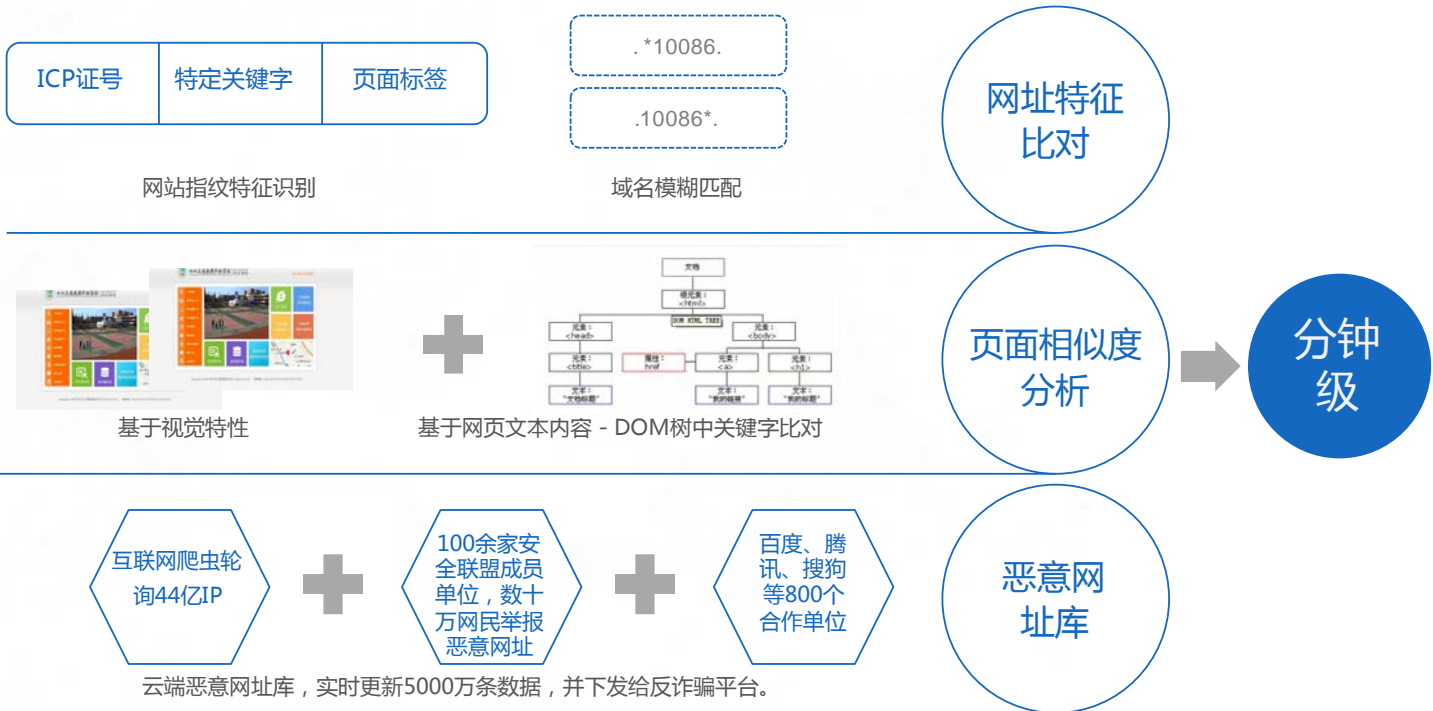


3

## 反网络诈骗云端计算中心



知道创宇以DPI / 网关/流控 / DNS提供上网url日志为基础数据，由反诈骗平台检测恶意网址和恶意app下载地址，提供给运营商的网关 / 流控设备对用户提出告警或屏蔽，形成一个反诈骗处理闭环，同时客服做不知情定制跟踪，业务部门对大客户网址被仿冒情况做通报，网络管理部门封堵所辖恶意网址。



### 检测方法：恶意网址黑白名单（云端产生，本地对比）



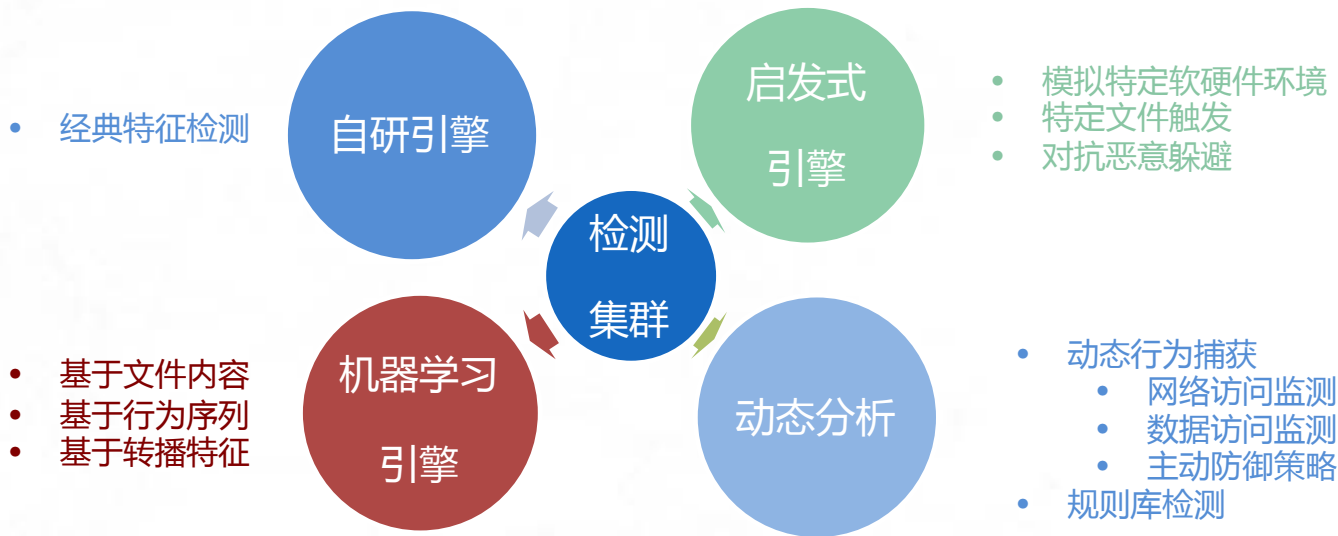
安全联盟是一个中立、公正权威的第三方组织，通过百度、腾讯、搜狗、知道创宇为首等近800家机构、企业等官方网站达成合作，可直接共享已经采集多年的恶意网址互联网数据库。

工业级互联网网站监测引擎，实时的对百度、腾讯每时每刻产生网址链接进行监测，日均处理百亿条以上数据，已经采集超过5000万条的诈骗信息数据，共享数据库。

腾讯目前针对互联网上的恶意网站、电话、APK病毒、PE木马进行大范围采集拦截，推出“天下无贼”反信息诈骗联盟，目前已有有效拦截4.4亿次诈骗网站。

面向整个互联网网民的安全联盟人工举报平台，共享数据库；中国移动xx分公司人工举报平台数据输入接口；电话、人工发现等渠道举报入口。

中国移动xx分公司本地日志留存系统数据入口；DNS域名解析系统流量镜像，提取解析域名信息；



### 检测证书





用户手机端拦截页面



无锡网警提示您:



访问该网页!

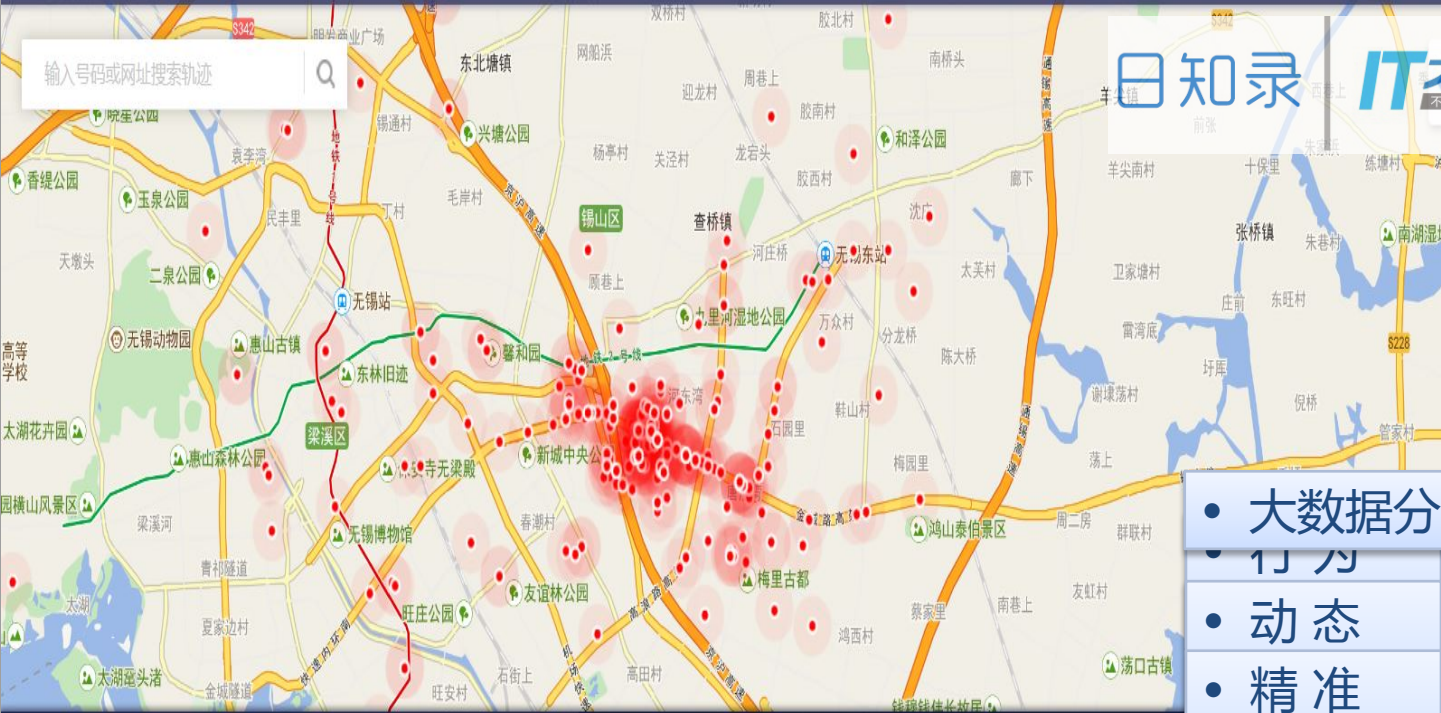


连接下载的文件存在  
行可能会损坏您的电  
长号信息

继续访问 (不推荐)

详情介绍

保证用户端反应不超过 **30毫秒**



输入号码或网址搜索轨迹

日知录 IT大咖说 不止于技术

- 大数据分析
- 行为
- 动态
- 精准研判

| 伪基站摘要       | 次数 | 最新活跃...  | 轨迹 | 出警时间 | 出警 | 时间                  | 伪...  | 短信内容                                                          | 地址                |
|-------------|----|----------|----|------|----|---------------------|-------|---------------------------------------------------------------|-------------------|
| m.ryylt.com | 39 | 14:46:22 | Y  | 未出警  |    | 2016-08-05 14:46:22 | 95533 | 尊敬的用户：我行将开展个人信息核实认证，请登录m.ryylt.com 按提示核实，未核实账户将于今日24点冻结【建设银行】 | 江苏省无锡市新吴区向阳路      |
| m.rzzlt.com | 1  | 13:32:24 | Y  | 未出警  |    | 2016-08-05 14:44:26 | 95533 | 尊敬的用户：我行将开展个人信息核实认证，请登录m.rzzlt.com 按提示核实，未核实账户将于今日24点冻结       | 江苏省无锡市新吴区长江路1号旺庄路 |





日知录

IT大咖说  
不止于技术



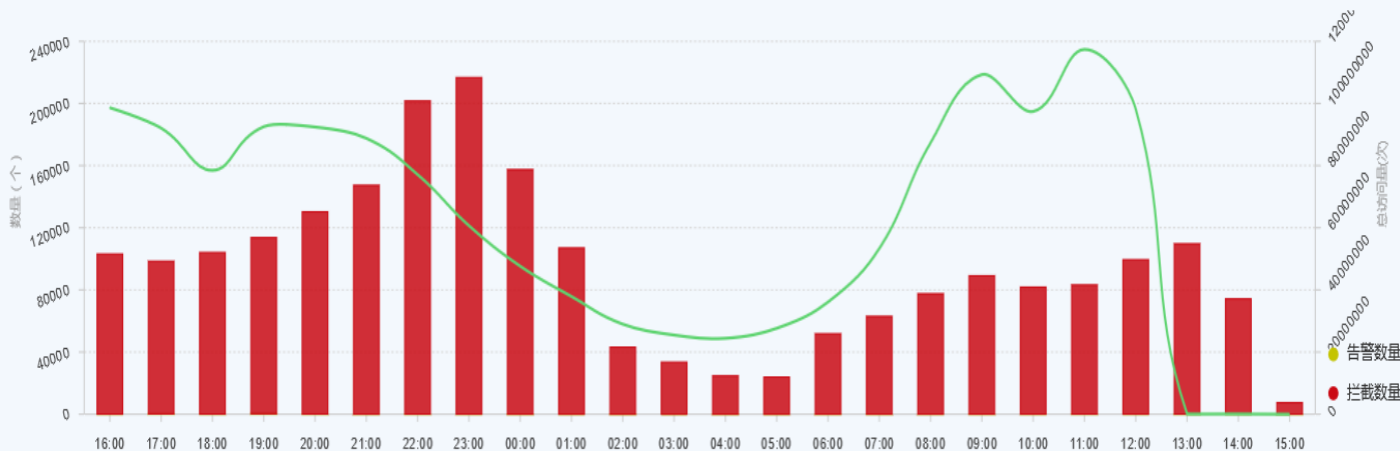
诈骗网址数量  
224.14万



告警数量  
1691

拦截数占比: 99.92%

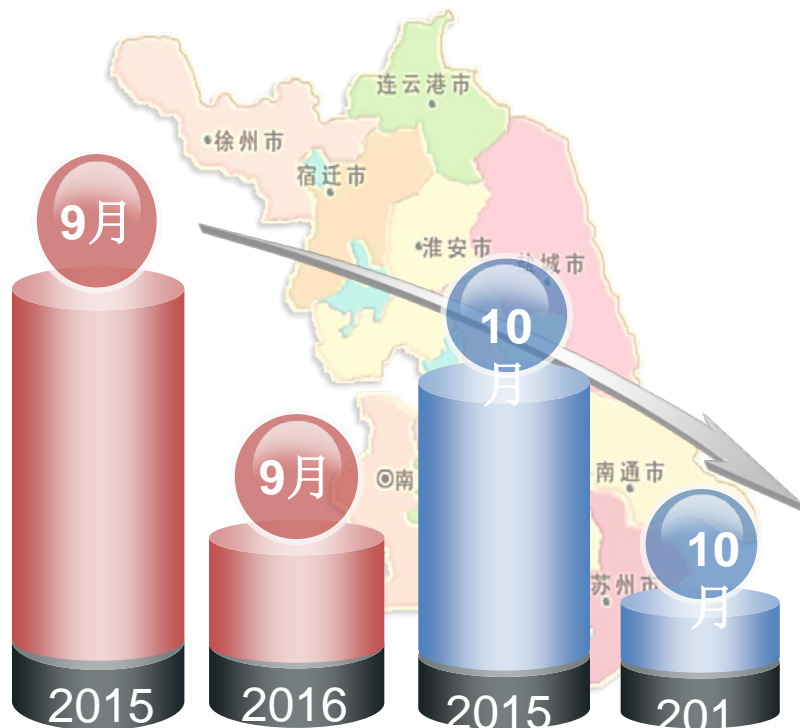
实时数据



# 无锡公安项目运行以来成效

日知录

IT大咖说  
不止于技术



今年9月，全省网络诈骗案件中涉及网址诈骗发案同比下降**48.2%**，我市同比下降**72.3%**。

10月1日至20日，全省网络诈骗案件中涉及网址诈骗发案同比下降**47%**，我市同比下降**88%**。

# 目录

contents



1 面临的安全挑战

2 诈骗电话检测技术

3 反网址诈骗系统

4 其他技术手段

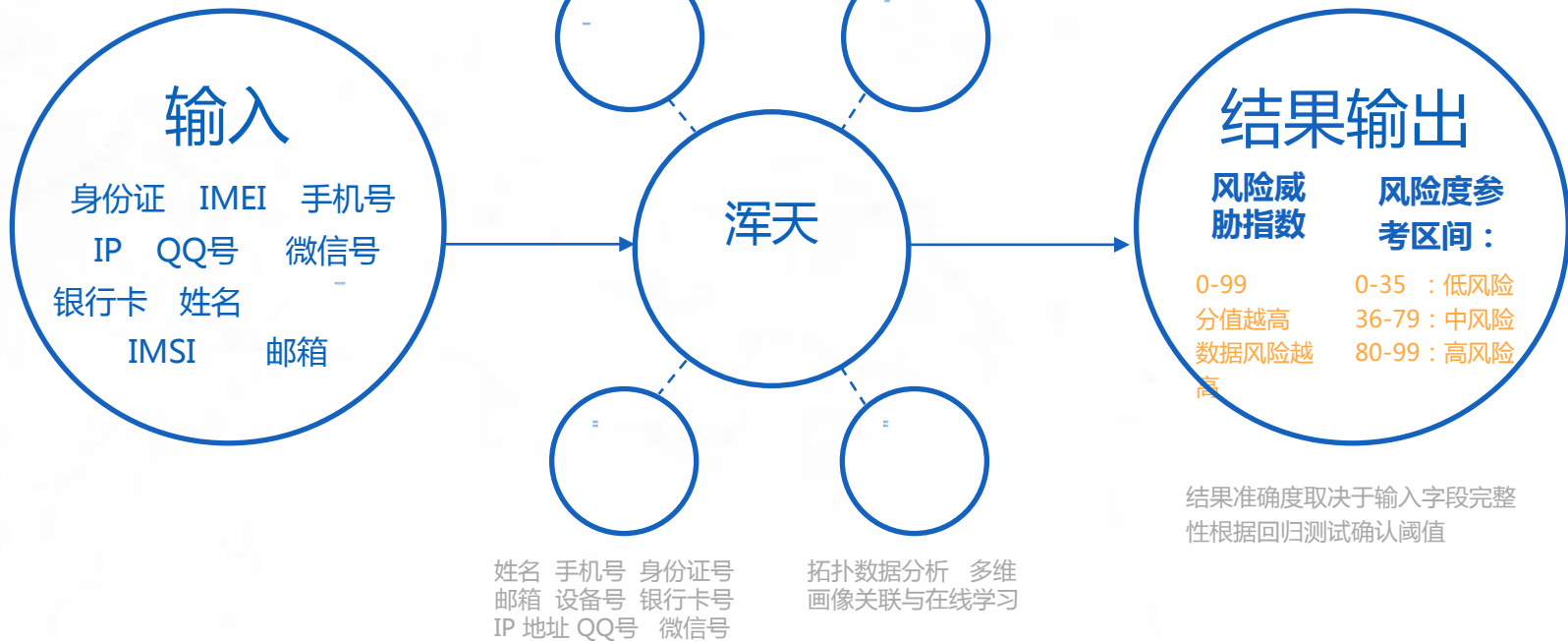
# 业务反欺诈

日知录

IT大咖说  
不止于技术

黑产数据 欺诈数据  
位置数据 爬取数据  
代理数据 公安数据  
设备指纹 运营商数据

登录保护 注册保护  
活动防刷 提现保护  
支付保护 短信保护  
借贷申请保护



结果准确度取决于输入字段完整性  
根据回归测试确认阈值

- 钓鱼网站反制技术手段进入后台系统
  - 取证诈骗分子信息
  - 提取受害人信息，由相关机构提醒
- 诈骗分子溯源
  - 在后台植入探针，实时取证定位
- 境外诈骗分子定位

日知录

IT大咖说  
不止于技术

THANKS