

# 守护网民安全，大数据驱动反诈骗

腾讯安全云部资深专家 邵付东

TENCENT

# 信息诈骗无处不在

---

# 信息诈骗成最大的网络黑色产业

## 回国探望生病老父一个电话他被骗991万 甘肃乡村教师23万积蓄被电话诈骗后自杀

2016-06-09 08:41:00 来源: 钱江晚报(杭州)

2016-05-22 17:18:49 来源: 澎湃新闻(上海)

(原标题: 回国探望生病老父一个电话他被骗991万)

中了大奖请交税费手续费、账户涉嫌诈骗洗钱请配合调查、孩子晕倒了被绑架骗,各路媒体一直在频繁报道。但时不时的,还是有人上当受骗。今天的这两起新闻奇之处,可惜的是,都得逞了。

尽管说了一百遍,恐怕还得再说一百零一遍:为了防止被骗,千万不要轻信微信。决不能因贪图小利而放松警惕性。决不能向对方透露自己和家人的身份情况。特别是涉及转账、汇款等事项,一定要核实清楚再做决定,决不能向陌生人转

“你被通报了”,老套的通讯诈骗,这回盯上了刚回国的他

回国探望生病老父

一个电话他被骗991万

(原标题: 夺命电话: 甘肃一乡村教师23万积蓄被骗后自杀,生前极节俭)

澎湃新闻记者 王健 发自甘肃天水




七件套的锦缎寿衣,是范银贵穿过的最好的衣服——在他自杀的时候,身上仍穿着姐给他做的一件灰白格子西服。

这个甘肃天水秦安县的乡村教师,以常人难以想象的节俭,积攒了23万积蓄,买下一套属于自己的房子。

但一个电话击碎了范银贵的全部希望,一个电话让他倾家荡产。为了洗清嫌疑,他不得不卖房、卖车、卖地,要冻结全部资金。

胆小内向的范银贵轻信了,他分两次给对方转账,对方却迟迟不接电话。等他反应过来时,积蓄已经空空如也。

## 深圳工程师遭电信诈骗,40天损失1127万

上网日期: 2015年06月03日 我来评论 字号 放大 | 缩小 分享到:   

今天上午,广东省公安厅召开新闻发布会,披露了深圳、珠海“2·07”特大跨境电信诈骗案。该案中,深圳男子常某被诈骗集团冒充青岛市公安局、检察院、法院等机关,持续40天连环诈骗掉1127万元。

据悉,被骗事主为深圳一家高科技公司的工程师。骗局从2014年12月21日开始。当天,常某接到自称顺丰快递的电话,称他通过顺丰快递寄了28张卡到泰国。事主矢口否认,表示没有寄过。对方威胁称,这么说来你的公民信息有可能被人盗用来洗钱,我给你转到公安局。而对方所转接的电话,在常某看来,与公安局的语音提示一致。参与办案的民警表示,该案涉及金额巨大,受害人数众多。

信息诈骗案例愈演愈烈  
与每一个人息息相关?

深圳市宝安公安机关接到事主报案,称其2014年12月21日至2015年2月1日,40天被冒充青岛市公安局、检察院、法院等机关,以其涉嫌洗钱黑钱为由诈骗人民币1127万元。同月,广东省深圳、珠海两地也接连发生多起跨境电信诈骗案件。

诈骗之害

2014年,全国电话网络诈骗发案40余万起,群众损失**150亿元**

2015年,因为电话网络诈骗造成的经济损失达**222亿元**

2013年至今,全国发生被骗千万元以上的电信诈骗案件超94起,百万元以上的案件2085起

# 信息诈骗的三大新特点



## 大数据

### 大数据成为信息诈骗的工具

诈骗分子会根据购买到的用户个人信息数据进行详细分析，并根据用户信息的特点设计诈骗环节和故事。

## 高精度

### 撒网式诈骗向精准诈骗升级

个人信息泄露，网站漏洞导致黑客入侵等，诈骗分子掌握了受害人的详细资料，衍生出各种有故事，有场景的“精准诈骗”。

## 大数额

### 诈骗个案金额越来越巨大

上百万或千万的案例越来越多，诈骗方式升级、诈骗人群变化、诈骗手段高科技都让诈骗分子可以骗到巨额资金。

# 反信息诈骗面临三大严峻挑战

- 信息诈骗与高科技手段结合，打击难度大
- 社会工程学进行诈骗，民众防范意识低
- 相关法律法规不健全，监管亟需加大力度



# 幕后推手：黑色产业链

---

# 黑色产业链走精细分工模式，形成规模经济

- 黑产的开发、传播、运营、洗钱每个步骤都有精细的分工模式
- 坏人模式多变，传统的事后黑名单的打击方式比较滞后
- 现状很恶劣，却没有明确的责任人



- 病毒开发
- 恶意网站制作
- 黑卡、改号线路

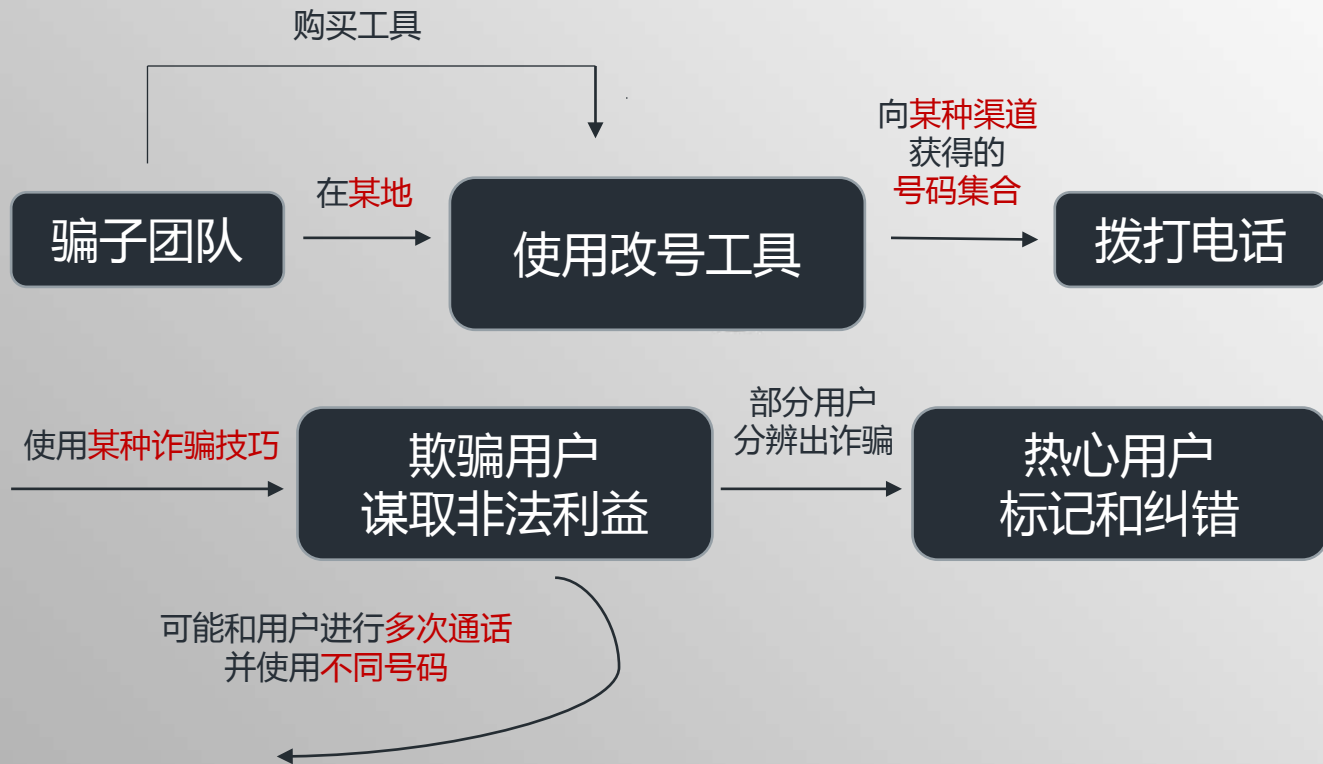


- 电话拨打
- 伪基站
- 短信群发



- 取出受骗资金
- 转移受骗资金

## 流程图



## 黑色产业链 运作流程



# 支付类病毒黑产



# 支付类病毒 黑产



银行卡

支付平台

洗钱

- 游戏充值
- 油卡充值
- 转账
- 在线购物
- 线上POS
- 话费充值

网上金融  
信用卡

套现

银行卡盗刷的资金流向：  
游戏充值、话费充值、彩票充值，  
网上购物、洗钱小公司

# 腾讯守护者计划：大数据驱动

---

TENCENT

# 腾讯守护者计划：开放合作

腾讯守护者计划是2015年腾讯公司成立的一个专门针对电信网络诈骗的联合开放品牌。基于腾讯主导的反诈骗联盟的成功经验，发挥腾讯海量大数据优势，与公安部、工信部一起，联合银行、运营商、企业一起对电信网络诈骗重拳出击。



犯罪打击



行业联合



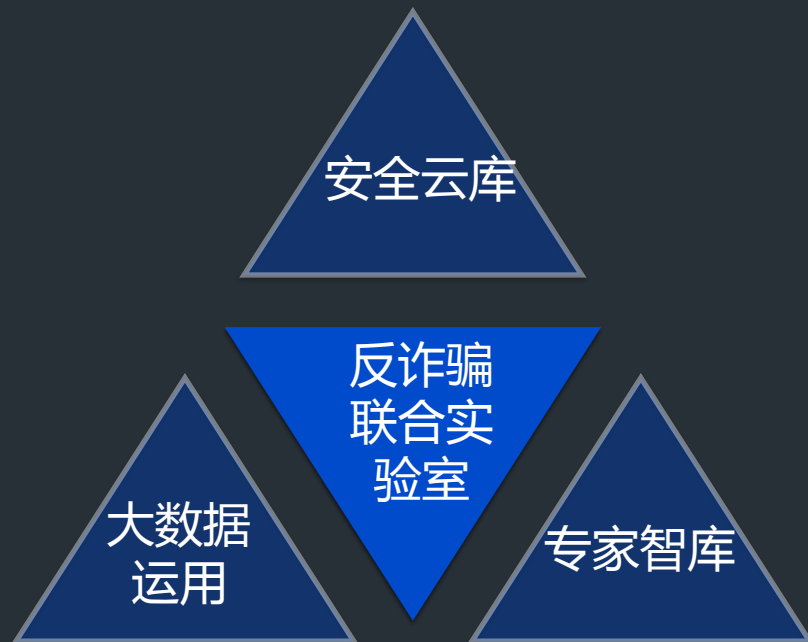
宣传教育



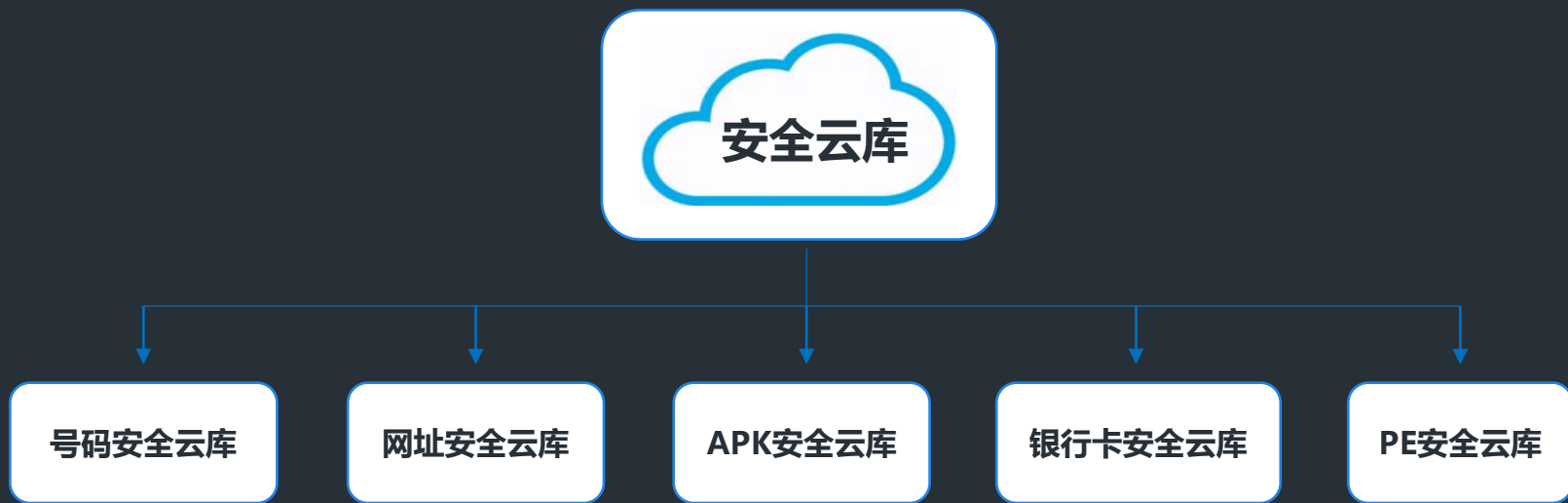
技术研究

# 腾讯守护者计划：反诈骗联合实验室

旗下成立由公安、银行、企业、运营商等反诈骗专家组成的智库，推动反诈骗实验室的技术方向。



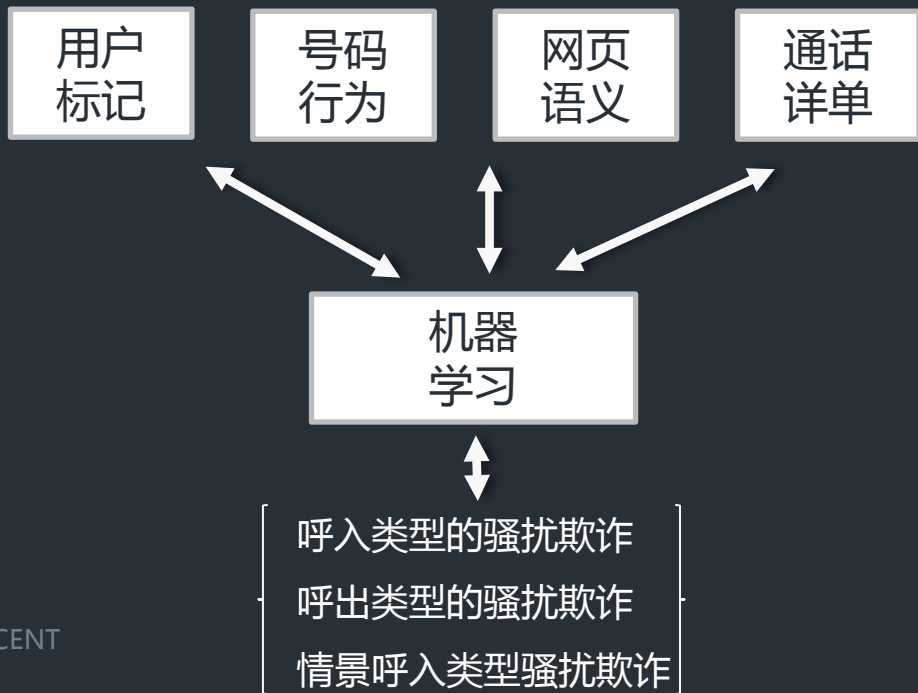
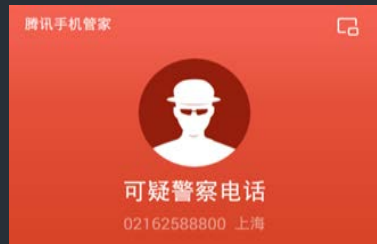
# 腾讯的五朵安全云库涵盖黑产作恶的主要要素



利用腾讯海量计算和存储资源，每天对海量的用户行为和程序运行过程进行数据建模  
在十年QQ黑产打击经验基础上，运用机器学习的方法，来识别互联网上的恶意数据

# 欺诈号码云库

- 250W的活跃欺诈号码库
- 鹰眼盒子首创基于话单事中发现受害人，解决改号诈骗难题
- 主动预防，提高坏人作案成本



# 腾讯网址安全云库

- 1.9亿的活跃黑网址库，每日提供350亿次安全服务
- 日检测恶意网址3000W条，检测能力业界第一
- 从域名注册到主机绑定到传播到下载，保证最全覆盖





# 腾讯APK安全云库

- 3500W的活跃APK黑库，业界最大
- 基于大数据分析，2014年配合警方6个小时破案 “XX神器”



- 国内首家通过了专业权威AV-C认证
- AV-C省电单项目测试的最好成绩



- 连续2次高分通过AV-TEST
- 两次测试也都实现了零误报



- 全球首次西海岸获得7项权威认证

XX神器，8月1日出现，次日爆发；当日转发含病毒链接短信达681.3万

腾讯安全当日令病毒传播迅速消灭，9小时协助警方抓获疑犯

看这个，<http://cdn.yyuplo ad.com/download/4279193/XXshenqi.apk>

转自：  
13910910156 (+8613910910556)  
各位亲朋好友：收到短信请立即删除，病毒短信，不要打开，打扰了！

10:25

动态监测发现大面积终端短信异常

10:30

手管捕捉终端异常病毒线索

10:40

大数据评估影响，判断危害性、传播性

10:59

病毒入库、挖掘嫌疑人在木马中预留的后台信息，确定嫌疑人位置

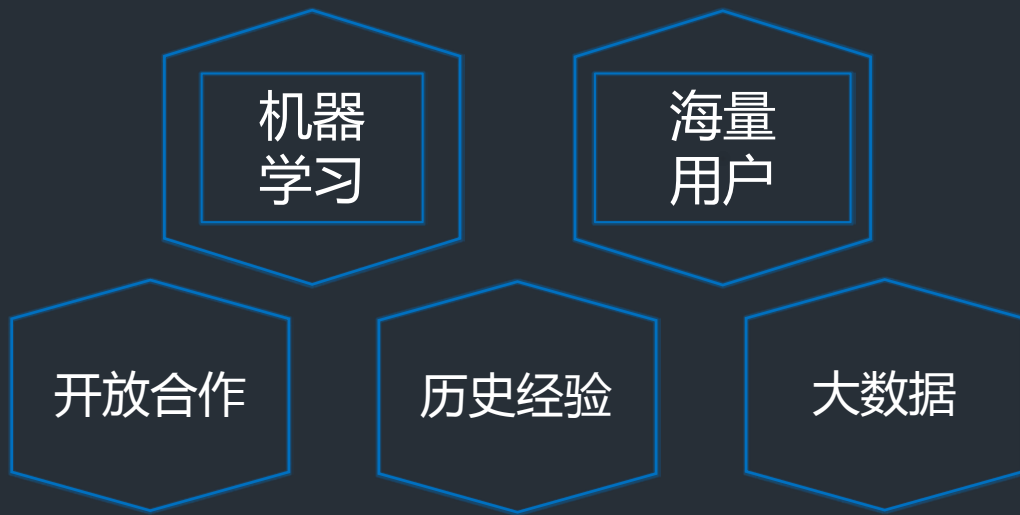
13:32

完成木马样本分析，下发策略、手机管家率先在全网开始完美查杀

16:00

深圳警方将木马病毒制作人李X抓获

# 打击社工诈骗：腾讯优势



多年的QQ黑产对抗经验

+

海量计算能力

黑产的传播渠道大数据

TENCENT

# 过去的反诈骗



缺乏技术手段



合作割裂



难打难防



主要依靠事前教育，事后打击

# 反诈骗流程革命

TENCENT

# 反诈骗流程革命

## 传统做法



### 基于事前教育

- 普适教育：浅层提醒  
内容滞后



### 基于事后弥补

- 报案：难度大，成本高
- 冻结：有一定作用，还是会造成损失

从“事前、事后”到“事中”



## 创新做法

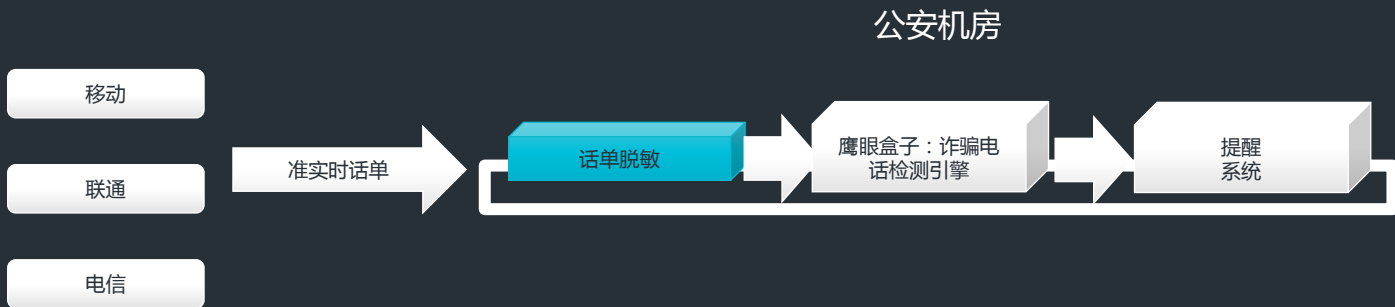


### 基于事中提醒

- 发现：准实时检测进行中的诈骗通话
- 提醒：短信+语音提醒，叫醒受害人
- 阻断：受骗被中止，完全避免损失

# 鹰眼盒子合作案例与效果数据

- 公安负责以十分钟粒度来采集准实时话单，然后对话单进行脱敏
- 鹰眼盒子负责依据脱敏后的话单来建模识别恶意号码和潜在受害用户
- 公安对潜在受害用户进行电话提醒，阻断其转钱
- 所有的数据在公安内网流转，没有隐私和安全风险



# 鹰眼盒子-北京实践效果数据

从服务器到  
话单准备

16个警察每天  
电话回访

每天预计  
挽回损失

2周

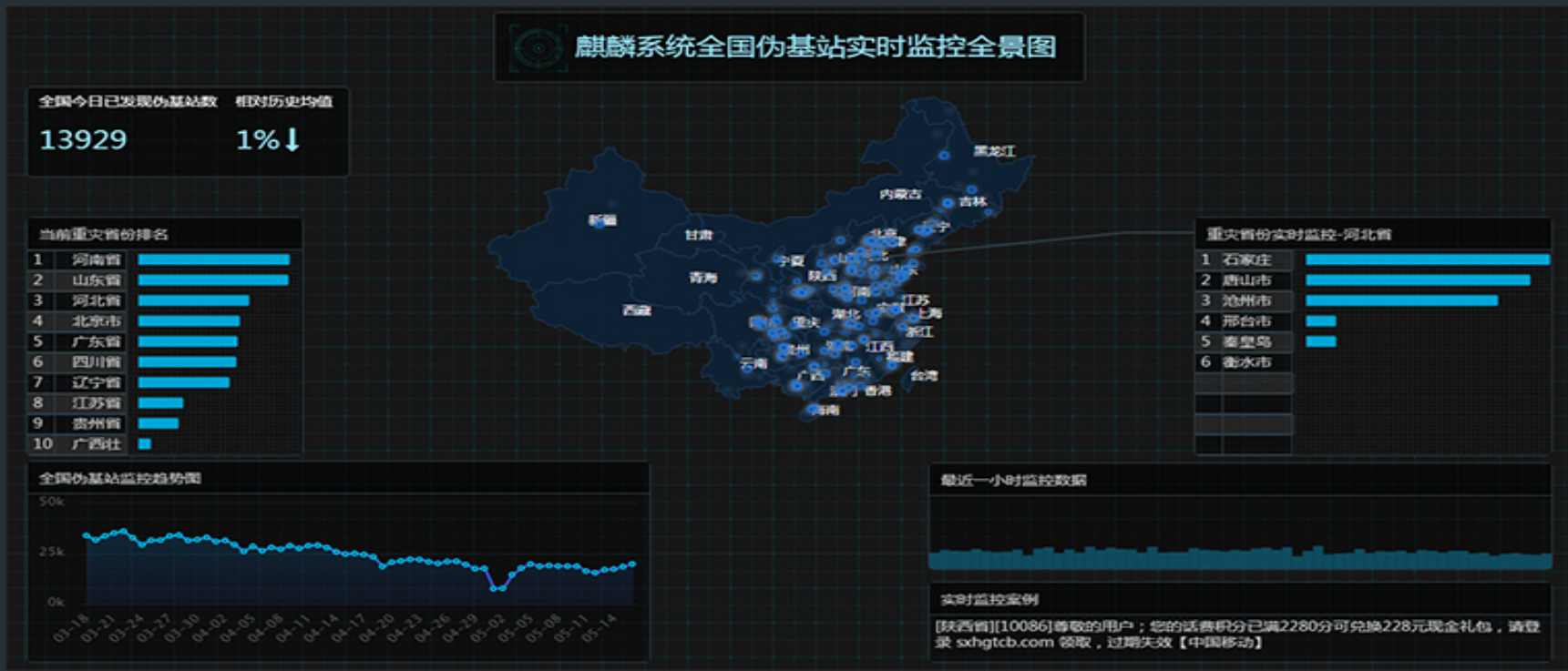
500人

100W



# 麒麟伪基站实时监控系统

- 客户端检测 + 云端大数据分析 + LBS定位
- 实时定位，及早抓捕





# 麒麟伪基站系统合作案例与效果数据

- 北京破案72起， 缴获伪基站设备77套， 抓获嫌疑人107名
- 深圳打掉11个团伙， 缴获伪基站设备53套， 抓获嫌疑人



**腾讯安全，值得信赖！**

TENCENT