# 互联网金融安全实战浅龙

行山 居

# 关于我和我的团队

付山阳 湖南人 爱好篮球和游泳

10 years+安全产品开发和安全运营的工作经验

平安科技产品安全团队负责人(白泽安全团队)

平安银行互联网金融安全负责人

## 

- 一、互联网金融-清算系统安全
- 二、互联网金融-移动客户端安全
- 三、互联网金融-业务安全

# 互联网金融 - 清算系统安全

网上银行

手机银行

电话银行

银行核心

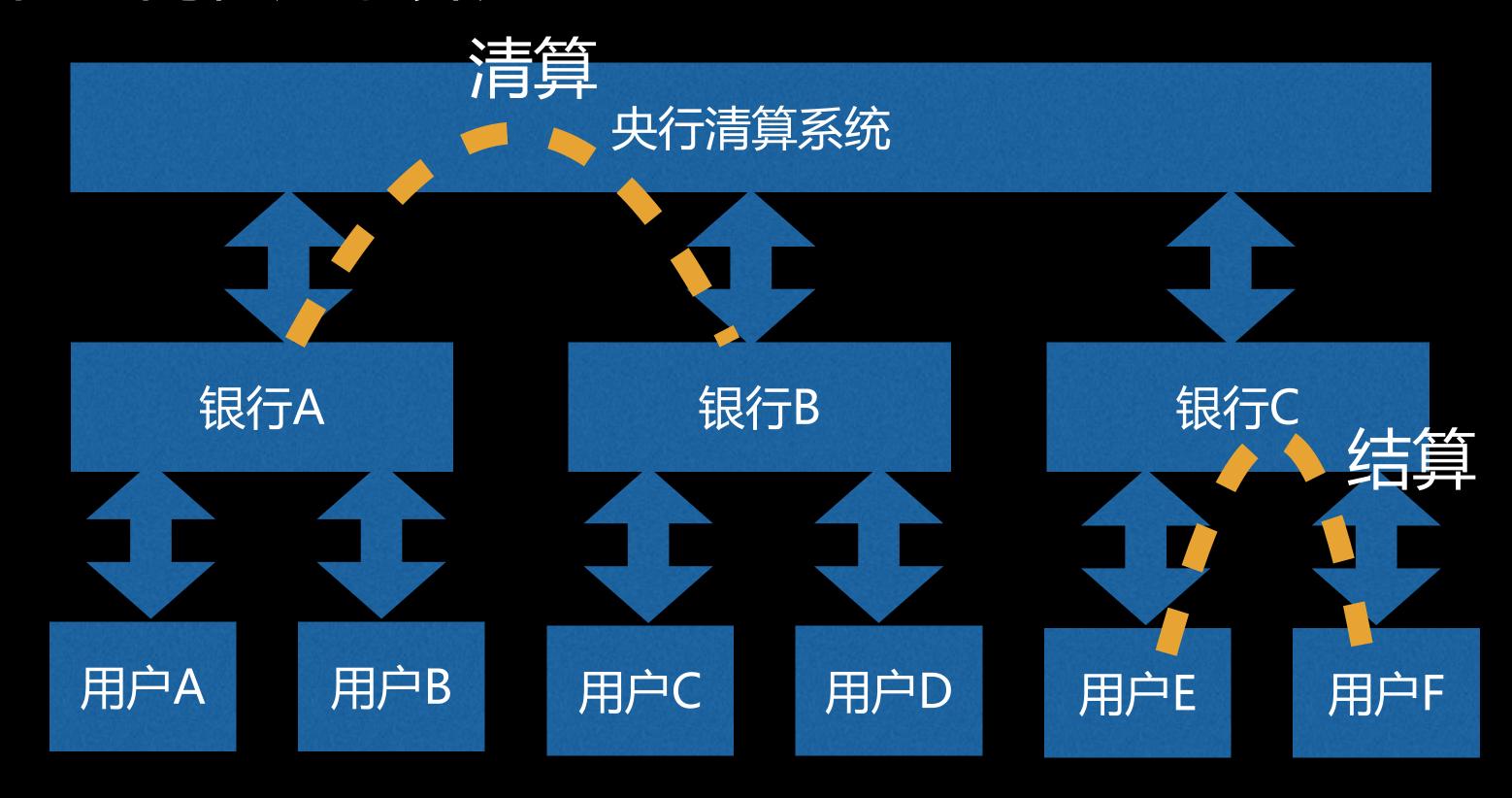
ATM前置

清算系统

•••••

# 什么是清算系统?

- 通俗地讲,银行与商户、消费者之间为结算关系。
- 而银行与银行之间构成清算关系。



# 史上最大银行抢劫案!

8100万 = 6吨 fandation = 9亿

# 盖加拉提行被攻击台边程

2、攻击实施

黎刹商业银行 收到4笔共8100 万美元,并经过

1、攻击准备两次转账,进入 3个攻击木马 3个赌场账户 完成编码和 其余31笔9亿美 编译 元汇款被暂停

3、清除痕迹 修改了其中2 个攻击木马,用 来消除攻击痕迹 4、发现并追索

孟加拉国央行 5、洗钱成功 发函要求黎 刹商业银行中被分5次提取 止转账并退款

8100万款项

2月4日 2月4日 13时45分39秒晚些时候

2月5日 11时46分20秒

2月8日

2月9日

# 孟加拉银行被攻击原因分析

一、事前网络隔离,访问控制,权限管理等都很糟糕,密码复杂策略等等都没有。

二、事中措施不到位,没有基于网络和主机的入侵检测安全系统,没有有效的对账系统。

# 清算系统的基本IT安全措施建议

#### 事前

- •银行跟银行之间应该采用专线传输和双向认证
- •SWFIT系统应该部署在单独的服务器上,并且进行网络隔离
- •网络访问应该限制到IP+端口
- 勤快的打补丁
- •定期的安全演习

#### 事中

- 要有网络入侵检测和主机入侵检测系统
- •有效的对账系统,区块链能在这块起一定的作用。

#### 事后

• 要有成熟快速的应急响应流程,对各种攻击都要有预案。

# 国内的清算系统安全准备好了吗?

安全应该跟业务同步发展!

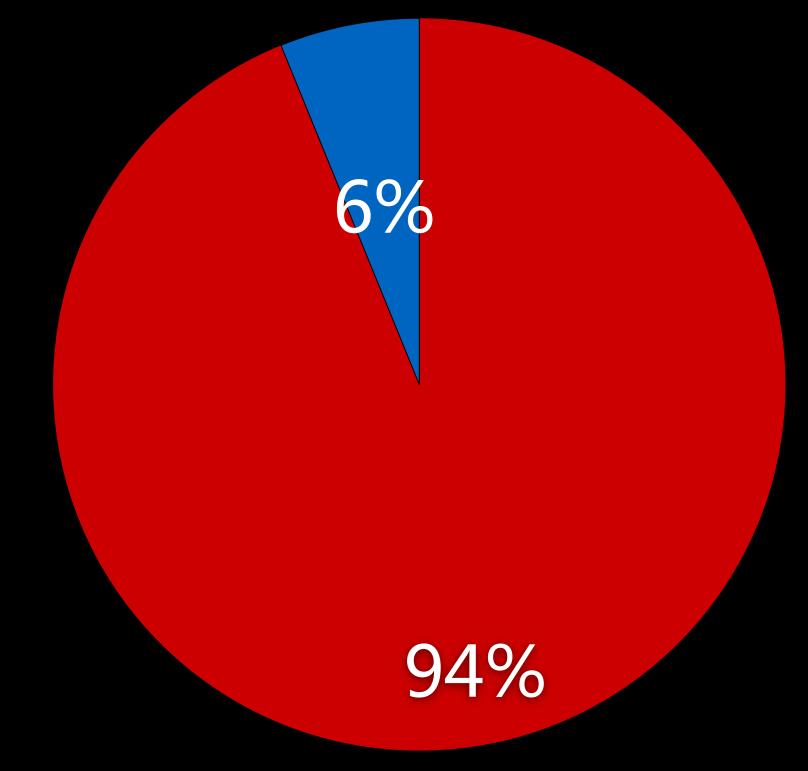
## 

- 一、互联网金融-清算系统安全
- 二、互联网金融-移动客户端安全
- 三、互联网金融-业务安全

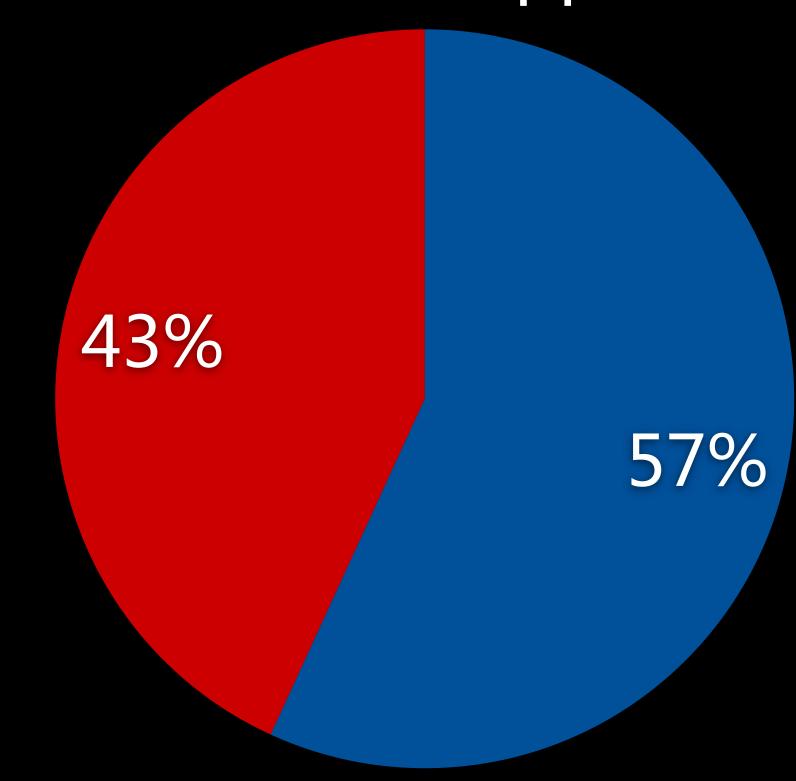
# 互联网金融的移动客户端安全需提升

我们白泽安全团队分析了146款互联网金融类APP,其中存在中风险安全漏洞的占比达 94% (共137 款APP),平均每款APP存在漏洞 11 个,此外63 款APP存在高风险安全漏洞,占比达 43%。

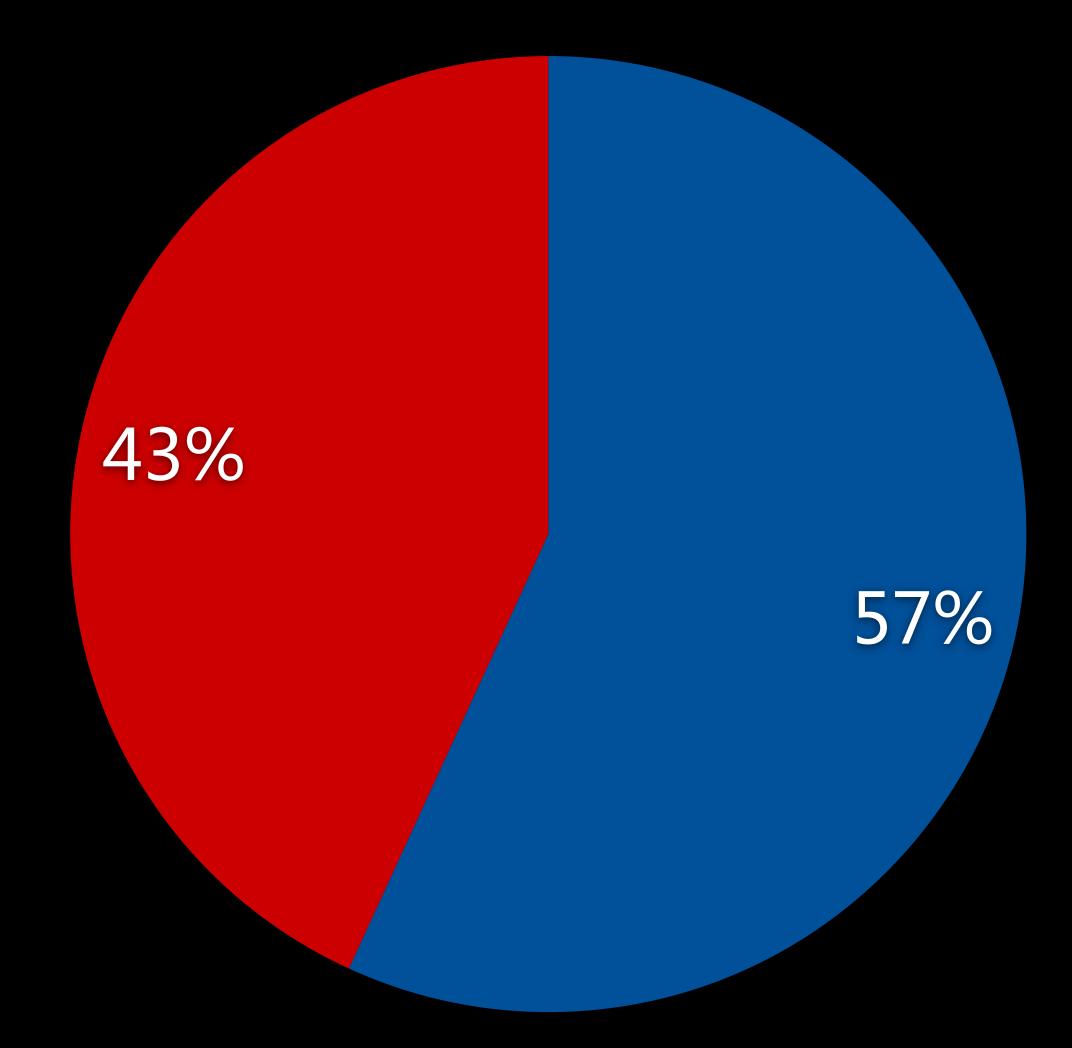




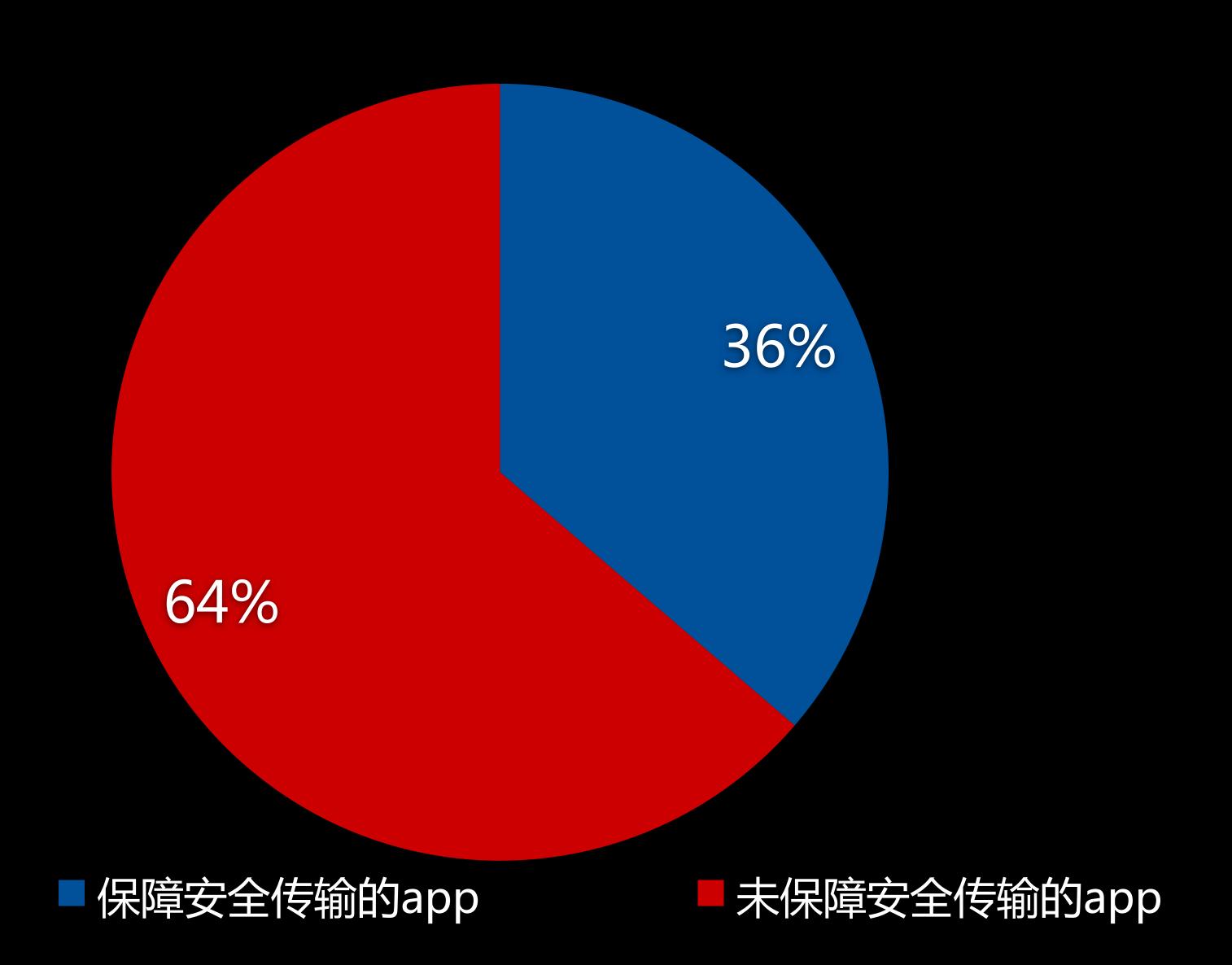
#### 高风险漏洞app占比



# 四成app存在webview代码注入漏洞

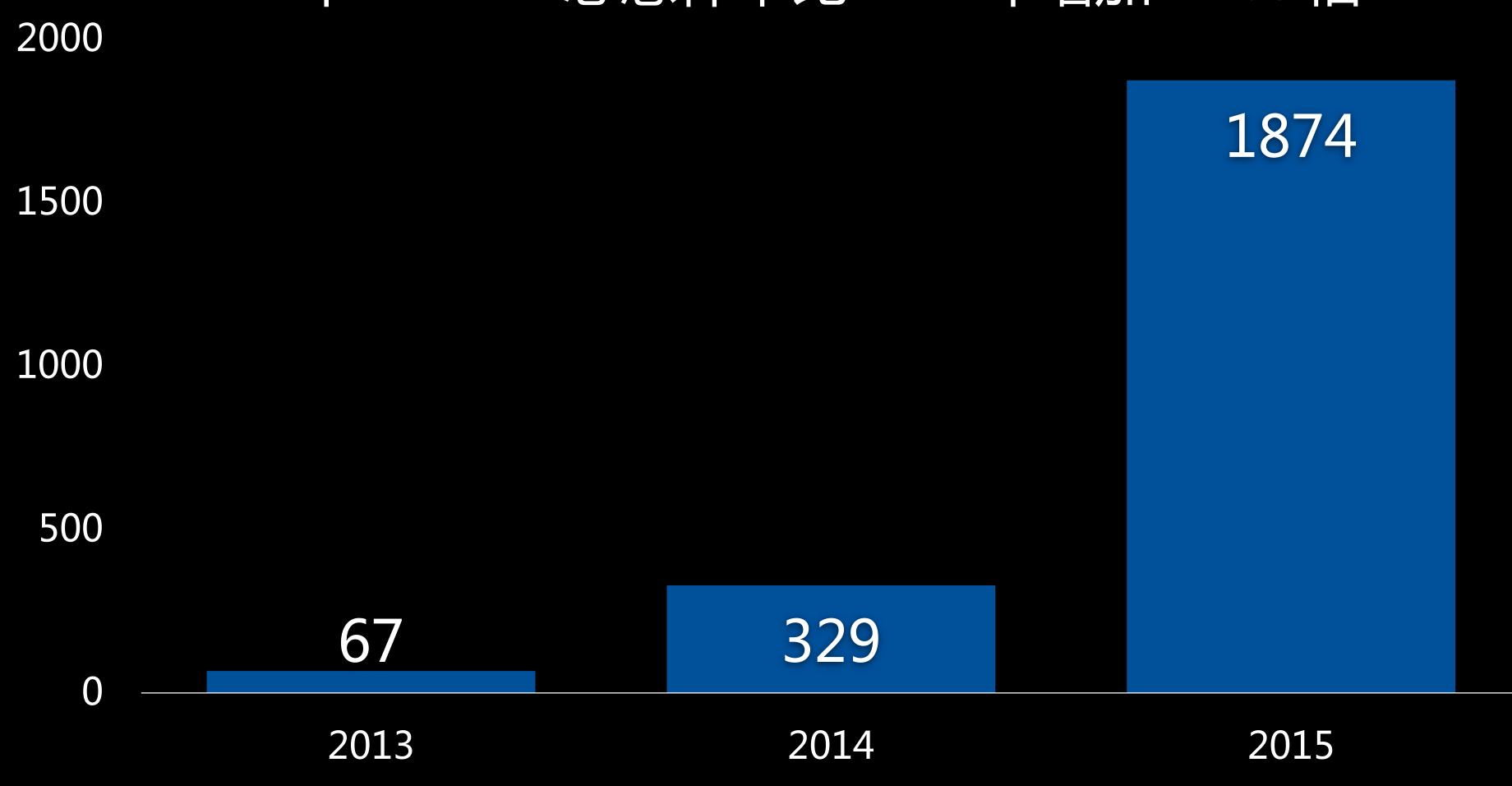


# 六成以上的app未能保障安全传输



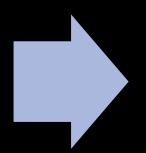
# 移动客户端恶意软件问题比较突出

2015年android恶意样本比2013年增加27.9倍

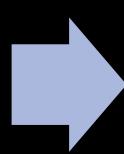


## 互联网金融类android木马的逆向分析

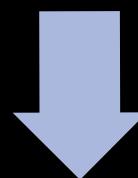
启动正版的金融 app



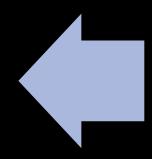
钓鱼app弹出登录 界面



盗取用户的姓名密 码等敏感信息



把姓名密码,以及短信发送到后台



监听手机短信

## 互联网金融类android木马的后台调查

福州市佛教居士林 乌山小区 ● 大洋晶典 育 弥陀寺 黨 蒙泉观音庵 萬 高爷庙 鼓楼区博物馆 福州北欧圣诞主题乐园 美 天章台 萬 冲天台 善 黎公亭 英 天香台 乌山历史风貌区 胡也频故居金 弟 先警亭 福州市委福州市政 府人民来访接待室 第 邻雪台 **弟** 沈葆桢祠堂 龙津陶瓷厨 双峰梦 中国工商银行图 号 乌山苑-东门 **善** 东壁亭 向阳峰 西河里新村 海阔天空 ⊙ 独木成林 一黎明戴斯酒店 梅聚 美餐榕 = 福州市教场小学 大厦车库-出入口 望耕台 福州市教场小学 福建移动 社区教育委员会 通信大厦 血 洪腾苑 0 洪腾苑 P 1 教场小区 协和公寓 血 南洋新村 № 乌山社区 加洋新村 加洋新村 东辰小区

## 移动木马攻击的防御建议

## 事前

- •你发给用户所有的短信都不要带链接。
- •提示用户不要点击任何短信链接

## 事中

•检测是否有activity劫持的情况,并提示用户

#### 事后

•利用用户画像,对钓鱼盗号的登录行为进行判别,阻止盗号者登录。

## 

- 一、互联网金融-清算系统安全
- 二、互联网金融-移动客户端安全
- 三、互联网金融-业务安全

# 互联网金融-业务安全

伪冒身份开户

绑卡盗刷

黑中介骗贷

# 伪冒身份开户影响很严重

伪冒身份开户会导致以下两大风险:

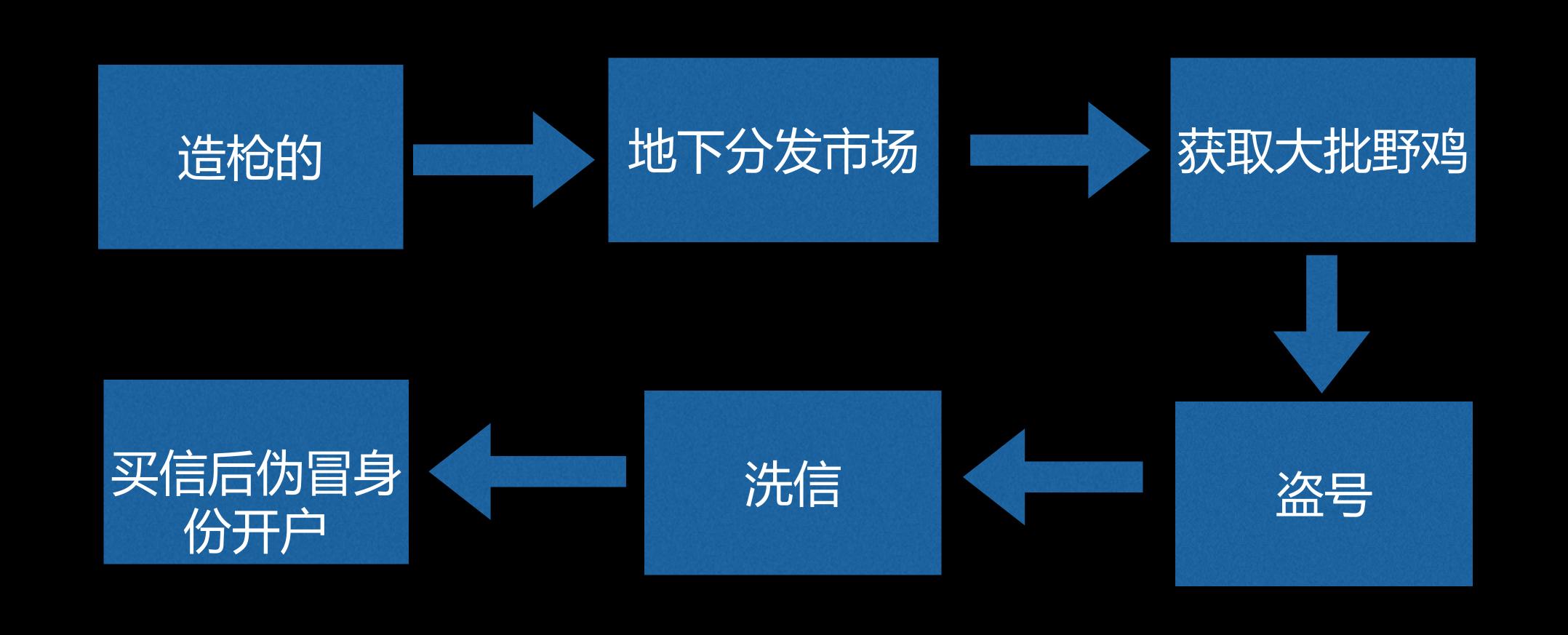
1、洗钱

《中华人民共和国反洗钱法》、《金融机构反洗钱规定》等法律规定金融机构应履行反洗钱义务,否则会被吊销牌照。

2、骗贷

骗贷会让创业中的互联网金融公司资金损失严重,甚至直接破产

# 伪冒身份开户的产业链分析



# 洗信方式与传统金融时代有所变化

黑产

传统金融

通过转账取现 来转移被盗账 户内的资金

获取短信 密码 验证 码 验证 号 敏 感信

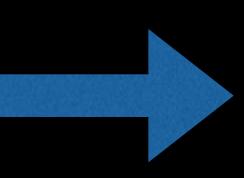
互联网金融

通过绑卡来转 移被盗账户资 金 利用其它金融业务的漏洞换卡洗信

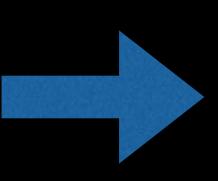
利用打车软件洗信

## 传统漏贷的套路也出现在互联网金融上

黑中介挑选合适 作案地点

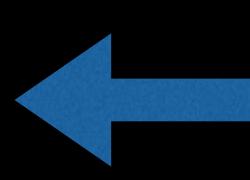


挑选容易得手 的作案对象

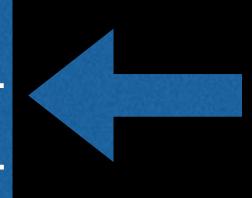


许诺注册app给予物质或金钱回馈

黑中介转移贷款账号内的资金



黑中介成功注册互联网贷款账号



受害者提供姓名,身份证号,银行卡,银信验证码,并配合一系列认证。

## 总结

#### 清算系统安全

- •分析了孟加拉国央行清算系统的案例,以及这件事件给我在安全建设上的启示。
- •国内的互联网金融安全企业需要注重发展与安全同步进行
  - 互联网金融app有很多的中高风险安全问题,普遍安全投入都不够。
  - •移动端的钓鱼问题比较突出,而且有从技术导向转向商业导向的趋势。

# •分享了三个业务安全的案例,伪冒身份开户导致洗钱,骗贷,影响很严重;洗信的方式与传统金融下有所差异;传统金融的骗贷套路也用到了互联网上。

#### 移动客户端安全

#### 业务安全

# Thanks & QA

