OWASP
Open Web Application
Security Project

AI VS AI，反欺诈正邪角力

宋超

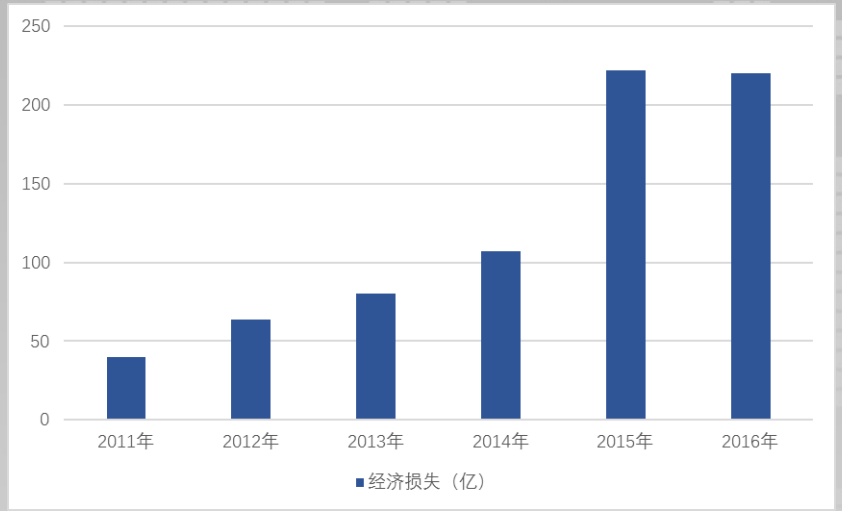
目录

CONTENT

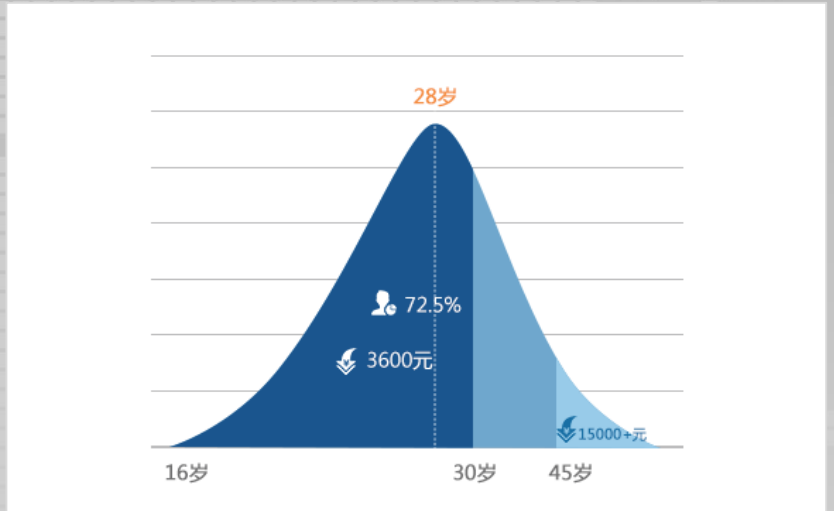
Part
01

欺诈态势

1.1 欺诈态势分析



2011-2016年上半年电信欺诈损失金额趋势图



各年龄段平均经济损失图

2011年至2015年，五年共造成经济损失**550亿元**，平均每年涉案金额的增长比例约为**60%**。由2011年的40亿元增长到2015年的222亿元，增长了近**5.6倍**。2016年电信欺诈形势仍不容乐观，仅上半年就立案**近百万件**，造成损失**逾两百亿元**。各年龄段群体均存在不同程度的经济损失，28岁是网络诈骗受害者最为集中的群体；16-30岁是网络诈骗受害者最为集中的年龄区间，占受害者总数的72.5%。 45岁以上的受害者平均损失最大，超过15000元。

1.2 公安部反欺诈工作开展情况

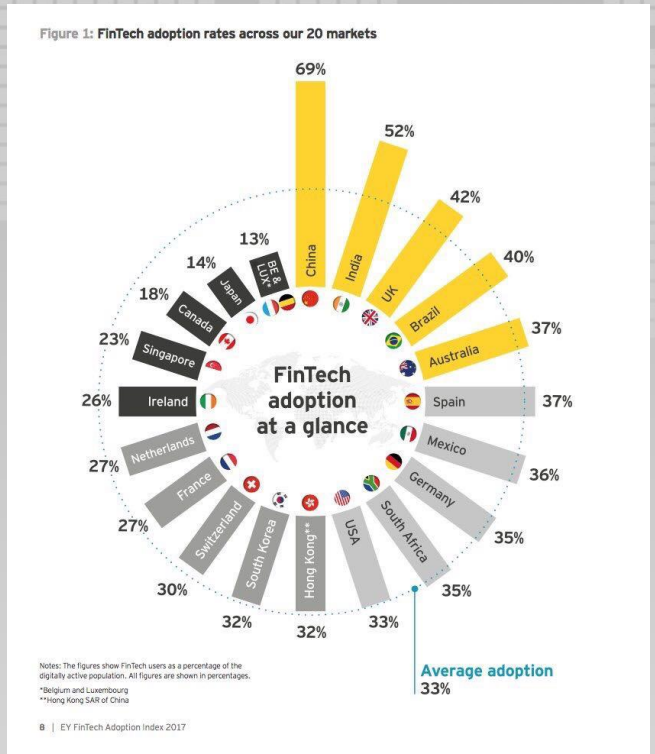
公安部破获电信网络诈骗案件情况

公安部查控中心处理涉案通讯工具

2016年1——8月专项行动期间，公安部在全国共破获电信网络诈骗案件7.1万起，同比上升2.4倍；查处违法犯罪人员3.8万名，同比上升2.5倍；收缴赃款赃物折合人民币16.5亿元，避免损失36.4亿元。2015年11月至2016年8月，公安部查控中心共冻结全国涉案账户80万余个，占全国公安机关冻结账户总量的90%以上，冻结资金11.81亿元，占全国公安机关冻结资金总量的80%以上；减少群众损失18.9亿元。关停涉案手机号码14.2万余个、网络固定电话3203余个，400号码近3万个，处理“伪基站”假链接1.54万个。

数据触目惊心！欺诈猖獗，反欺诈工作的全面开展和进一步加强迫在眉睫！

1.3 反欺诈的历史性机遇



Part
02

欺诈案例分析

2.1 欺诈案例

基于数据泄露的**精准诈骗黑色产业链**：黑客非法获取用户个人信息，拿到数据以后，就会有人接手，这里面还有大量二道贩子的存在，在中间赚差价。**这个链条上的人分工特别明确**，而且都是**“专业”**级别的团队操作。有些人会专门去联系相关的培训机构或诈骗团伙，从而把手上的**数据卖到下游**。而下游这些团队，有专人负责**诈骗的话术**编写培训、线上通过第三方支付平台**洗钱**、线下ATM机**提款**等，分工非常明确。”

2.2 案例分析

专业的欺诈话术培训和“技术支持”

浏览一些网站，查找问题。而获取到山东考生信息就是杜天禹在测试网站漏洞时找到的。利用网站漏洞获取到权限后，杜天禹在数据库中找到了山东高考考生的信息并将信息下载。

杜天禹

5角 / 条左右，卖了十万余条高考考生信息，获利共计一万四千余元。

电话组

取钱组

冒充教育局

一组

二组

冒充财政局

2015 年 11 月至 2016 年 8 月，骗取金额共计人民币 56 万余元，通话次数共计 2.3 万余次。犯罪团伙中的几个人分工协作、环环相扣，形成完整的诈骗链条；他们扮演不同的角色，引人入局，骗取钱财；得手之后，又利用专业团队洗钱，隐蔽性极强。明显的产业化，并且趋于智能化。

1

2

3

得手后在异地福建泉州ATM取款逃逸。

2.3 欺诈的产业化与智能化

海量数据泄漏：

在2016年，共有超过十亿数据被窃取，其中的95%属于科技、金融、政府、和零售等行业。海量的用户敏感数据泄露为欺诈行为撕开了一道口子。

欺诈行为凸显非接触性和隐蔽性

传统的欺诈行为，是行为人通过与一定自然人之间的沟通，即“人人对话”而实现的。相比之下，新型欺诈行为更多是行为人通过“人机对话”的方式实施犯罪，行为呈现非接触性和隐蔽性。

欺诈方式更具专业化、智能化，诈骗手段翻新速度快：

欺诈的手段不断升级，软、硬件攻击，社会工程等方式并举，犯罪分子欺诈手段和能力不断提升，翻新的频率极快。

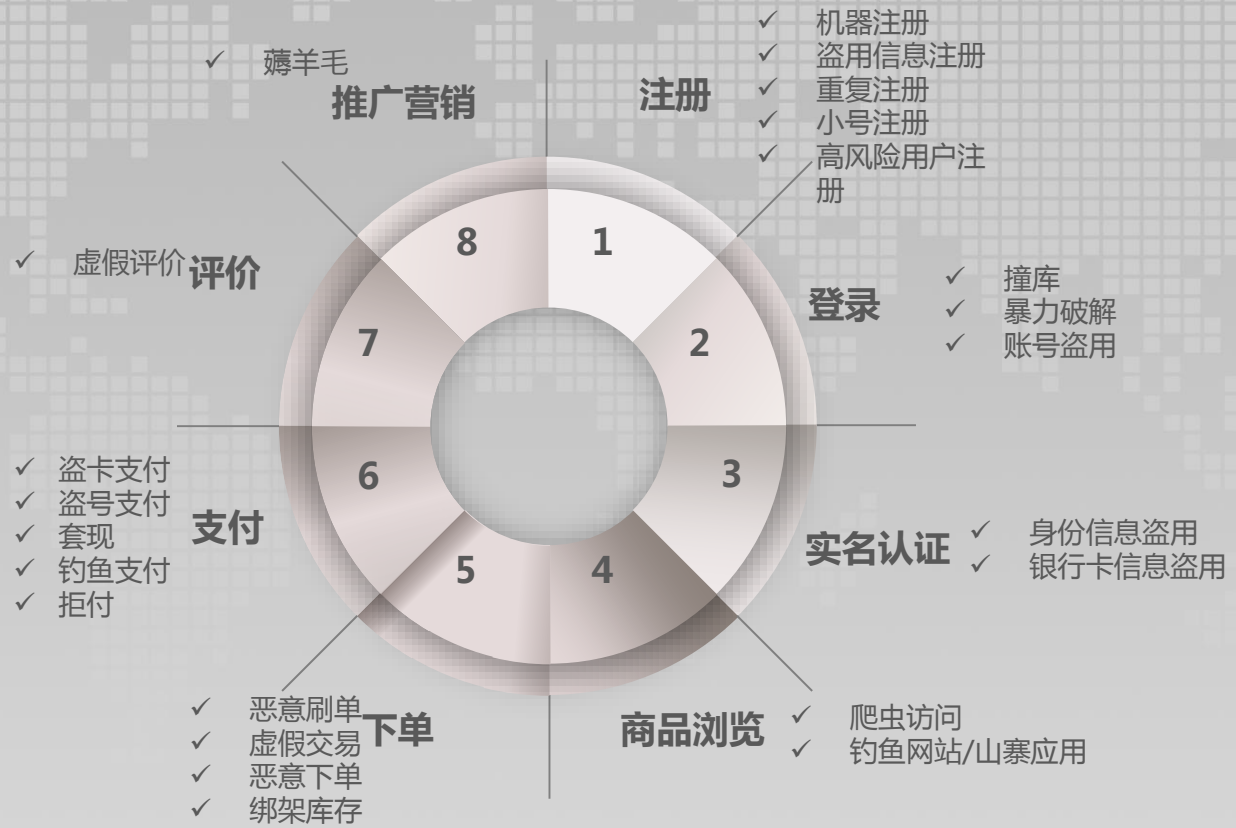
金融欺诈集团化：

随着欺诈工具不断升级，犯罪分子作案分工明确，呈现跨地域、多渠道的集团化特征。逐步形成了包括上、中、下游结构完整黑色产业链。增加了风控的难度。

Part
03

人工智能反欺诈

3.1 反欺诈场景-识别欺诈



3.2 “天网”反欺诈平台-防范欺诈

全流程反欺诈，事前预警、事中管控、事后分析。

事前预警

事中管控

事后分析

监控

风险中心
设备中心

事件报表
响应报表

报表

事件

事件详情
风控建议

业务规则
模型策略

策略

分析

关联分析
位置分析

业务管理
服务管理

管理

3.3 复杂网络分析（“漫网技术”）-分析欺诈

1、工具：neo4j（支持分布式部署）；

2、构建关系图谱采用的数据以及数量：

（1）身份证号：2.6千万+

（2）手机号码：7.3千万+

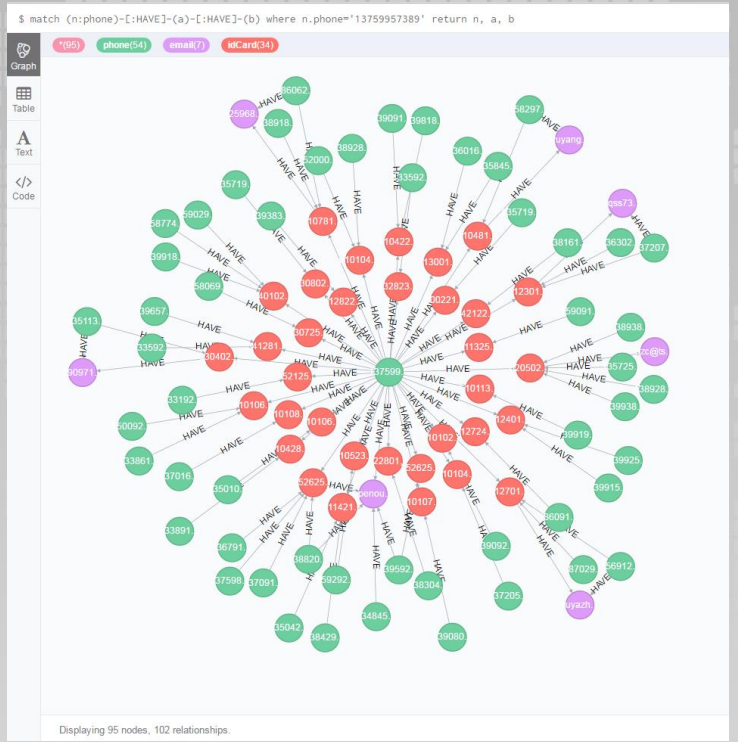
（3）邮箱：1亿+

3、速度（搭建在一台机器）：

（1）一级搜索平均耗时：10ms/条；

（2）二级搜索平均耗时：200ms/条；

4、应用场景：借助关系图谱进行数据挖掘。



Part
04

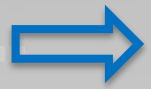
未来展望

4.1 加强个人信息保护

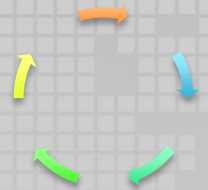
- 5月10号上午，最高人民法院、最高人民检察院联合召开新闻发布会，发布《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》（下称《解释》）对侵犯公民个人信息犯罪的定罪量刑标准和有关法律适用问题作了全面、系统的规定
- （一）出售或者提供行踪轨迹信息，被他人用于犯罪的；
- （二）知道或者应当知道他人利用公民个人信息实施犯罪，向其出售或者提供的；
- （三）非法获取、出售或者提供行踪轨迹信息、通信内容、征信信息、财产信息五十条以上的；
- （四）非法获取、出售或者提供住宿信息、通信记录、健康生理信息、交易信息等其他可能影响人身、财产安全的公民个人信息五百条以上的；
- （五）非法获取、出售或者提供第三项、第四项规定以外的公民个人信息五千条以上的；
- （六）数量未达到第三项至第五项规定标准，但是按相应比例合计达到有关数量标准的；
- （七）违法所得五千元以上的；

4.2 欺诈态势感知

4.3 未来安全：云端大脑 + 机器人



盾盾
（安全机器人）



云端安全大脑

网络攻击和金融欺诈已经集团化、产业化、智能化。精准风控帮助金融科技打赢这场 **AI VS AI** 的新战争！