基于大数据的涉网犯罪行为分析

360猎网平台——冯广彬

ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）

目录

以数据观现状

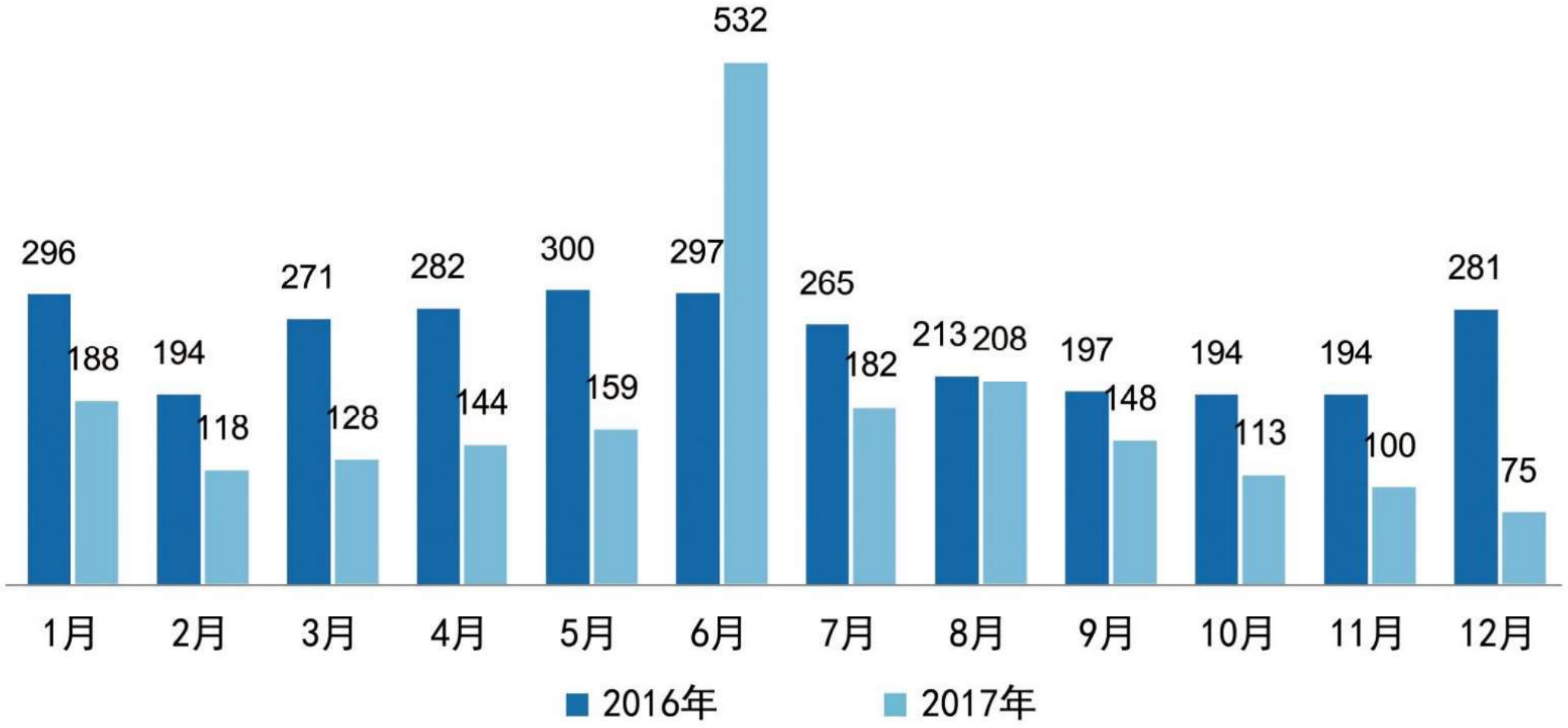
(数据来源: 中国互联网信息中心&国家互联网应急中心)

近十年互联网发展趋势

来源: CNNIC 中国互联网络发展状况统计调查

2017.12

近两年病毒木马感染终端量



来源:CNCERT互联网安全威胁报告

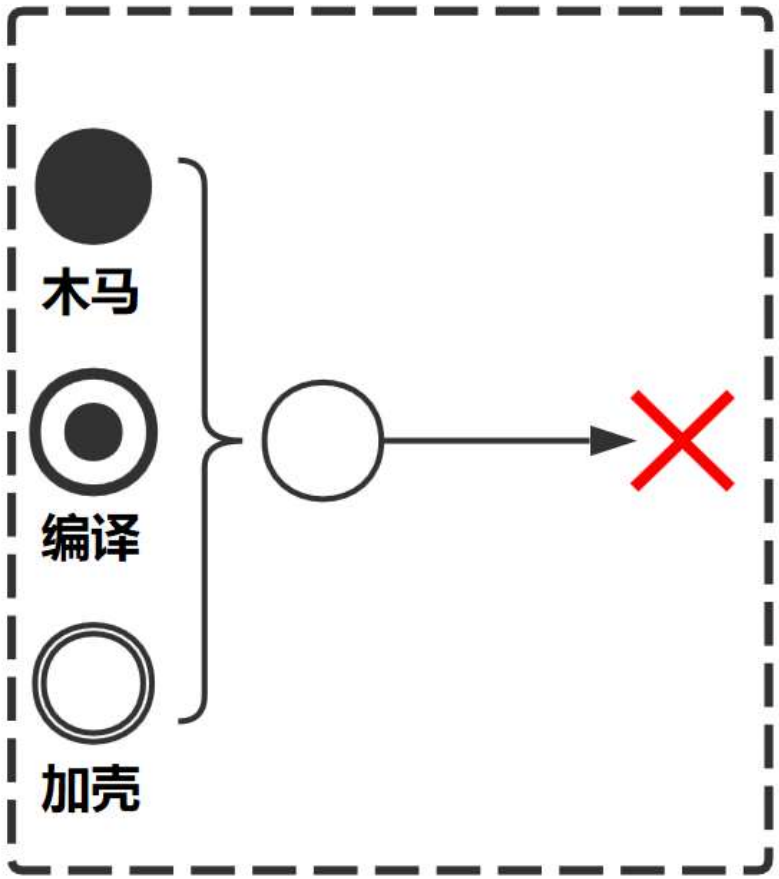
2017.12

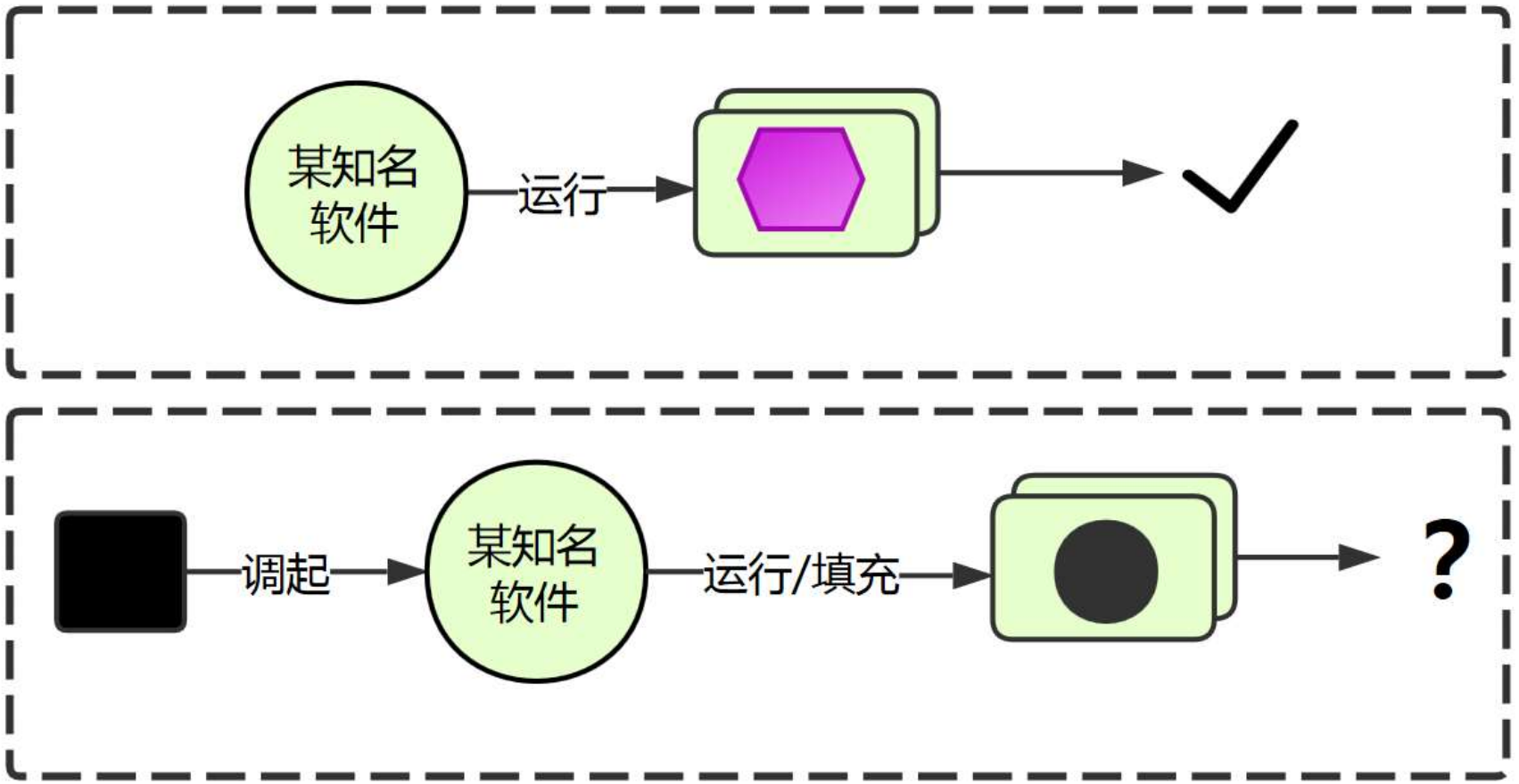
归纳的几点原因


01
网民
自身安全意识
02
环境
互联网厂商
03
监管
打击力度法律
04
技术
对抗提升门槛
05
制作
性价比收益低
06
其他
云时代移动端

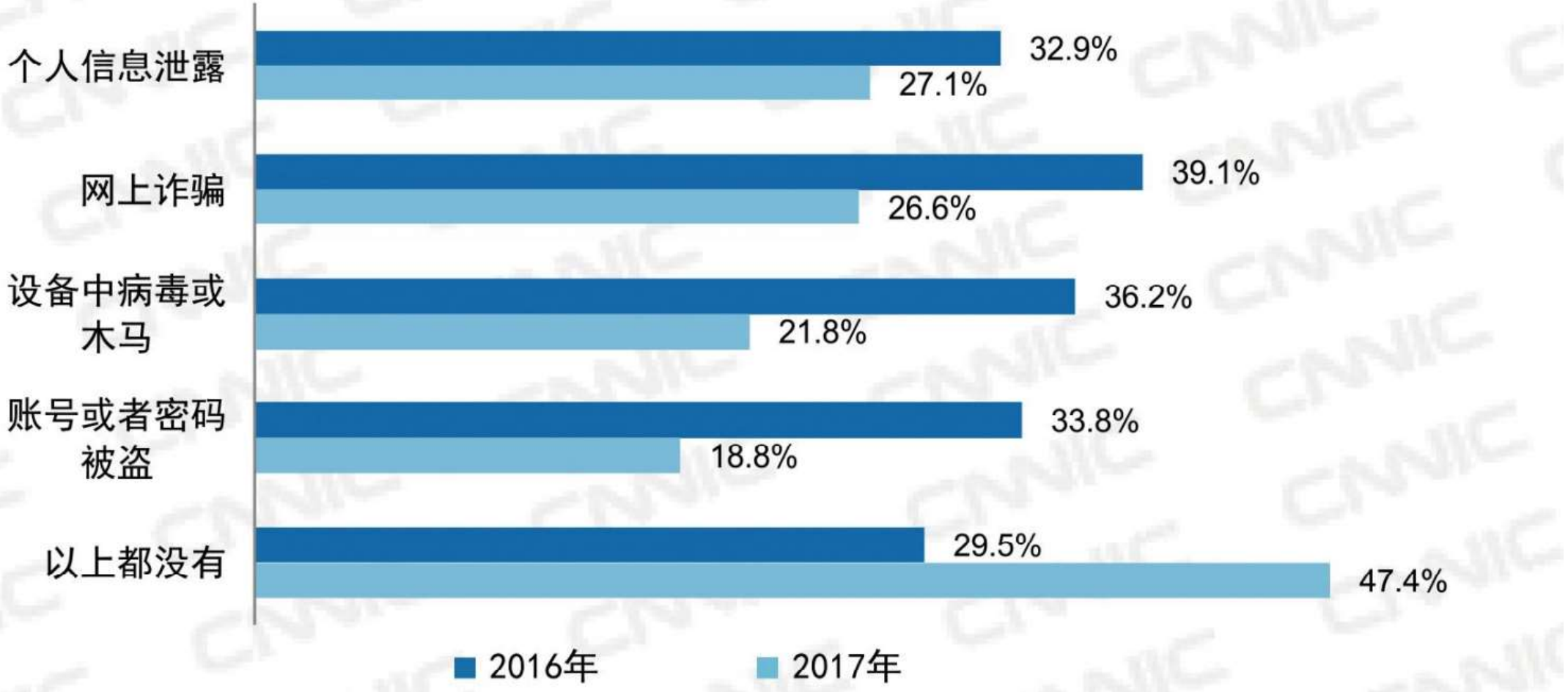
木马免杀哪些事

裸奔 → 文件查杀 → 编译 → 特征查杀 → 变形 → 沙箱查杀 → 驱动 → 主防查杀 → 白利用





当前网络威胁



来源: CNNIC 中国互联网络发展状况统计调查

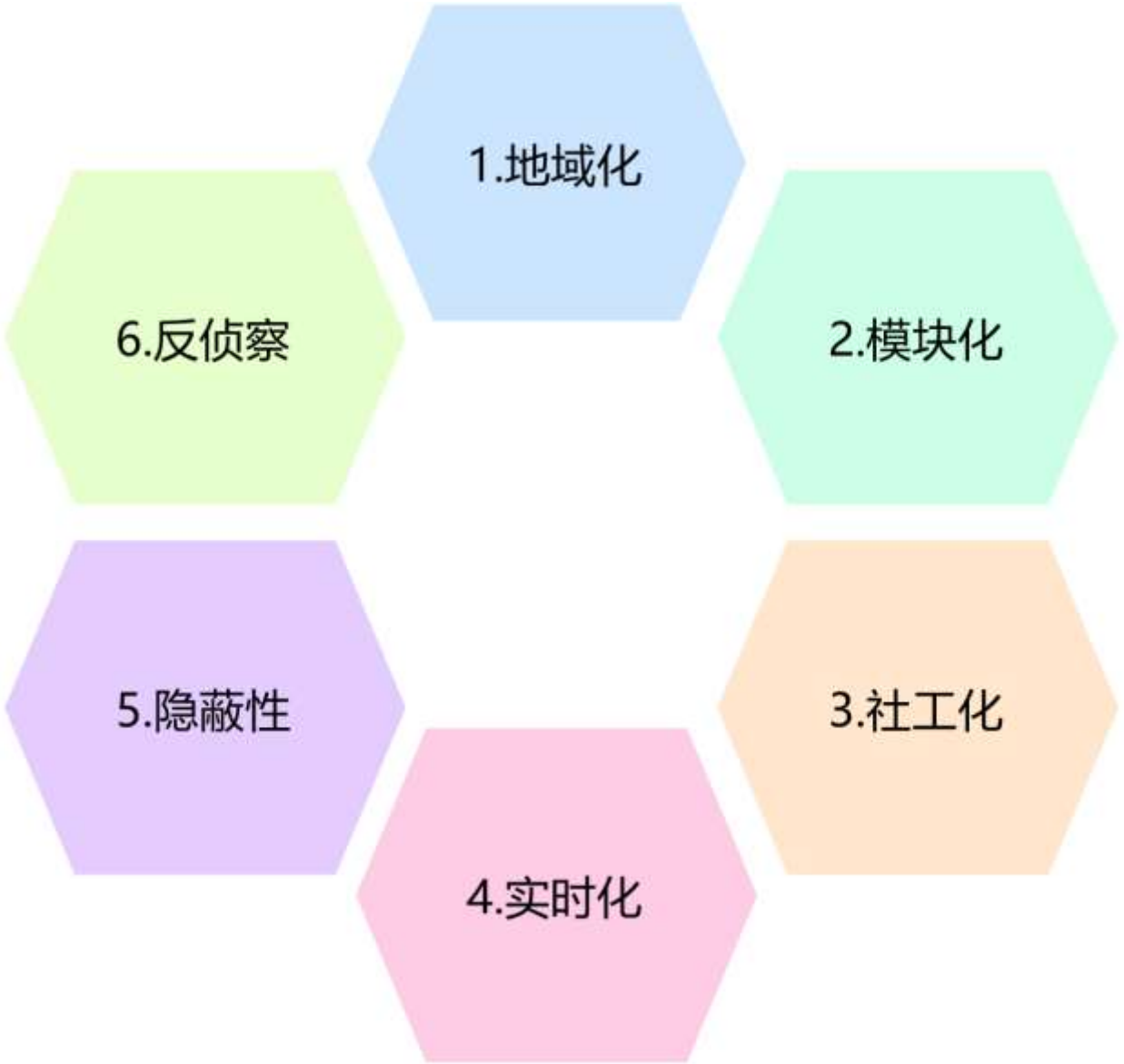
2017.12

涉网犯罪及发展趋势

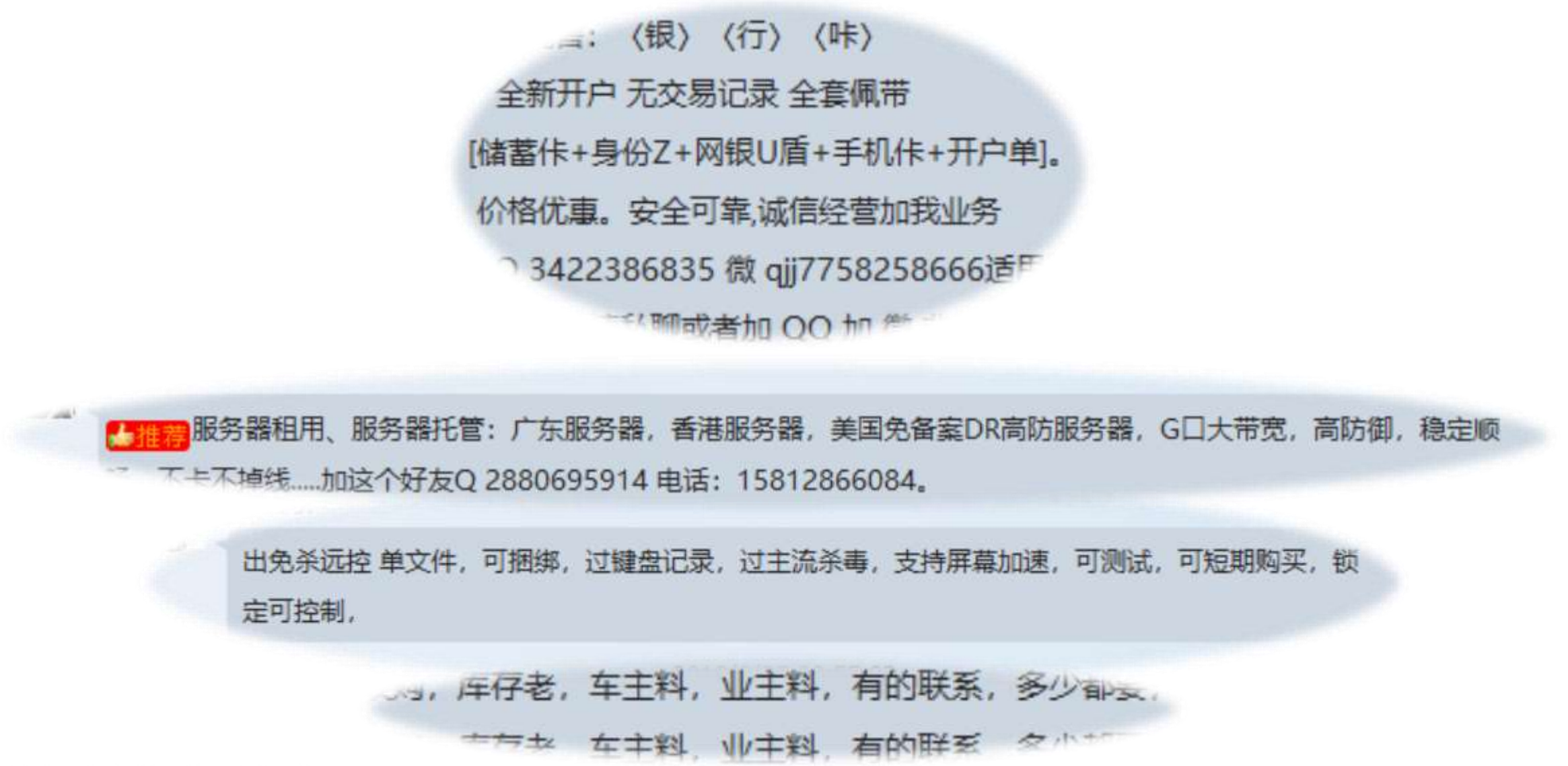
涉网犯罪概述

运用计算机技术，借助于网络对其系统或信息进行攻击、破坏，**或利用网络进行其他犯罪的总称。**

涉网犯罪趋势



模块化实例


〈银〉〈行〉〈咔〉
全新开户 无交易记录 全套佩带
[储蓄伴+身份Z+网银U盾+手机伴+开户单]。
价格优惠。安全可靠,诚信经营加我业务
3422386835 微 qjj7758258666适
聊或者加 QQ 加
推荐服务器租用、服务器托管：广东服务器，香港服务器，美国免备案DR高防服务器，G口大带宽，高防御，稳定顺
不卡不掉线.....加这个好友Q 2880695914 电话：15812866084。
出免杀远控 单文件，可捆绑，过键盘记录，过主流杀毒，支持屏幕加速，可测试，可短期购买，锁
定可控制，
，库存老，车主料，业主料，有的联系，多少都
车主料，业主料，有的联系

社工化案例

过程描述:

放长线

刚开始有个女的加我，和我聊天想做我女朋友，聊了几天后就跟我说叫我帮她打重庆时时彩，我觉得反正也没什么损失，就帮她打了**(红颜交友)**

投鱼饵

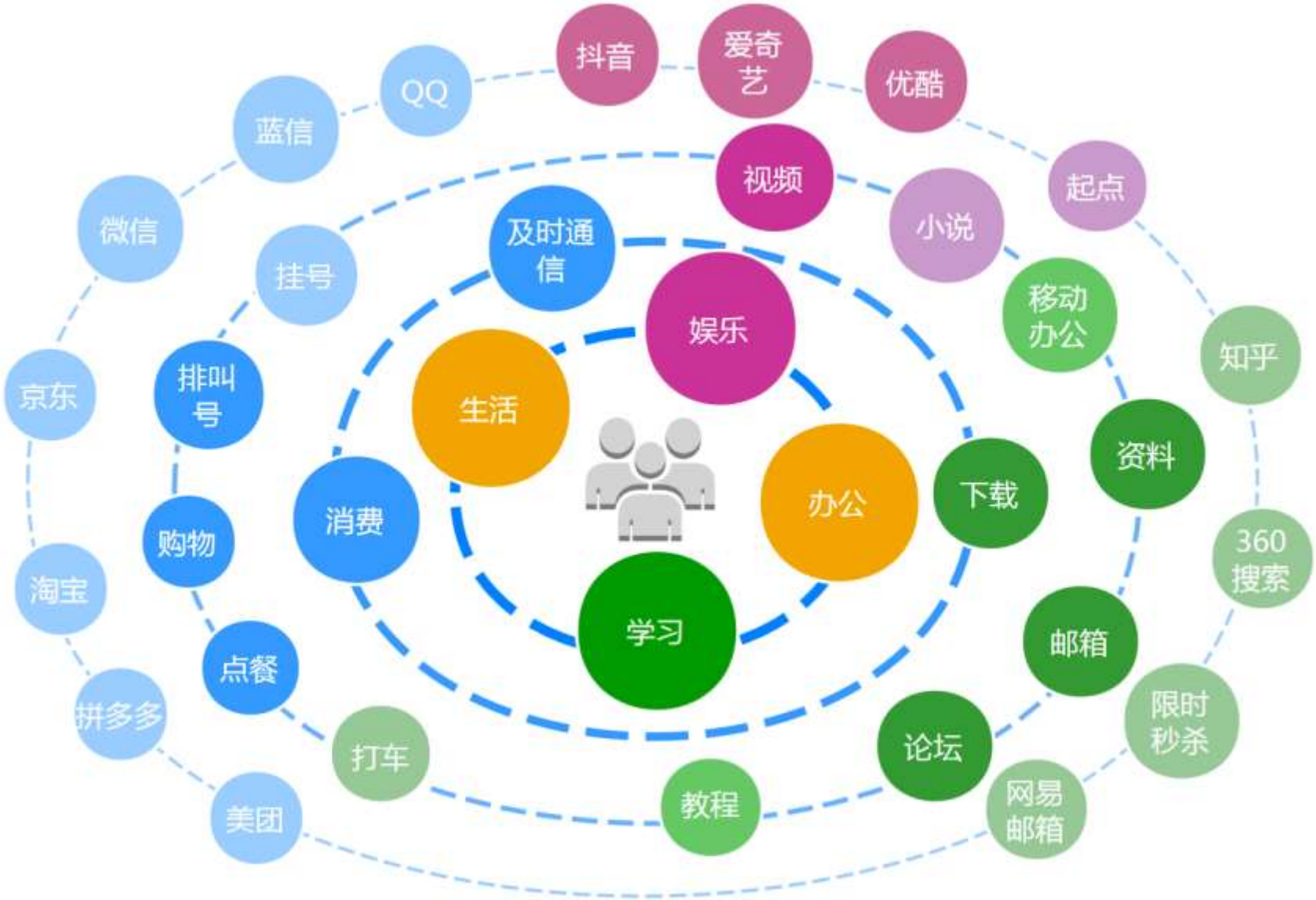
她说有表哥在那个平台做客服，能把大小和单双赔率1.95改成2.05倍，帮她打的过程觉得赚钱挺不错的，我就自己注册一个账号跟她一起买，也赚了点钱，两次提现都能到账**(引诱让利)**

钓大鱼

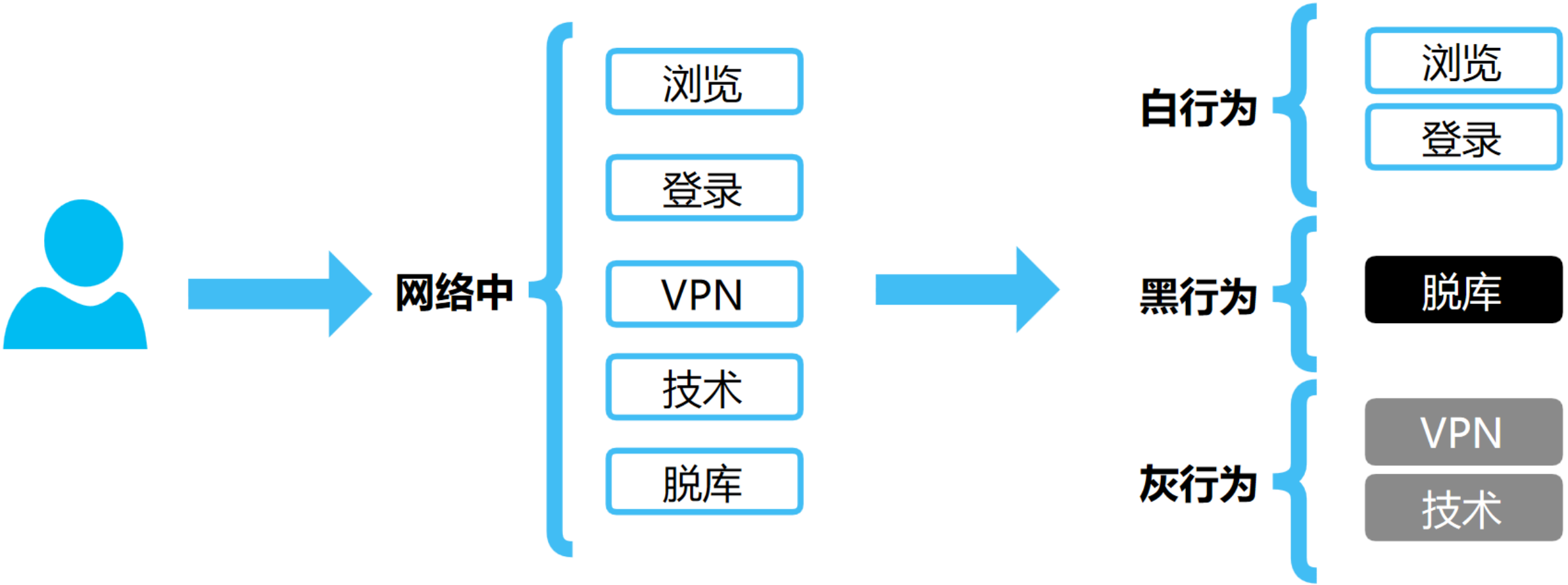
第三次迟迟没到账，心急就问她为什么提现不到账，她说表哥忙要等公司人不注意时再帮我提现，就这样一直拖着，提不出来，损失10800元

涉网行为概述

什么是涉网行为

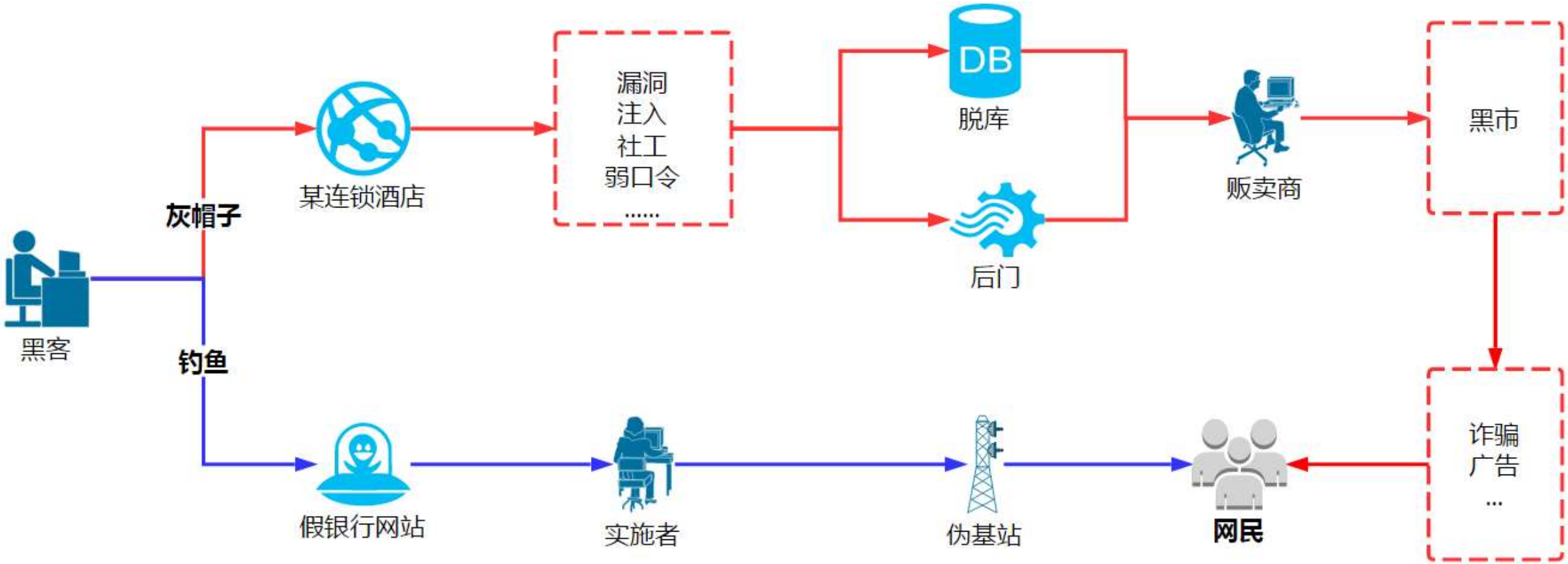

抖音
爱奇艺
优酷
QQ
蓝信
视频
起点
微信
及时通信
小说
挂号
移动办公
娱乐
知乎
京东
排叫号
生活
资料
消费
办公
下载
购物
360搜索
淘宝
学习
邮箱
点餐
拼多多
限时秒杀
论坛
打车
教程
网易邮箱
美团

涉网行为分类

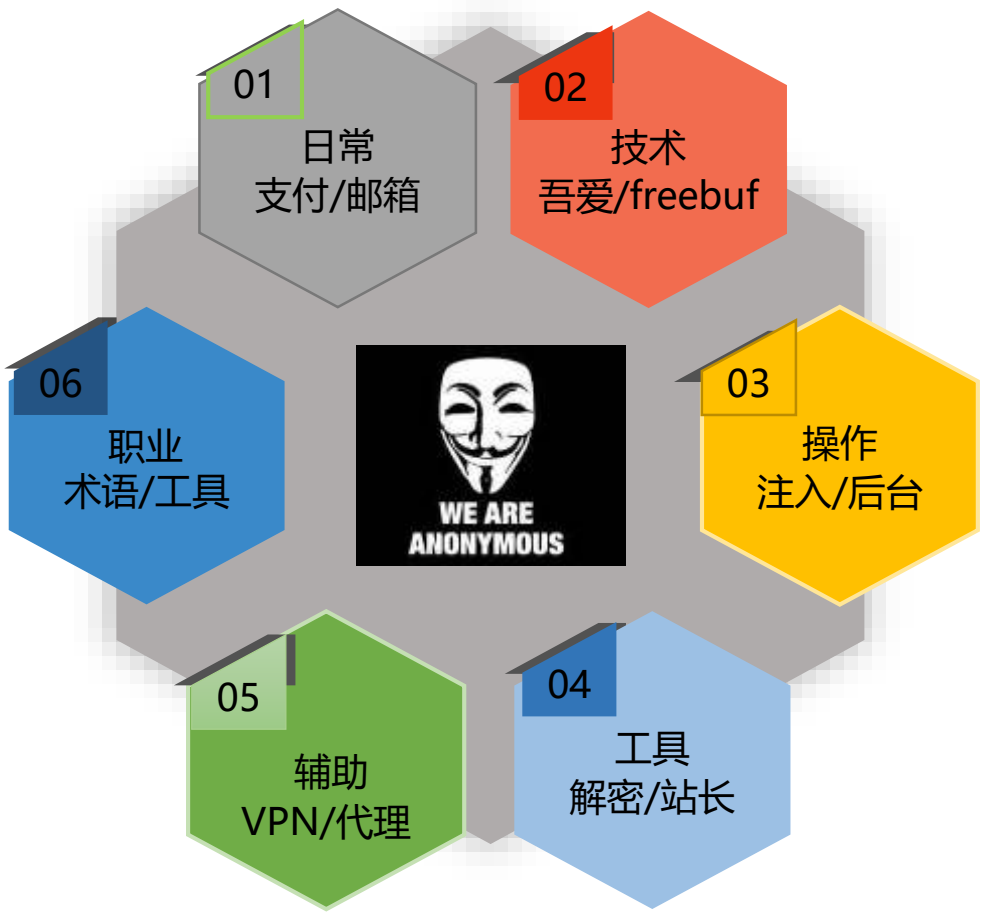


涉网犯罪行为特征分析

黑客产业链



黑客涉网行为概览


01
日常
支付/邮箱
02
技术
吾爱/freebuf
03
操作
注入/后台
04
工具
解密/站长
05
辅助
VPN/代理
06
职业
术语/工具
WE ARE
ANONYMOUS

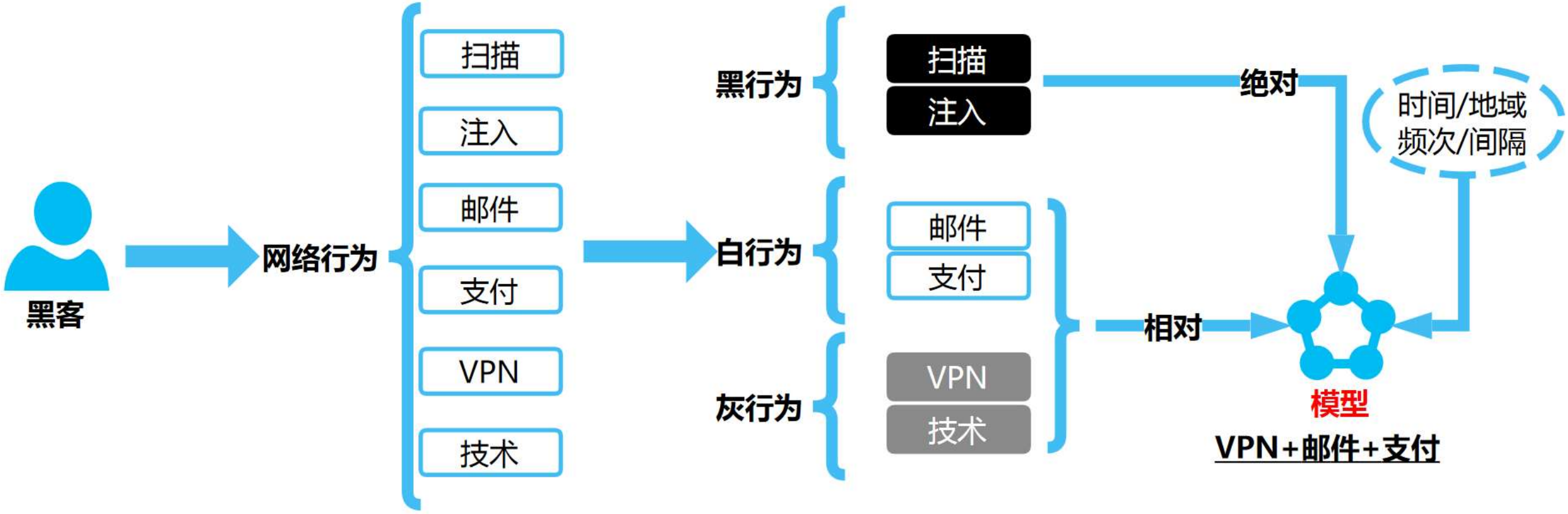
黑客涉网行为分析

昌河铃木北斗星 汽车之家 广汽传祺 ssdp协议 DDOS md5加密 md5加密 xss hunter 注册
一汽马自达4s店 ssdp反射DDOS 针对域名 ssdp协议 宇通客车 xss hunter 注册
centos7如何改变ssh端口号 汽车之家 xss免费平台 xsshunter 墙 sqlmap oracle注入 穿山甲SQL注入
linux下web扫描工具 如何改变ssh端口号 一汽马自达4s店 一汽马自达4s店 一汽马自达4s店
ssdp协议 DDOS ssdp协议干什么用 linux 安装 git xss免费平台 威努特 宇通客车
海马dealer Management system xss平台 重庆快键网约车系统 买DDOS攻击 excel合并单元格保留所有内容
先知白帽 海南马自达 先知白帽 重庆快键网约车系统 sqlmap 重庆快键网约车系统 xss hunter 注册
蓝盾 穿山甲SQL注入 linux 安装 git xsshunter linux下的web漏洞扫描 廊坊卫生职业学院 ssdp协议
一汽马自达4s店 一汽马自达4s店 海马dealer Management system 宇通易学堂 xss平台 medusa
莲花汽车 KOL矩阵 双龙汽车 xss平台 沧州医学高等专科学校 流量攻击多少钱一次 xss hunter 注册
穿山甲 xsspt.com 海马dealer excel合并单元格保留所有内容 xss平台 xss免费平台
sqlmap oracle注入 宇通客车 流量攻击多少钱一次 linux下web扫描工具 海马dealer Management system
KOL矩阵 沧州医学高等专科学校 海南马自达 xsshunter 墙 50107端口 汽车之家 东方大学城学校

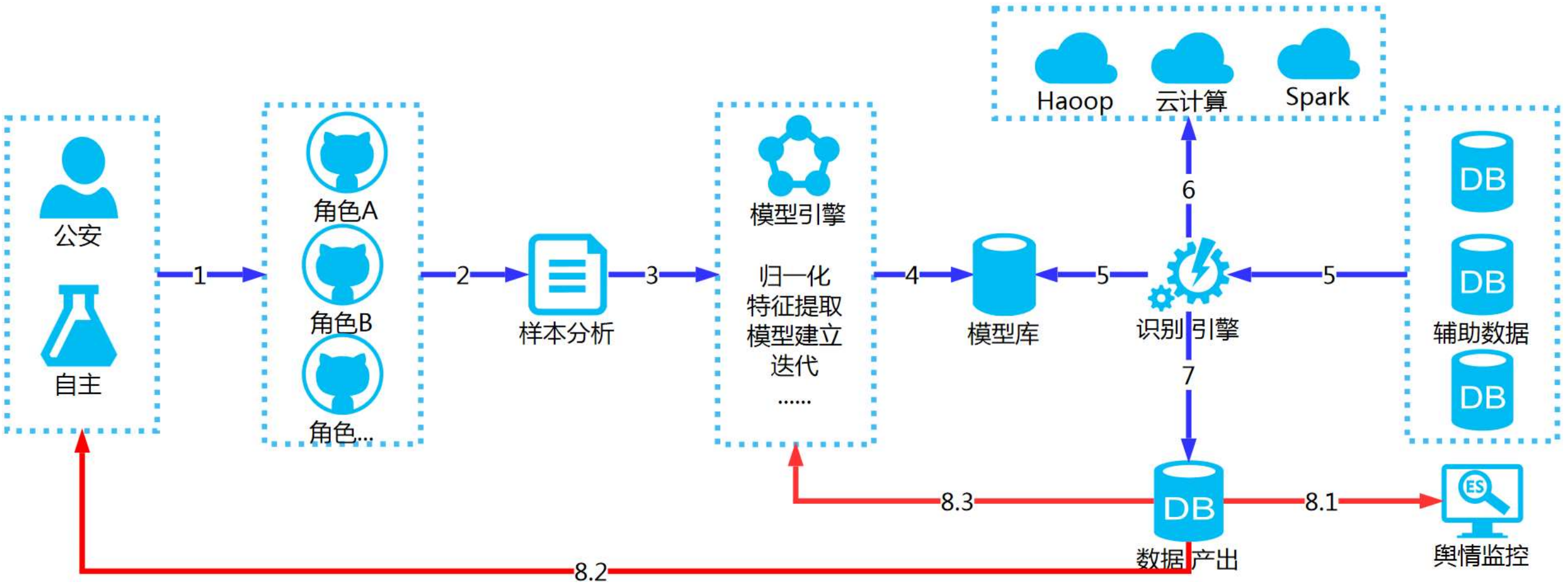
黑客涉网行为分析

HOST	次数	标题
www.baidu.com	257	百度一下，你就知道
www.52pojie.cn	135	吾爱破解 - LCG - LSG|安卓破解|病毒分析|破解软件|www.n
pan.baidu.com	134	百度网盘，让美好永远陪伴
bbs.ichunqiu.com	118	i春秋论坛|白帽黑客论坛|网络渗透技术|网站安全|移动安全
www.freebuf.com	80	FreeBuf互联网安全新媒体平台 | 关注黑客与极客
home.console.aliyun.com	64	登录
tool.chinaz.com	57	站长工具 - 站长之家
account.aliyun.com	57	登录

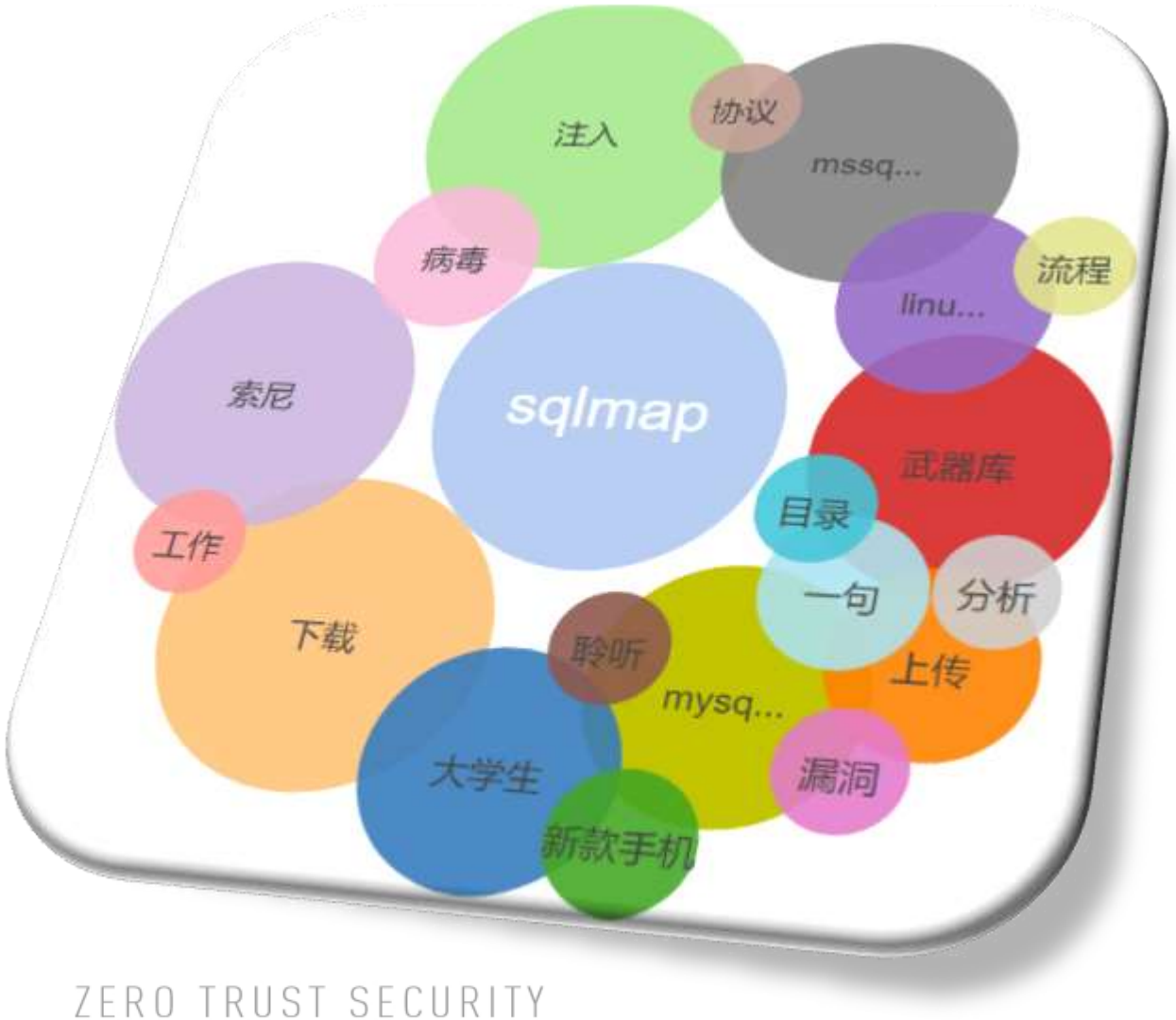
黑客行为分类及模型生成



涉网犯罪行为识别引擎流程图

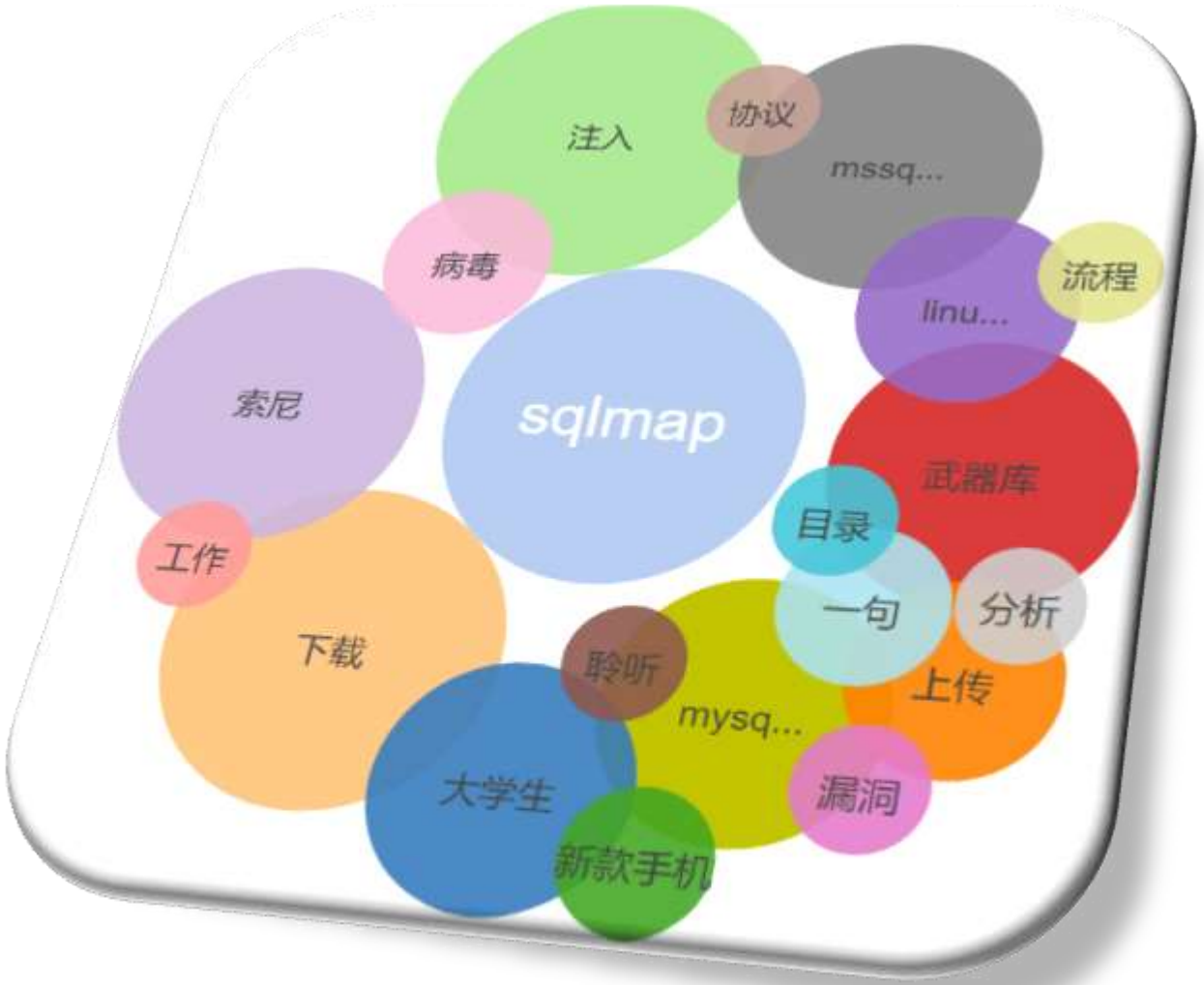


样本数据&示例模型




```
{
……
 “xxx_” : : [ “一句话”，“漏洞”，“注入", "sqlmap"],
"yyy": 1,
"Regional": ["全部地域"],
"Url_xxx": [{
            "Match": 1,
            "Value": "www.freebuf.com",
            "xxx": 10
}],
"xxx_Count": 1,
"Filter": [{
            "xxx": 1,
            "Hit": 1000,
            "Regional": 10
}]
……
}
```

样本数据&示例模型


注入
协议
mssq...
病毒
流程
linu...
索尼
sqlmap
武器库
目录
工作
一句
分析
下载
聆听
上传
mysq...
大学生
漏洞
新款手机


inur...
查看
mysq...
工具
注入
网站
linu...
入侵
翻译
端口
菜刀
站长
绕过
银行
文件
pape...
后台
漏洞
上传
开启

MORE

ZERO TRUST SECURITY

结束语

猎网平台是一个面向全体网民开放的网络诈骗信息举报平台，平台致力于建设一个警、企、民联动的反网络诈骗信息系统。


ISC
2018
ISC互联网安全大会
360互联网安全中心
谢 谢!
ISC 互联网安全大会 中国 · 北京
Internet Security Conference 2018 Beijing · China
（原“中国互联网安全大会”）