# 透视黑产——
# 谁动了你们公司的数据

喻峰

腾讯安全云鼎实验室
2019.05

Geekbang 极客邦科技 | TGO 鲲鹏會

# TGO鲲鹏会

# 汇聚全球科技领导者的高端社群

全球12大城市

850+高端科技领导者

**使命 Mission**

为社会输送更多优秀的科技领导者

**愿景 Vision**

构建全球领先的有技术背景优秀人才的学习成长平台

扫描二维码，了解更多内容

极客时间 | 企业服务

这是一封正经“福利”贴

# 想做团队的领跑者 需要迈过这些“槛”

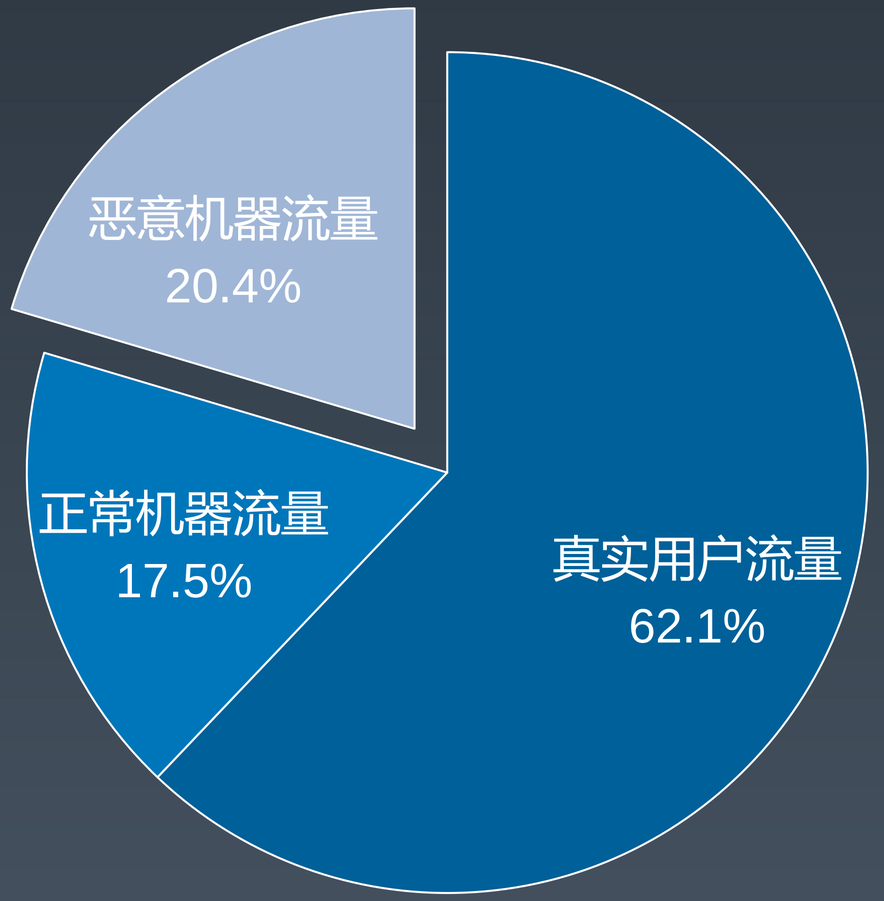
| | | |
|---|---|---|
| 成长型企业，易忽视人才体系化培养<br>企业转型加快，团队能力又跟不上 | VS | 从基础到进阶，超100+一线实战<br>技术专家带你系统化学习成长 |
| 团队成员技能水平不一，<br>难以一“敌”百人需求 | VS | 解决从小白到资深技术人所遇到<br>80%的问题 |
| 寻求外部培训，奈何价更高且<br>集中式学习 | VS | 多样、灵活的学习方式，包括<br>音频、图文 和视频 |
| 学习效果难以统计，产生不良循环 | VS | 获取员工学习报告，查看学习<br>进度，形成闭环 |

课程顾问「橘子」

回复「QCon」
**免费获取**
学习解决方案

**# 极客时间企业账号 #** 解决技术人成长路上的学习问题

# 2018年互联网「人类 vs 机器」流量情况



# 自我介绍

- 喻峰，腾讯安全 云鼎实验室，负责威胁情报和云安全研究
- 「全栈安全」工程师

# 目录

# 云安全

@2008

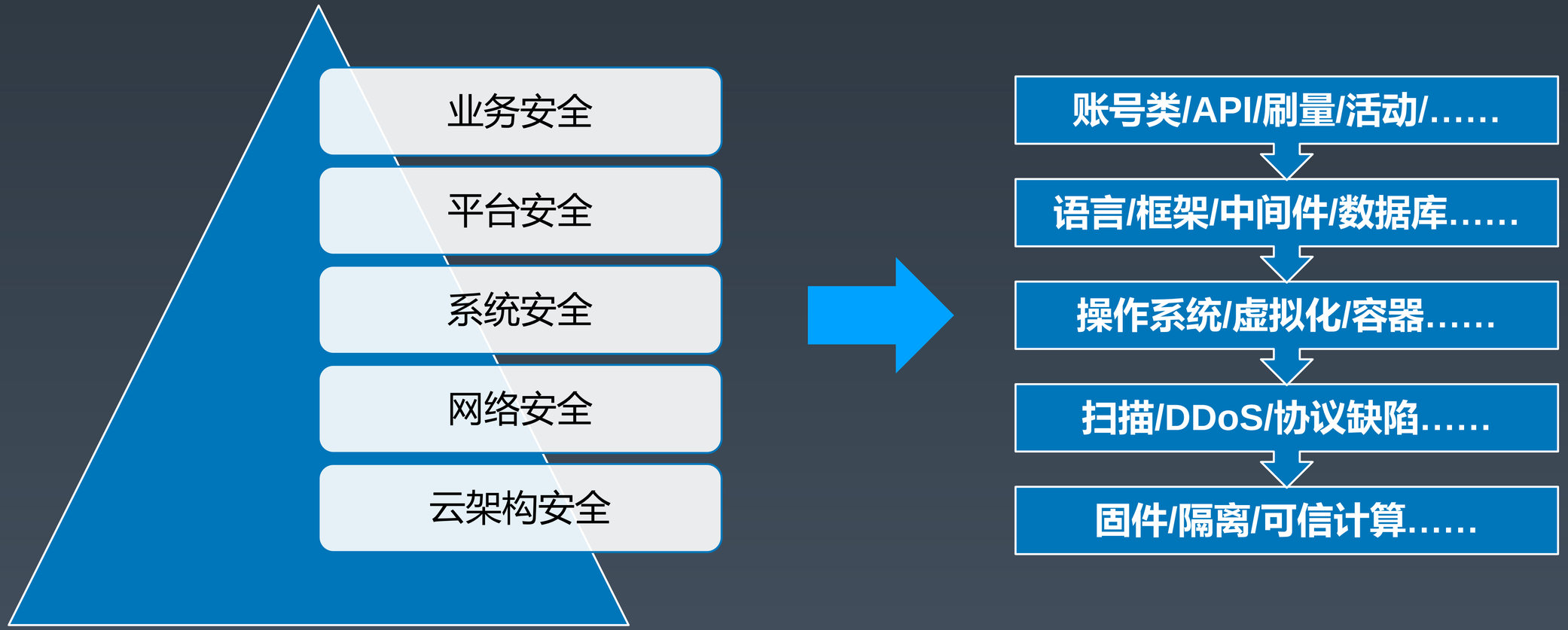
云安全 == 云查毒

@9102

云安全 == 云计算安全

# 上云

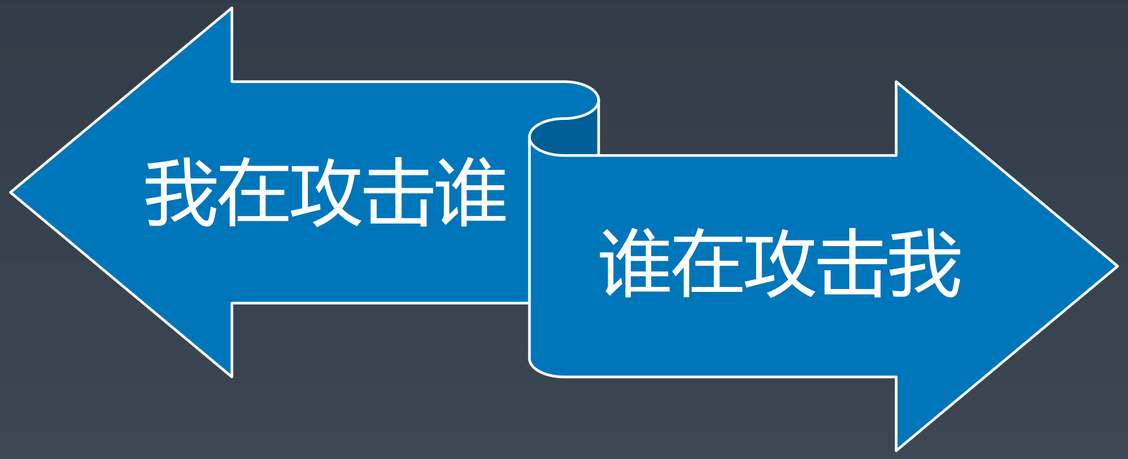
# 云上安全


业务安全
平台安全
系统安全
网络安全
云架构安全
账号类/API/刷量/活动/……
语言/框架/中间件/数据库……
操作系统/虚拟化/容器……
扫描/DDoS/协议缺陷……
固件/隔离/可信计算……

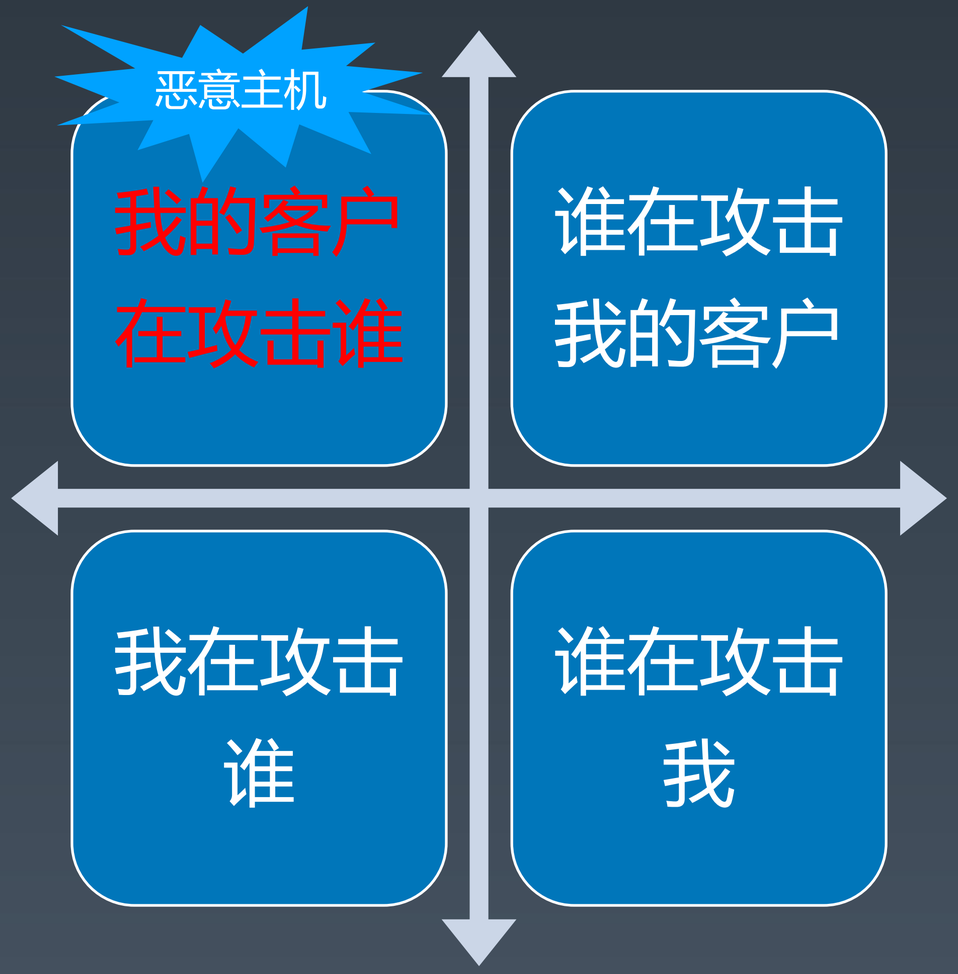
# 安全研究三板斧

# 目录

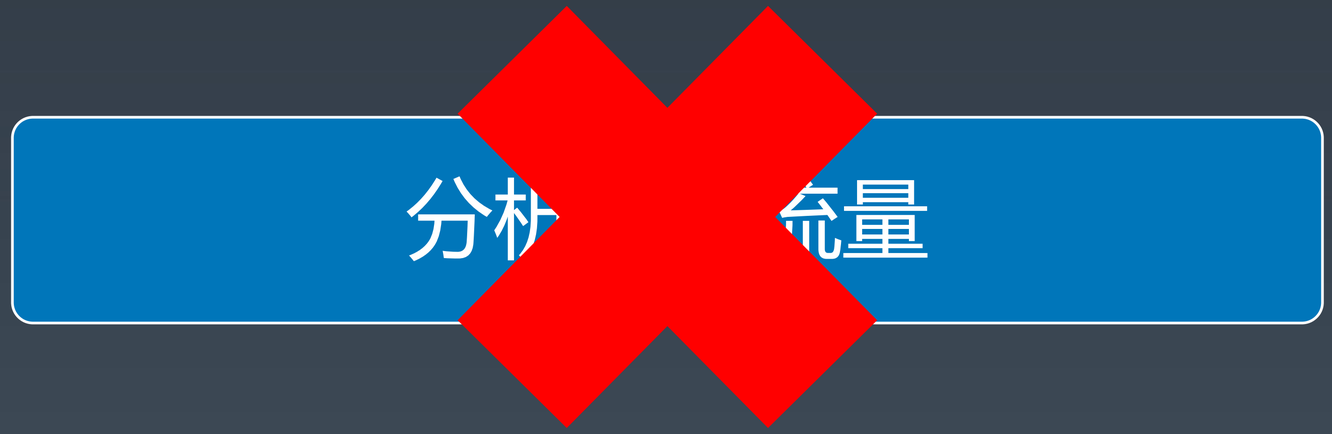
# 两方场景攻击面



# 三方场景攻击面



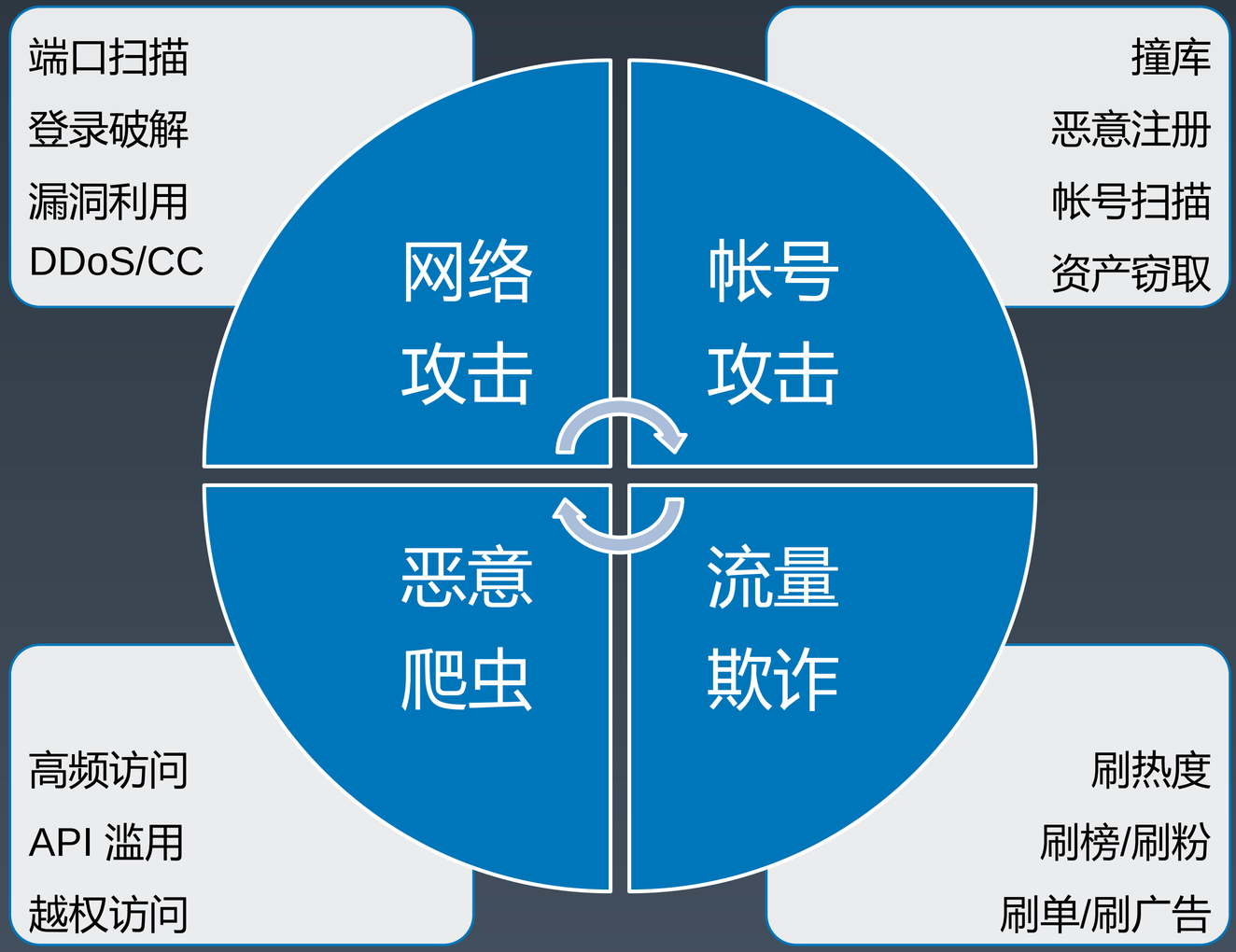
# 怎么研究



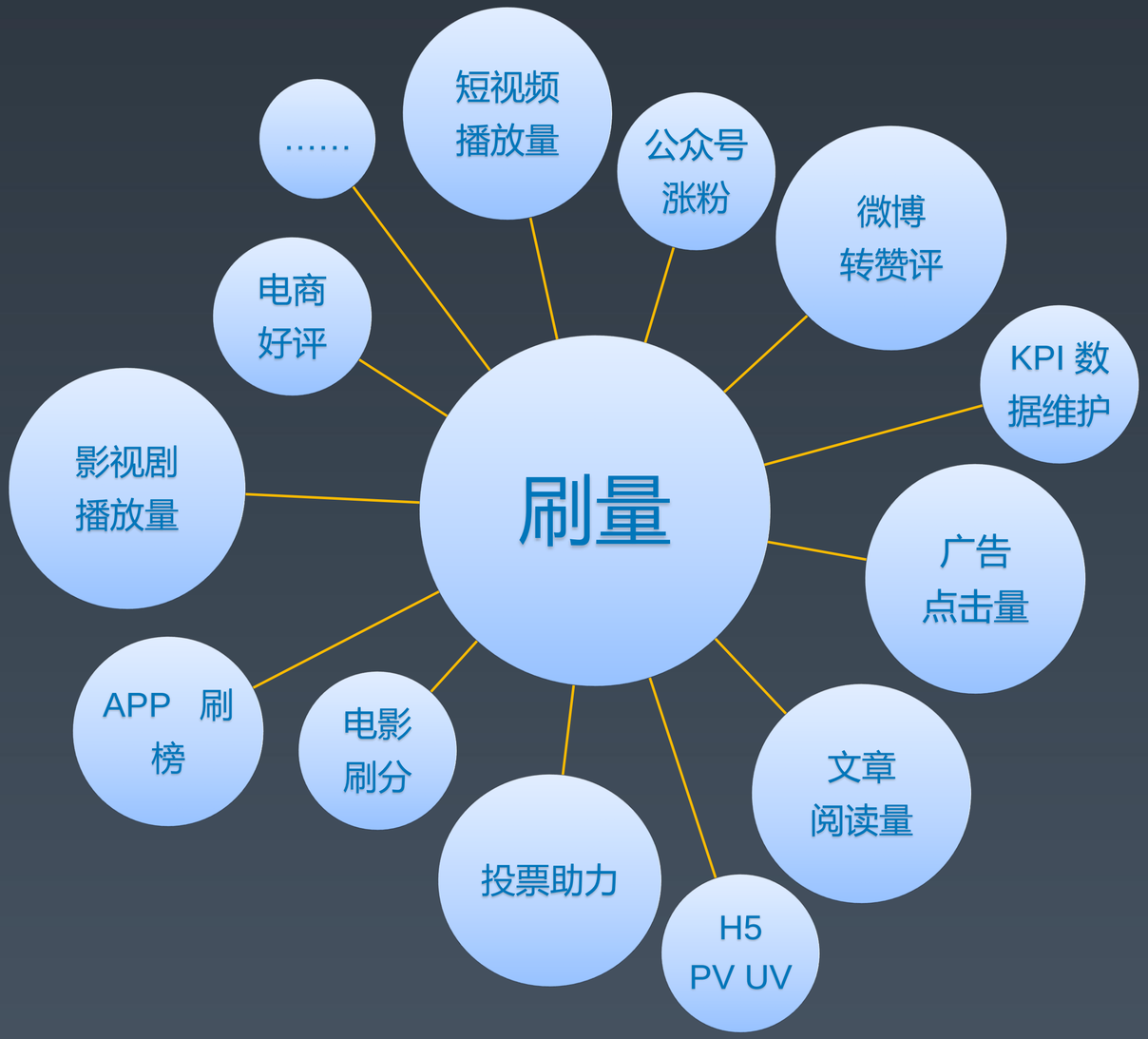
# 怎么研究

**捕获** 恶意流量

# 恶意流量 是什么


端口扫描
登录破解
漏洞利用
DDoS/CC
网络
攻击
撞库
恶意注册
帐号扫描
资产窃取
帐号
攻击
恶意
爬虫
流量
欺诈
高频访问
API 滥用
越权访问
刷热度
刷榜/刷粉
刷单/刷广告

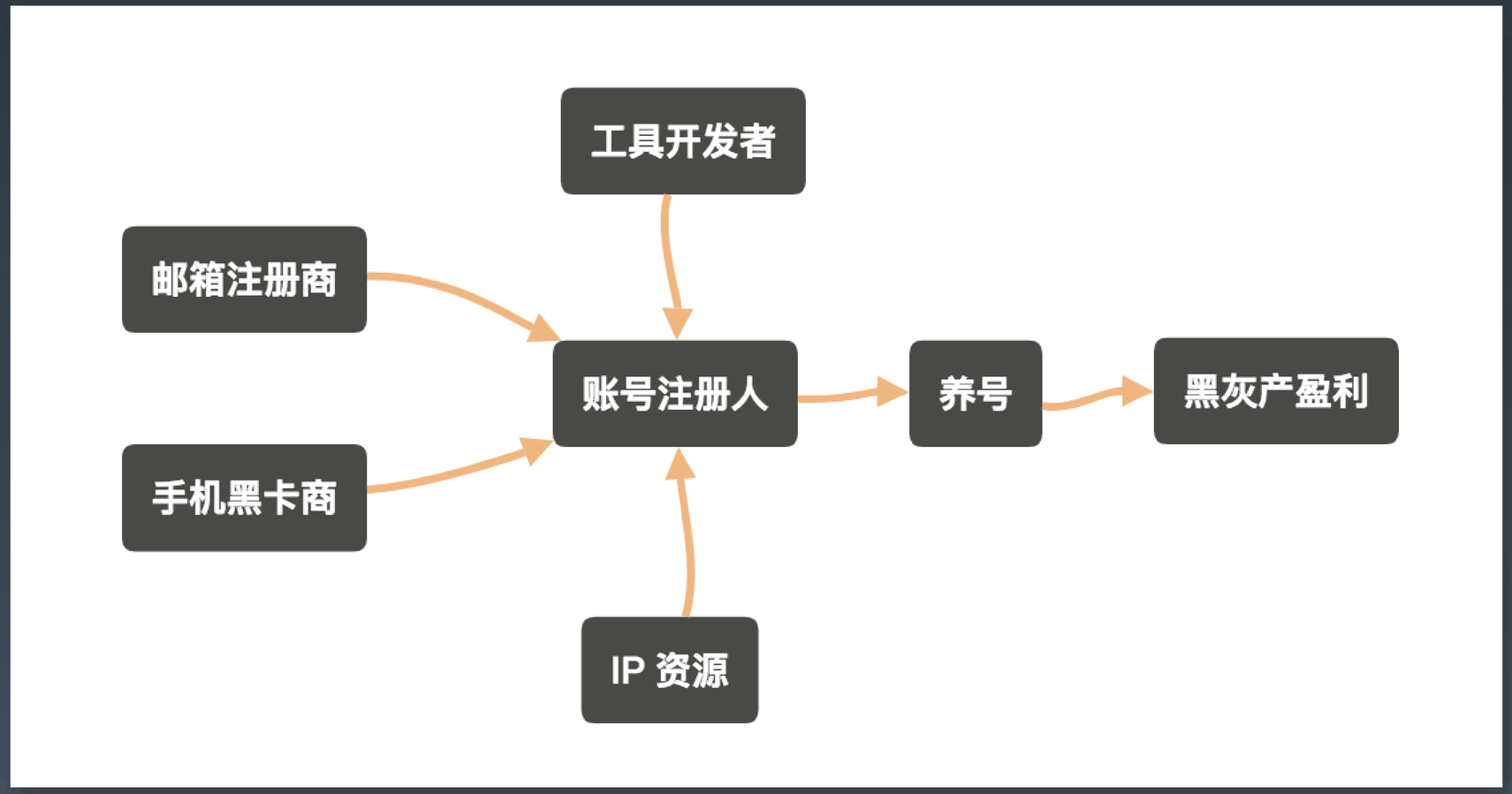
# 流量欺诈产业


刷量
短视频
播放量
公众号
涨粉
微博
转赞评
KPI 数
据维护
广告
点击量
文章
阅读量
H5
PV UV
投票助力
电影
刷分
APP 刷
榜
影视剧
播放量
电商
好评
……

# 《流浪地球》巅峰期吴京 vs 流量鲜肉的日常

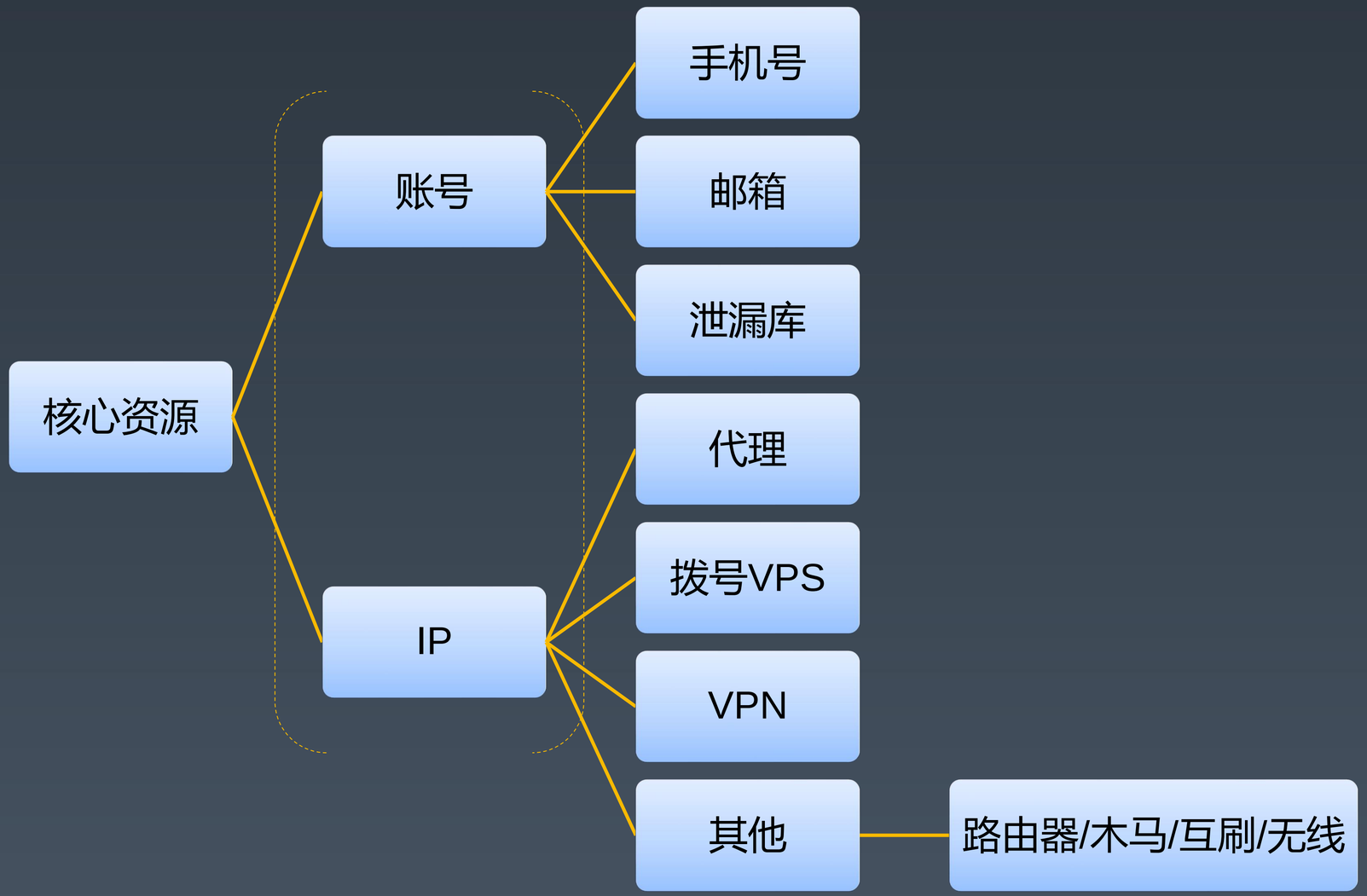

VS

# 恶意注册养号产业链



# 论 IP 资源的重要性

# 黑产核心资源

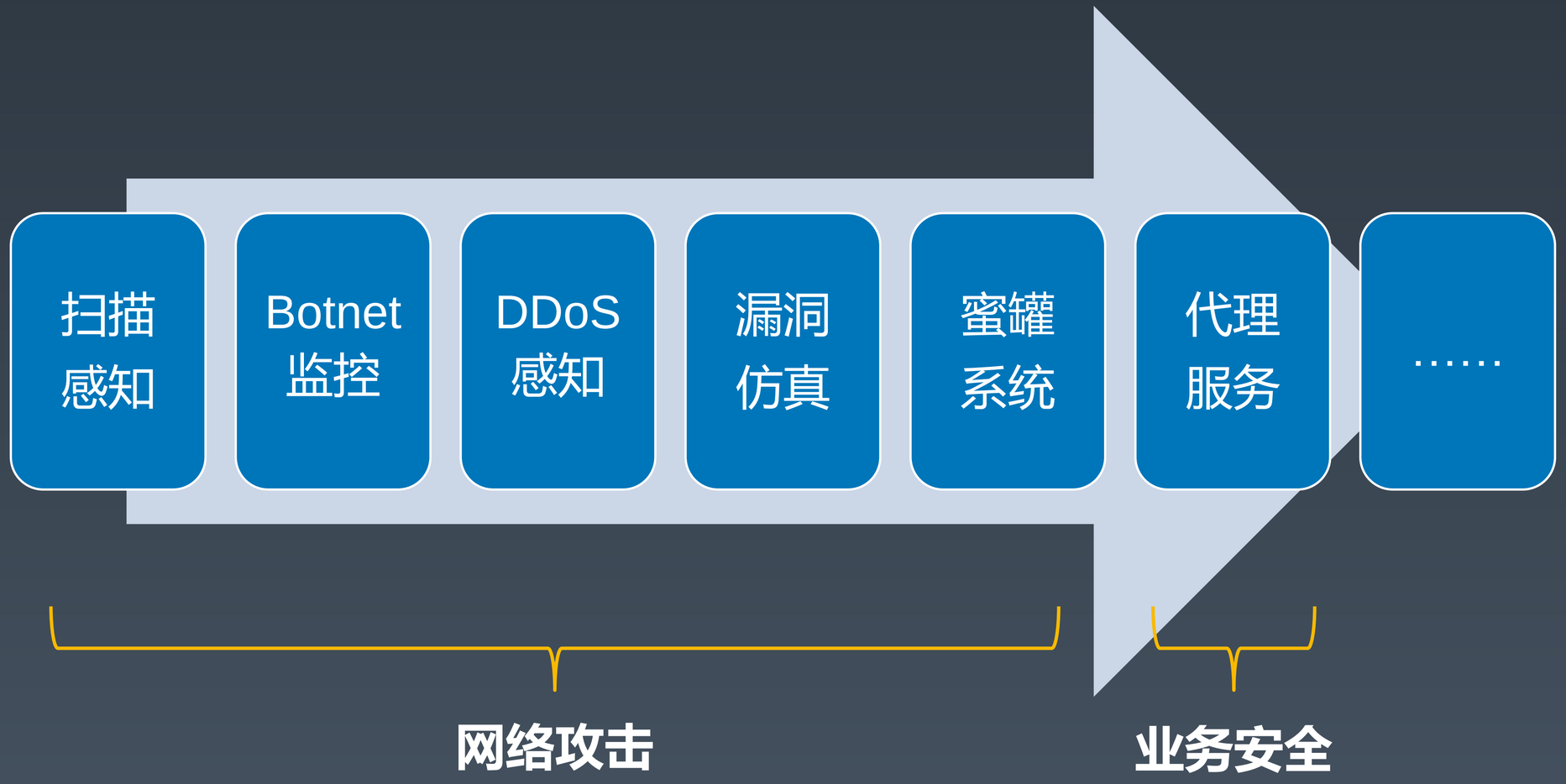


# 目录

1. 关于云安全
2. 恶意流量和互联网黑产
3. 恶意流量捕获
4. 一些宏观数据

# 构建恶意流量捕获体系

# 恶意流量捕获体系



# 端口扫描感知——传统方案

socket:
    bind, listen

缺点：
    1、只适合监听有限个数的端口
    2、如大量监听会占用大量文件句柄，易导致系统资源卡死
    3、大量高端口占用，影响正常网络连接
    4、无法捕获半开扫描，ICMP协议等

# 全端口扫描感知

实现方案：

NFQUEUE + Scapy

```
iptables -A INPUT -j NFQUEUE --queue-num 0
```

优点：

1、极低资源占用下监控完整 65535 个 TCP/UDP 端口

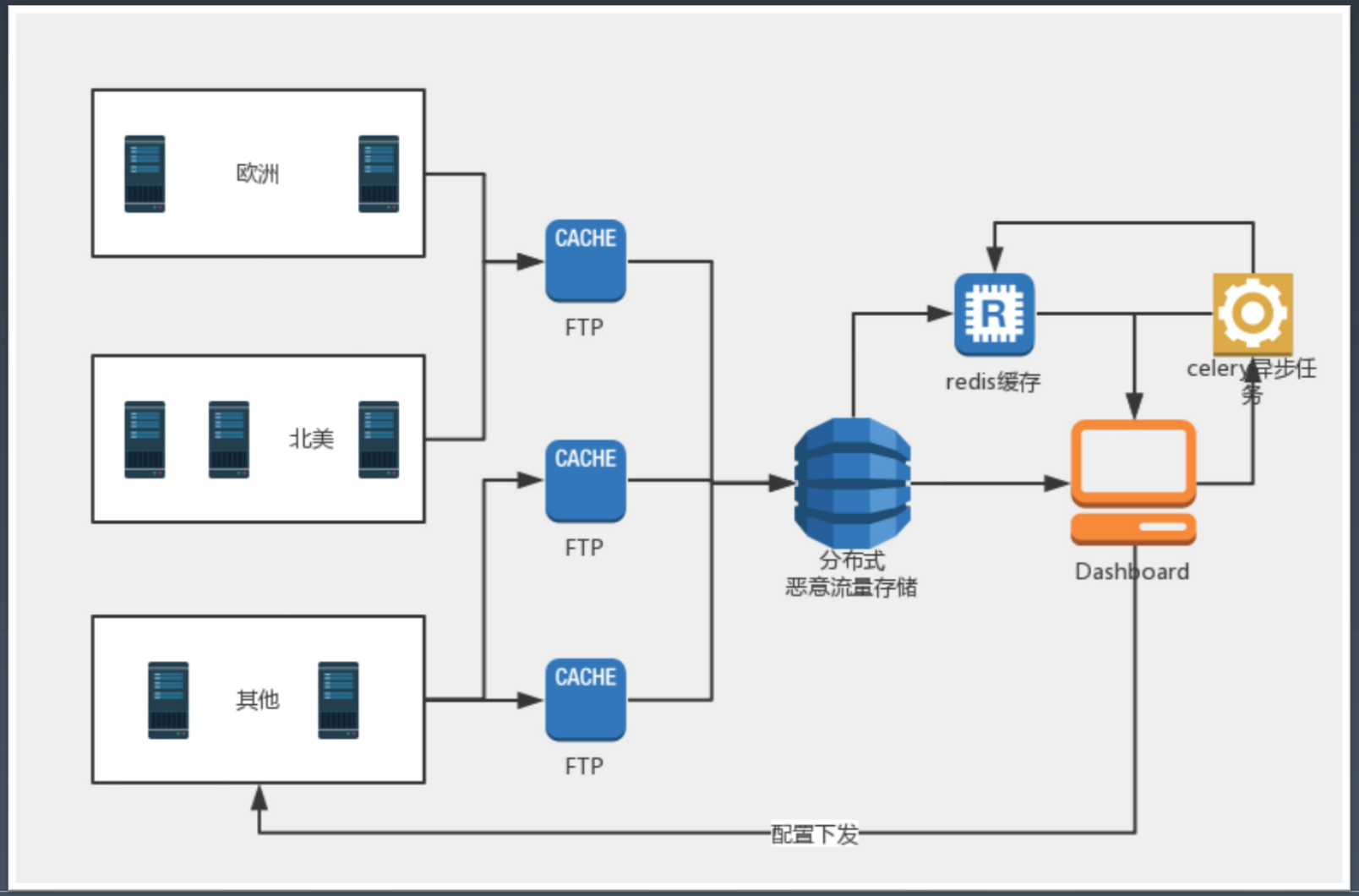
2、完全自主，灵活性高

缺点：

1、要自己实现底层功能，如 TCP 三次握手。

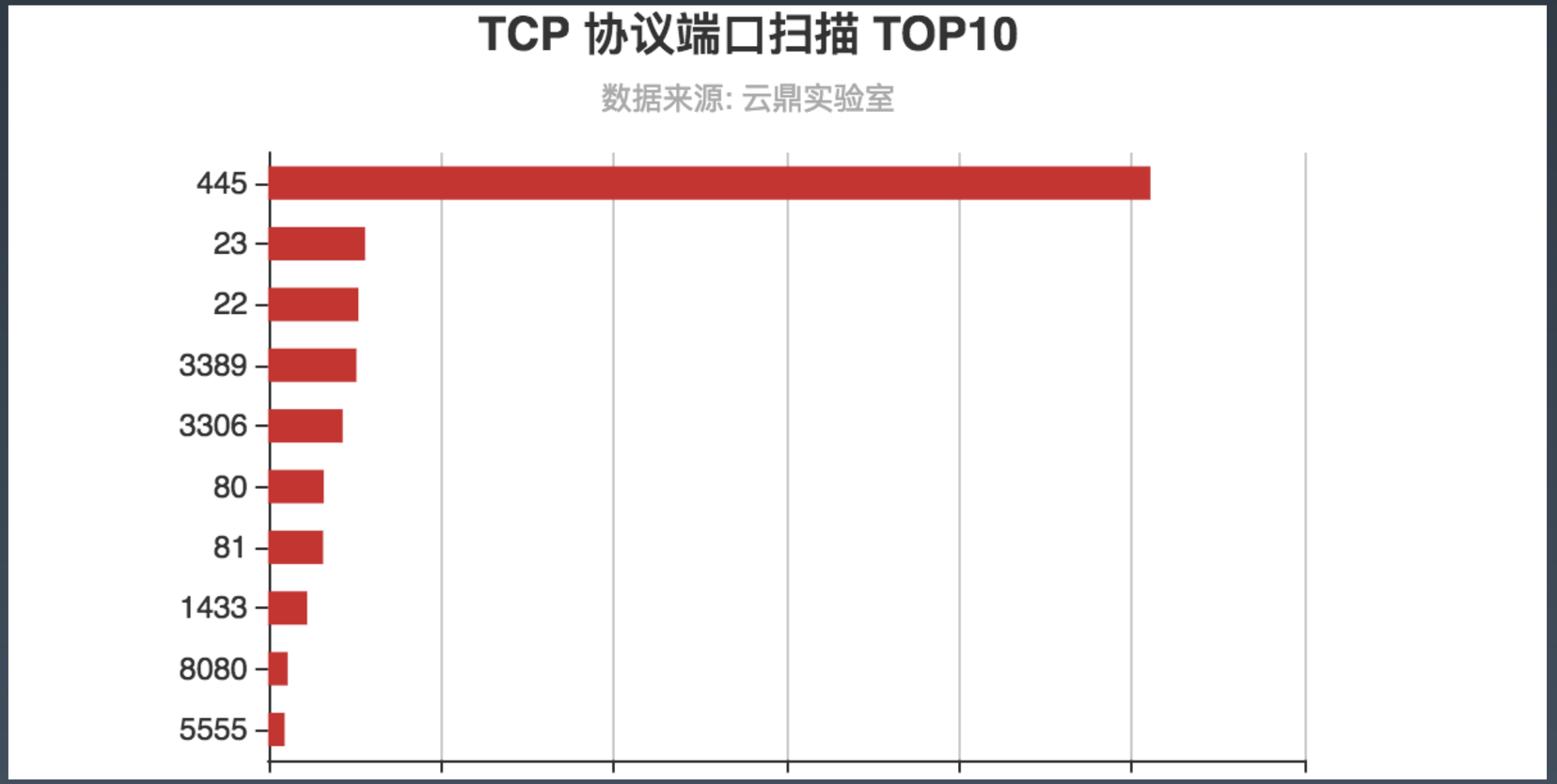
# 业务安全类最佳切入点——代理服务

# 听风系统架构图


欧洲
北美
其他
CACHE
FTP
CACHE
FTP
CACHE
FTP
redis缓存
celery异步任务
分布式
恶意流量存储
Dashboard
配置下发

# 目录

# TCP 协议端口扫描 TOP 10



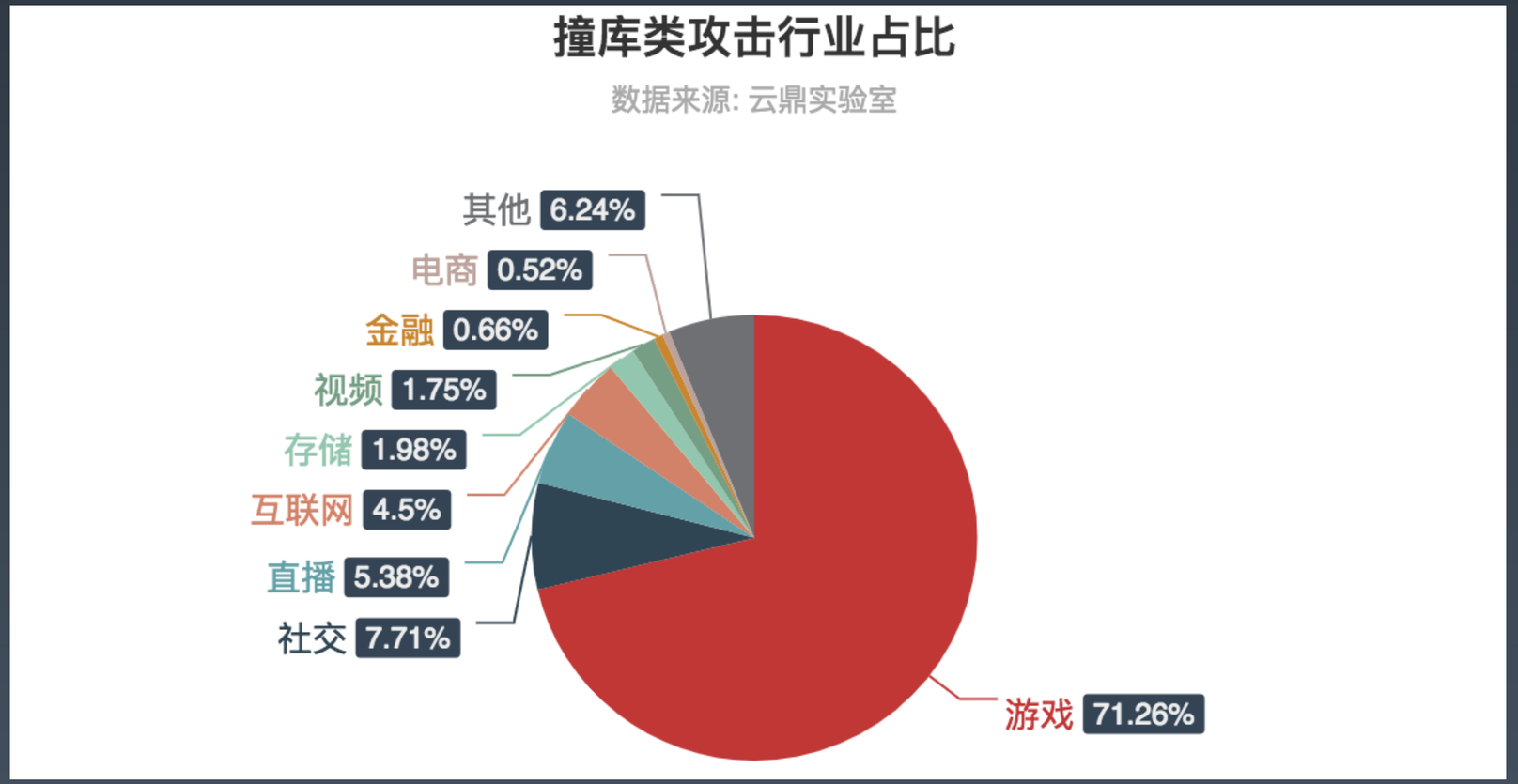
# TCP 扫描 TOP 10 端口详情

| TCP 端口 | 涉及环境/协议 | 说明 |
| --- | --- | --- |
| 445 | SMB | 永恒之蓝/勒索病毒 |
| 23 | Telnet | Telnet 登录 |
| 22 | SSH | Linux 远程登录 |
| 3389 | RDP | Windows 远程桌面 |
| 3306 | MYSQL | 数据库 |
| 80/8080 | Web | 众多web服务 |
| 81 | Web/IoT | web服务或某些物联网设备 |
| 1433 | SQL Server | 数据库 |
| 5555 | adb 远程调试 | Android |

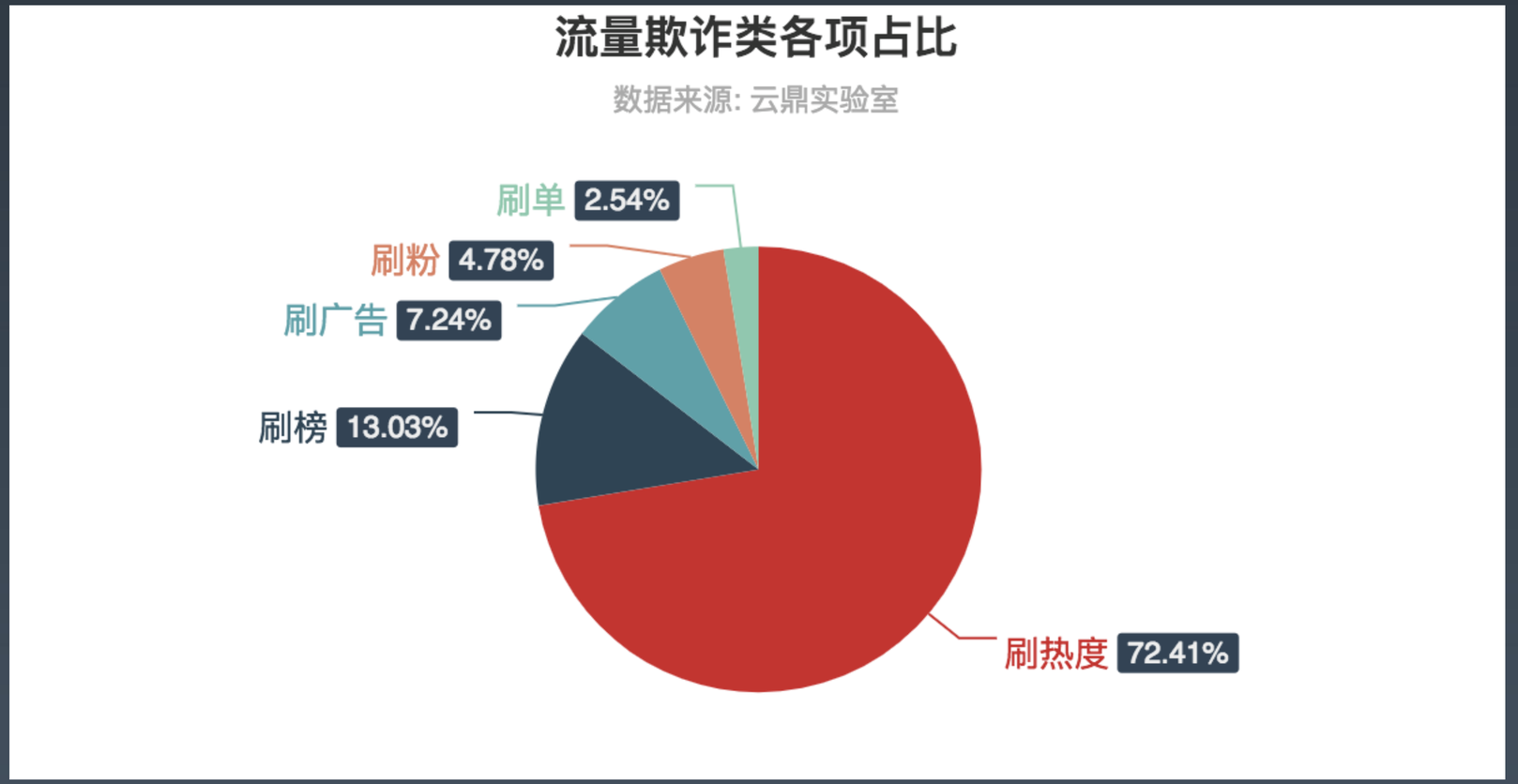
# TCP 扫描部分长尾端口详情

| TCP 端口 | 涉及环境/协议 | 说明 |
| --- | --- | --- |
| 7547 | TR-064 协议 | 涉及多个路由器品牌 |
| 8291 | MikroTik Winbox | 路由器漏洞 |
| 8088 | Hadoop | 远程执行漏洞 |
| 5900 | VNC | 远程控制弱口令漏洞 |
| 8545 | JSON-RPC | 以太坊节点服务器，盗取ETH |
| 9300 | ElasticSearch | 漏洞 |
| 11211 | Memcache | 漏洞 |
| 5984 | CouchDB | 漏洞 |
| …… | …… | …… |

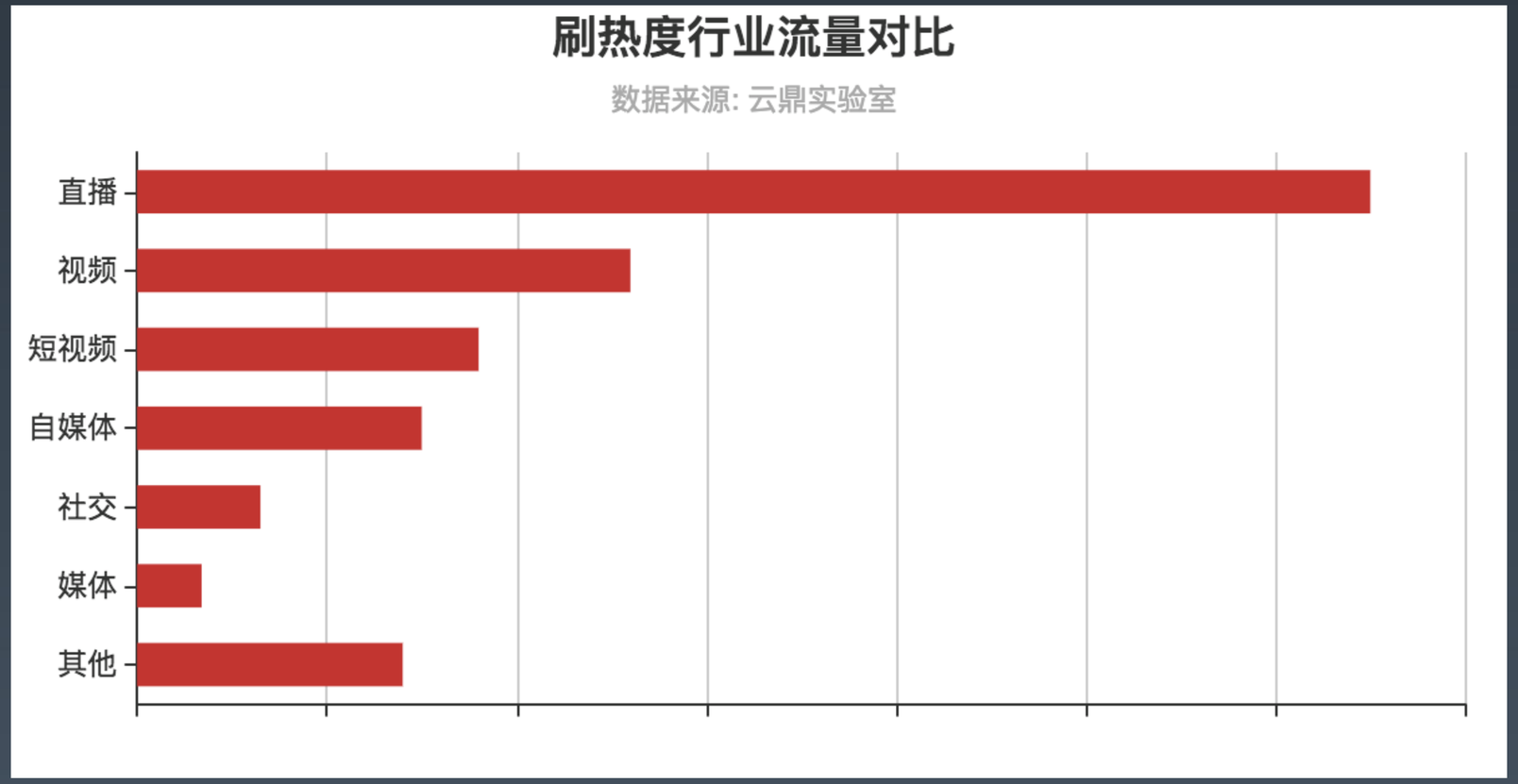
# 撞库类攻击行业占比


撞库类攻击行业占比
数据来源: 云鼎实验室
其他 6.24%
电商 0.52%
金融 0.66%
视频 1.75%
存储 1.98%
互联网 4.5%
直播 5.38%
社交 7.71%
游戏 71.26%

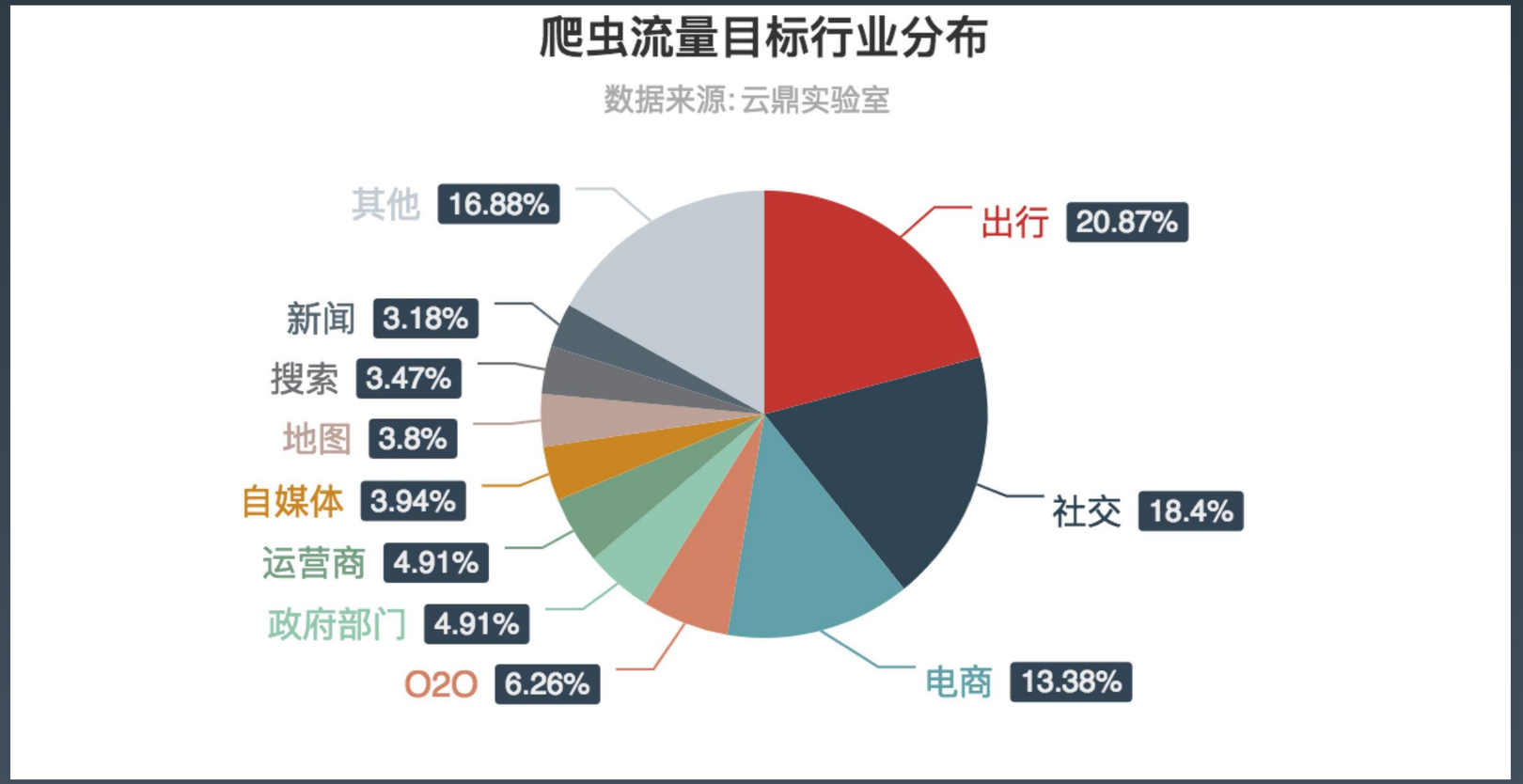
# 流量欺诈类各项占比



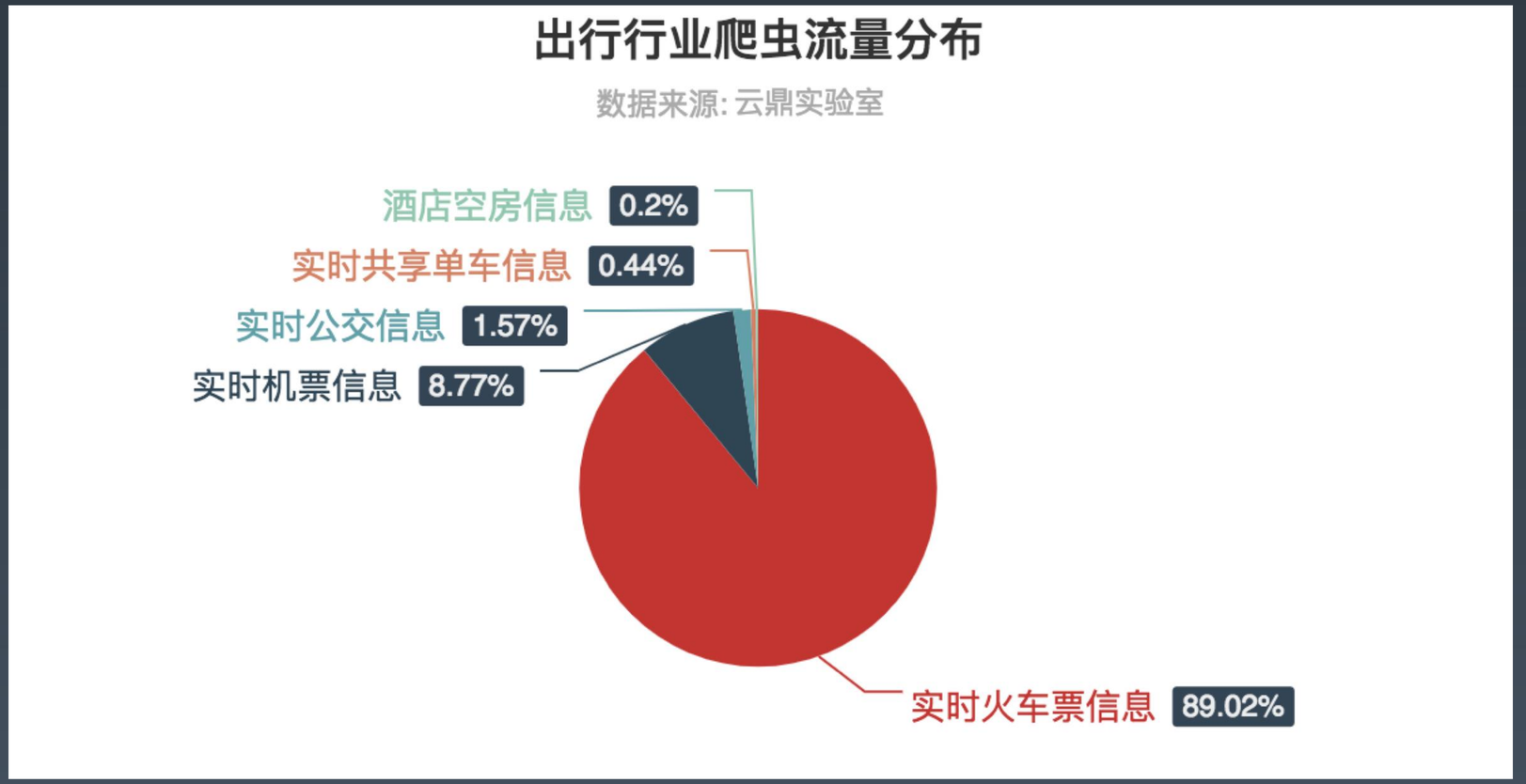
# 刷热度行业流量占比



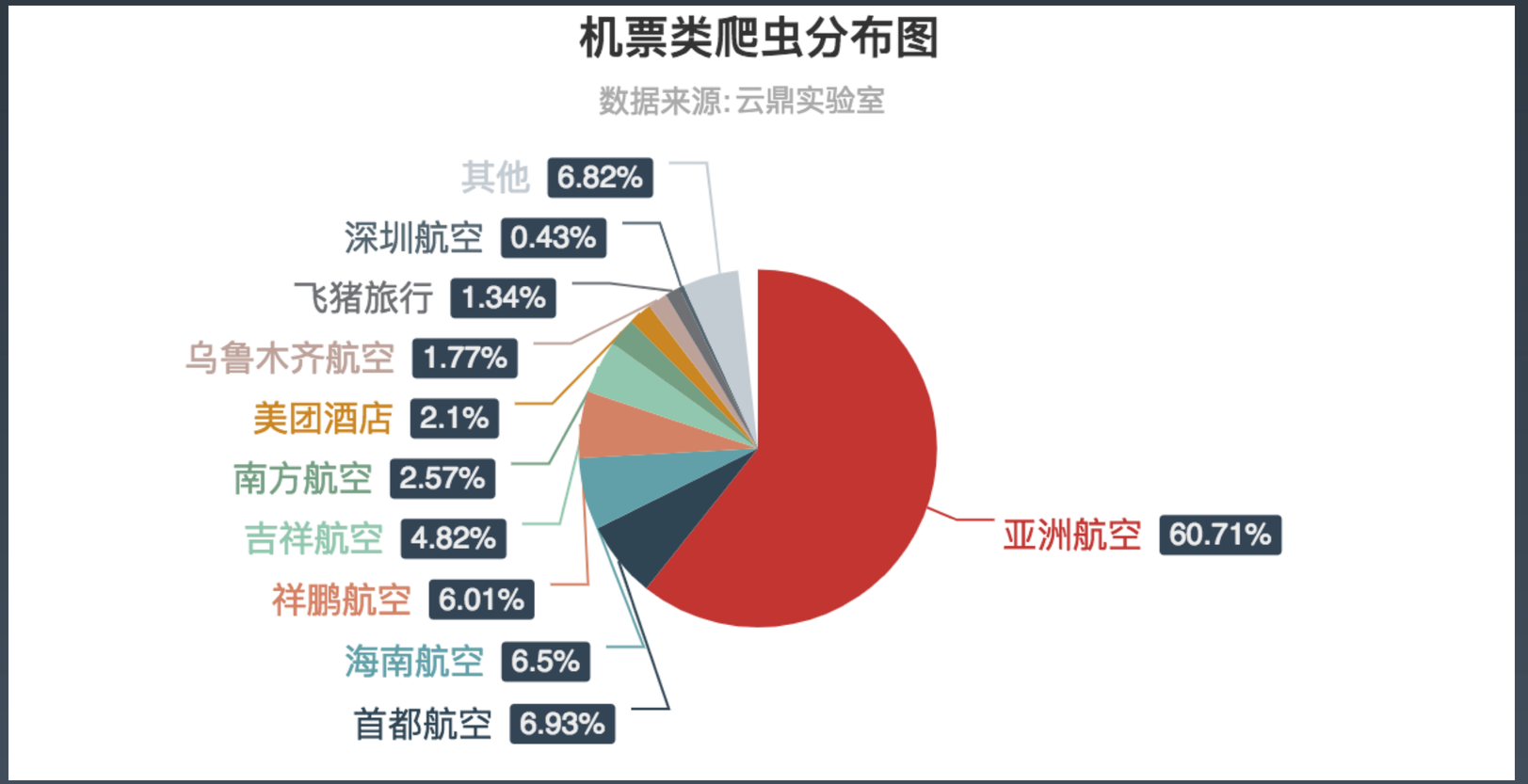
# 爬虫流量目标行业分布


爬虫流量目标行业分布
数据来源: 云鼎实验室
其他 16.88%
出行 20.87%
新闻 3.18%
搜索 3.47%
地图 3.8%
自媒体 3.94%
社交 18.4%
运营商 4.91%
政府部门 4.91%
O2O 6.26%
电商 13.38%

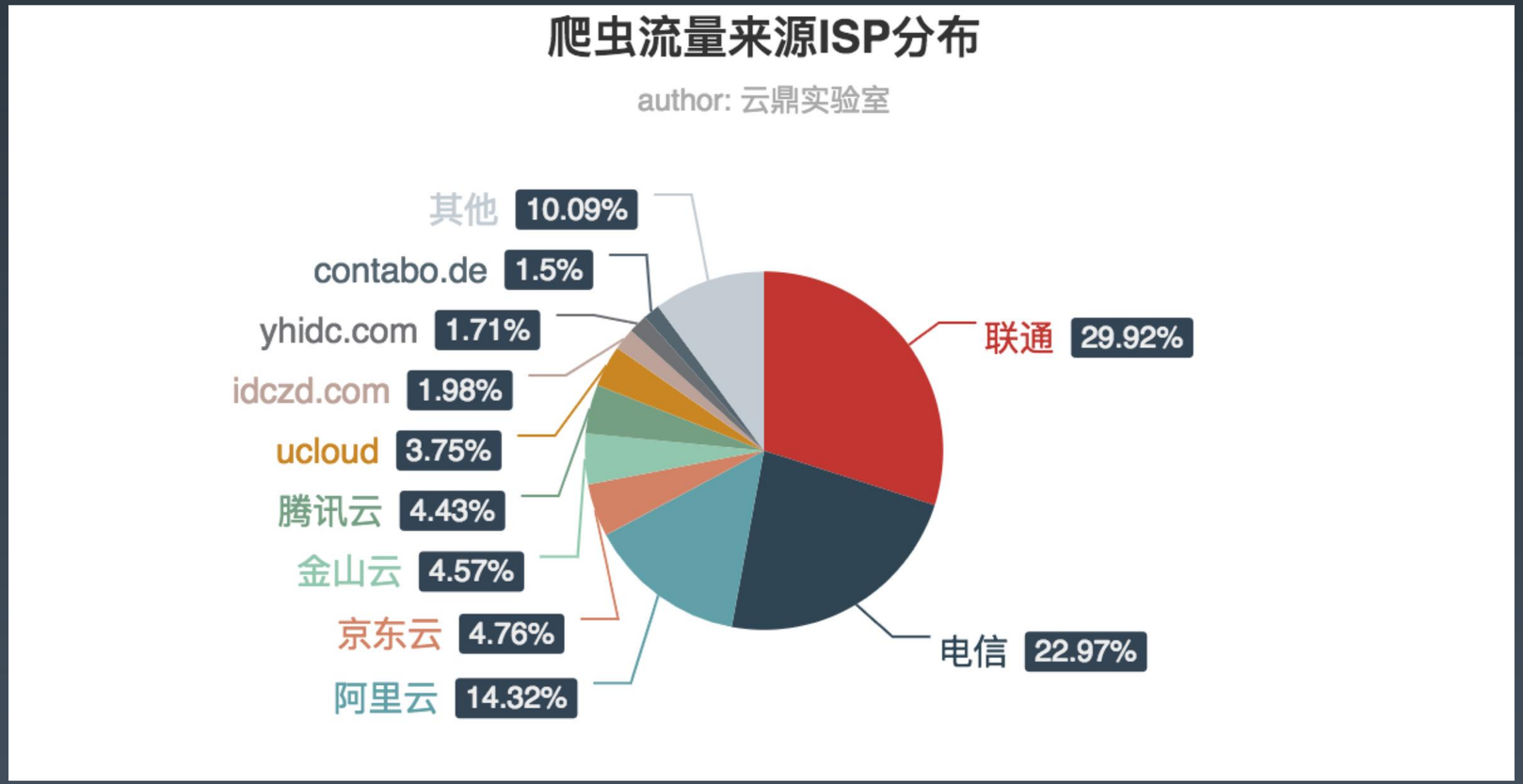
# 出行行业爬虫流量分布


出行行业爬虫流量分布
数据来源: 云鼎实验室
酒店空房信息 0.2%
实时共享单车信息 0.44%
实时公交信息 1.57%
实时机票信息 8.77%
实时火车票信息 89.02%

# 机票类爬虫分布


机票类爬虫分布图
数据来源: 云鼎实验室
其他 6.82%
深圳航空 0.43%
飞猪旅行 1.34%
乌鲁木齐航空 1.77%
美团酒店 2.1%
南方航空 2.57%
吉祥航空 4.82%
祥鹏航空 6.01%
海南航空 6.5%
首都航空 6.93%
亚洲航空 60.71%

# 爬虫流量来源 ISP 分布



# 爬虫光顾榜TOP 50

（2018上半年采样数据，仅供参考）

| 序号 | 公司 | 域名 | 流量占比 | 序号 | 公司 | 域名 | 流量占比 |
|---|---|---|---|---|---|---|---|
| 1 | 中国铁路客户服务中心 | 12306.cn | 18.65% | 26 | 国家企业信用信息公示系统 | gsxt.gov.cn | 0.16% |
| 2 | 微博 | weibo.cn | 18.05% | 27 | 首都航空 | jdair.net | 0.14% |
| 3 | 淘宝 | taobao.com | 12.16% | 28 | 拼多多 | yangkeduo.com | 0.13% |
| 4 | 百度 | baidu.com | 6.22% | 29 | 海南航空 | hnair.com | 0.13% |
| 5 | 大众点评 | dianping.com | 6.14% | 30 | 祥鹏航空 | luckyair.net | 0.12% |
| 6 | 联通 | 10010.com | 4.82% | 31 | 四川住建厅 | scjst.gov.cn | 0.11% |
| 7 | 微信搜索 | weixin.sogou.com | 2.85% | 32 | 58同城 | 58.com | 0.10% |
| 8 | 最高人民法院公告查询 | court.gov.cn | 2.78% | 33 | 吉祥航空 | juneyaoair.com | 0.10% |
| 9 | 腾讯 | qq.com | 2.24% | 34 | 摩拜单车 | mobike.com | 0.09% |
| 10 | Google | google.com | 2.10% | 35 | 优酷网 | youku.com | 0.08% |
| 11 | 新浪 | sina.com.cn | 1.45% | 36 | 阿里妈妈 | alimama.com | 0.06% |
| 12 | 亚洲航空 | airasia.com | 1.22% | 37 | 唯品会 | vip.com | 0.06% |
| 13 | 智联招聘 | zhaopin.com | 1.02% | 38 | 太平洋汽车网 | pcauto.com.cn | 0.05% |
| 14 | 360搜索 | 360.cn | 0.79% | 39 | 南方航空 | csair.com | 0.05% |
| 15 | 北京市预约挂号统一平台 | bjguahao.gov.cn | 0.74% | 40 | 盛大游戏 | sdo.com | 0.04% |
| 16 | 搜狗 | sogou.com | 0.73% | 41 | Youtube | youtube.com | 0.04% |
| 17 | 京东 | jd.com | 0.58% | 42 | 美团 | meituan.com | 0.04% |
| 18 | 搜狐 | sohu.com | 0.55% | 43 | 中国港口网 | chinaports.com | 0.04% |
| 19 | 高德地图 | amap.com | 0.50% | 44 | 乌鲁木齐航空 | urumqi-air.com | 0.04% |
| 20 | 国家知识产权局 | sipo.gov.cn | 0.48% | 45 | 信用福建 | fjcredit.gov.cn | 0.04% |
| 21 | 车来了 | chelaile.net.cn | 0.33% | 46 | 飞猪旅行 | fliggy.com | 0.03% |
| 22 | 天猫商城 | tmall.com | 0.30% | 47 | 全国建筑市场监管公共服务平台 | mohurd.gov.cn | 0.02% |
| 23 | 信用中国 | creditchina.gov.cn | 0.24% | 48 | 韵达快递 | yundasys.com | 0.02% |
| 24 | 信用安徽 | creditah.gov.cn | 0.23% | 49 | 乐途旅游网 | lotour.net | 0.02% |
| 25 | ASK.com | ask.com | 0.18% | 50 | 芒果TV | mgtv.com | 0.02% |

即使是黑洞
依然有眼睛在注视着它！

Geekbang. 极客邦科技 InfoQ

# 极客邦科技
# 会议推荐2019

## 5月

QCon 北京
全球软件开发大会
大会：5月6–8日
培训：5月9–10日

QCon 广州
全球软件开发大会
培训：5月25–26日
大会：5月27–28日

## 6月

GTLC GLOBAL TECH LEADERSHIP CONFERENCE 上海
技术领导力峰会
时间：6月14–15日

GMTC 北京
全球大前端技术大会
大会：6月20–21日
培训：6月22–23日

## 7月

ArchSummit 深圳
全球架构师峰会
大会：7月12–13日
培训：7月14–15日

## 10月

QCon 上海
全球软件开发大会
大会：10月17–19日
培训：10月20–21日

## 11月

GMTC 深圳
全球大前端技术大会
大会：11月8–9日
培训：11月10–11日

AiCon 北京
全球人工智能与机器学习大会
大会：11月21–22日
培训：11月23–24日

## 12月

ArchSummit 北京
全球架构师峰会
大会：12月6–7日
培训：12月8–9日

# THANKS!

QCon 10th