一人之下，建立黑色产业帝国

徐三中 | FreeBuf年度优秀作者

黑色产业链生态

流量获取分发

最重要一环

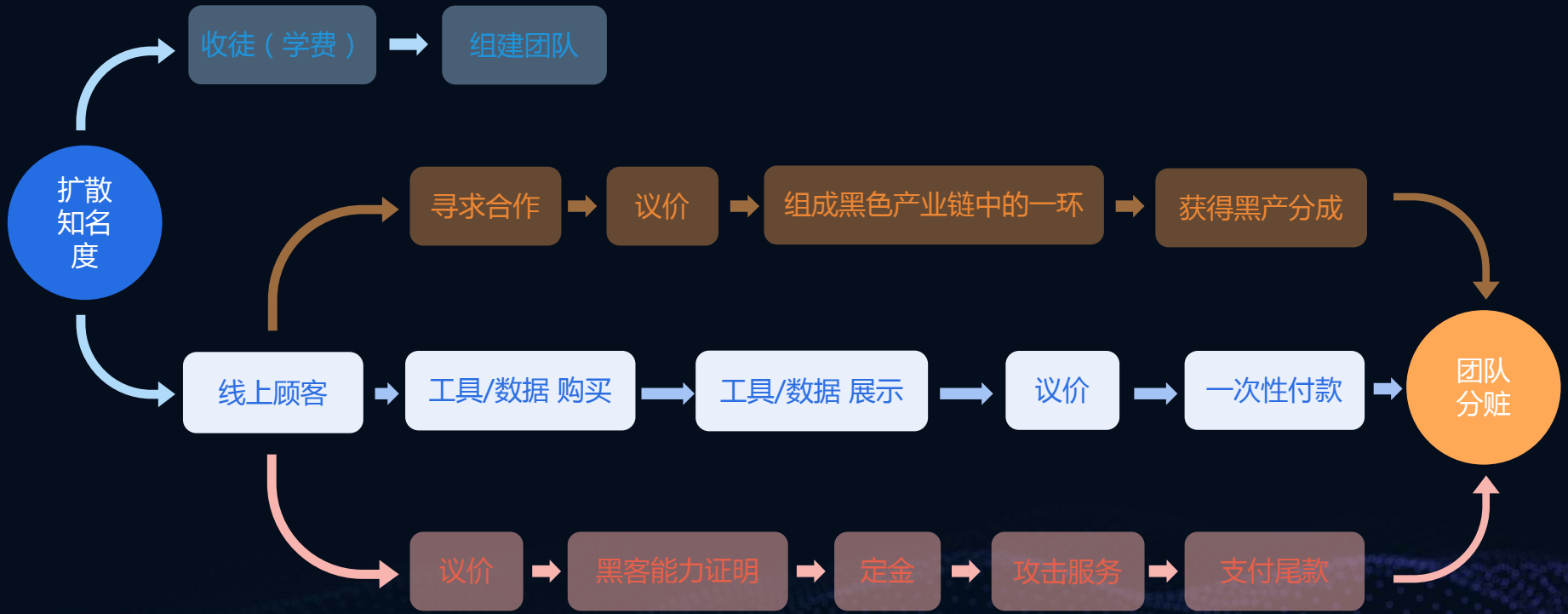
流量变现盈利

最根本生存法则

用户隐私与重要数据

影响最大、最复杂

典型的黑色产业链条

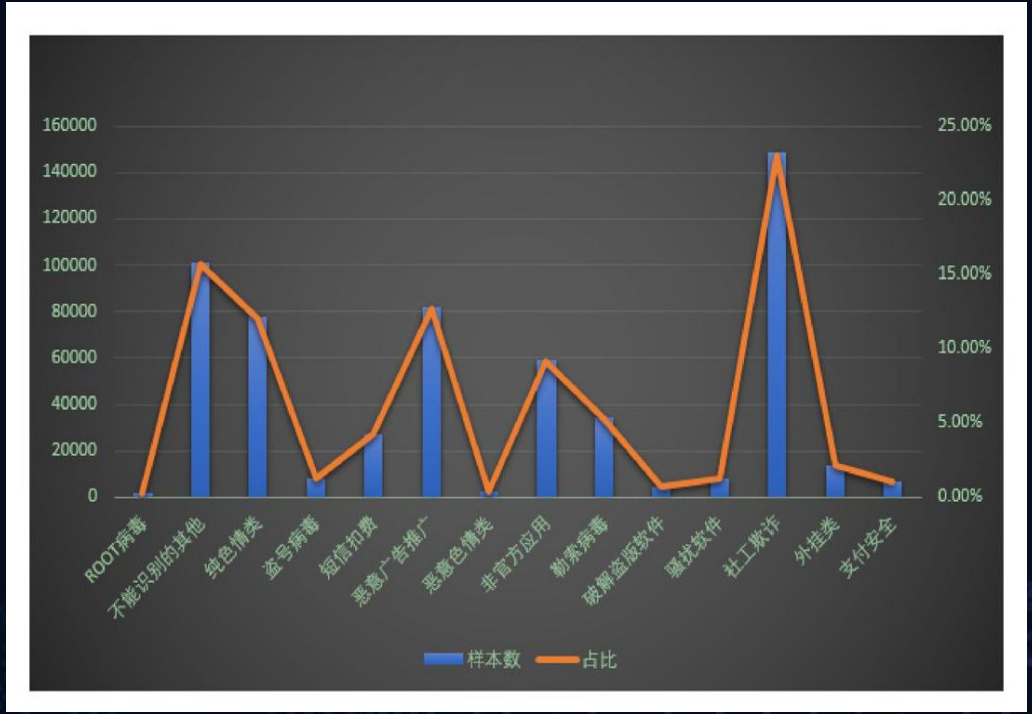

收徒（学费）
组建团队
扩散知名度
寻求合作
议价
组成黑色产业链中的一环
获得黑产分成
线上顾客
工具/数据 购买
工具/数据 展示
议价
一次性付款
团队分赃
议价
黑客能力证明
定金
攻击服务
支付尾款

典型的移动互联网黑色产业链

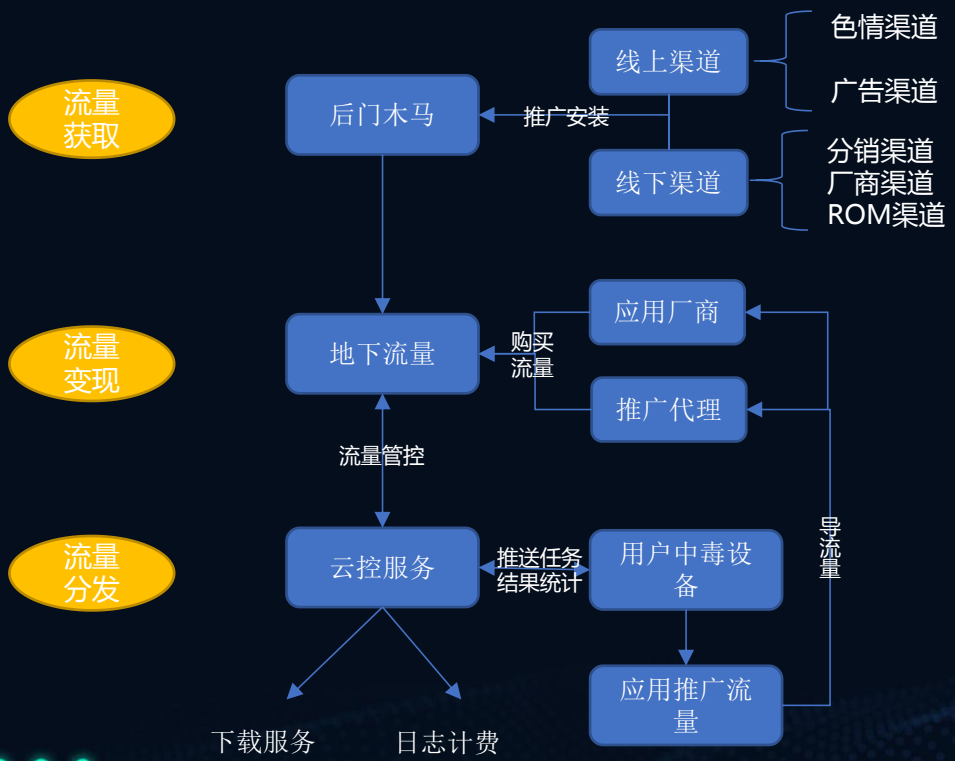
移动黑色产业链—制作


2008-2017年移动互联网恶意程序数量走势图
（来源：恒安嘉新（北京）科技股份公司）
30000
25000
20000
15000
10000
5000
0
396
664
1286
1945
2642
3053
3804
5103
8907
16022
24876
268
522
659
897
411
751
7115
8854
2008年
2009年
2010年
2011年
2012年
2013年
2014年
2015年
2016年
2017年
总量
新增

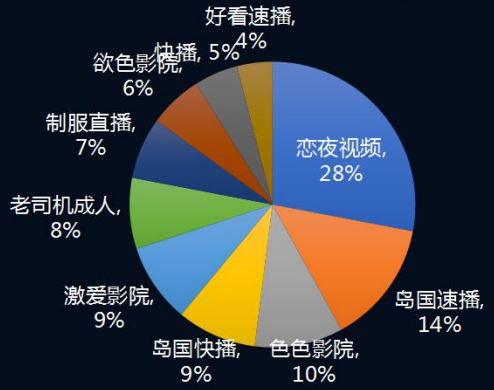

2017年移动互联网恶意程序捕获月度统计
（来源：恒安嘉新（北京）科技股份公司）
10000
9000
8000
7000
6000
5000
4000
3000
2000
1000
0
459
394
853
573
1426
517
1943
679
2622
968
3590
876
4466
1320
5786
1017
6803
743
7546
641
8187
667
8854
1月
2月
3月
4月
5月
6月
7月
8月
9月
10月
11月
12月
新增
总量


160000
140000
120000
100000
80000
60000
40000
20000
0
25.00%
20.00%
15.00%
10.00%
5.00%
0.00%
ROOT病毒
不能识别的其他
纯色情类
盗号病毒
短信扣费
恶意广告推广
恶意色情类
非官方应用
勒索病毒
破解盗版软件
骚扰软件
社工欺诈
外挂类
支付安全
样本数
占比

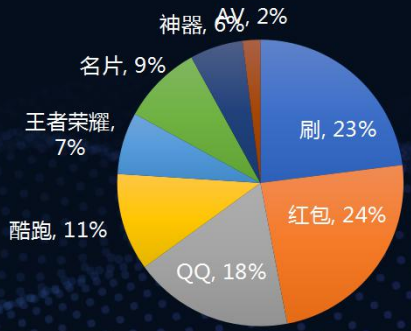
移动黑色产业链—传播



色情类病毒统计



勒索类名称统计



移动黑色产业链—获利

- 勒索病毒
  - 解锁费
  - 进群费
  - 收徒费
- 色情病毒
  - 广告费
  - SP扣费
  - 诱导收费
- 拦截木马
  - 钓鱼获利
  - 信息贩卖
  - 钓鱼获利
- 银行木马
  - 资产转移
  - 信息贩卖
- 挖矿木马
  - 对于黑客来说，由于其掌握了大量的手机资源，则无需任何成本就能进行远程挖矿，从而导致了挖矿木马的迅速增长。
- 钓鱼网站
  - 银行卡盗刷
  - 好友诈骗
  - 敲诈勒索
- 博彩
  - 这种对外发行的彩票没有任何关系，通过高中 称之为“博彩”或黑。通过高中 奖率来吸引彩民，同时以类似于间借贷方式进行 奖率来吸引彩民
- 网络诈骗
  - 移动互联网传销使用了隐秘的不公开手段，它得利方式同样是交纳会费，然后再拉人进入作为自己的下线

黑色产业链的新趋势

恶意软件加固技术

云端动态加载技术

移动端APT攻击

挖矿病毒

定向勒索病毒

薅羊毛攻击

案例：创建视频黑色产业链

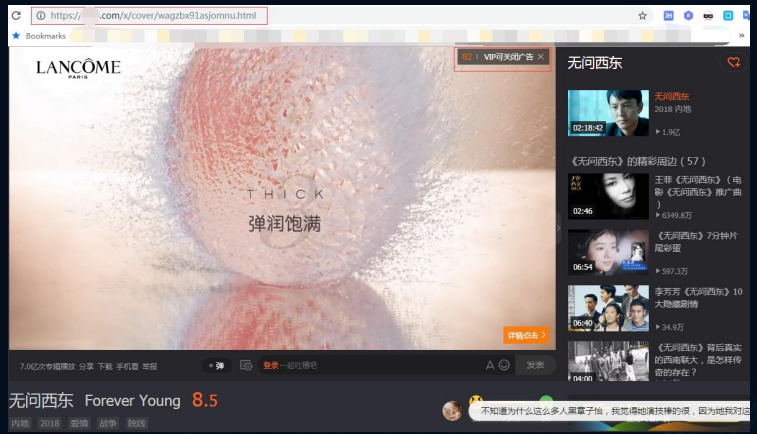
- 点播视频
- 直播视频
- 移动短视频
- 音乐视频
- 培训课程视频

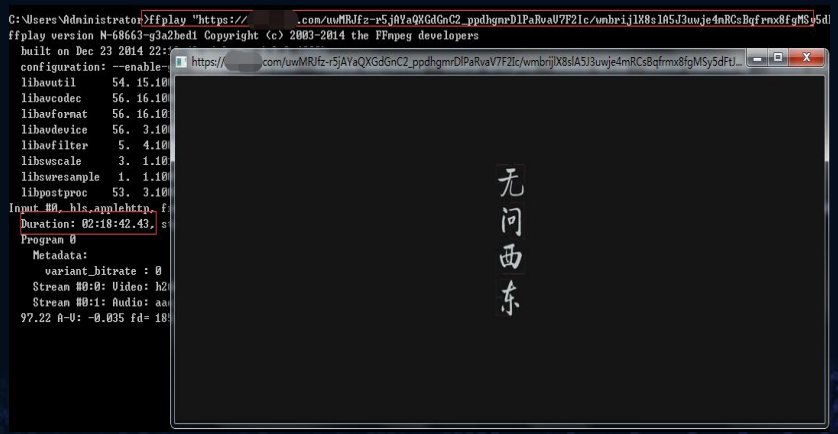
案例：创建视频黑色产业链

资源爬虫 → 盗链解析 → 视频聚合 → 应用分发 → 获利 → 用户流量 → 产业拓展

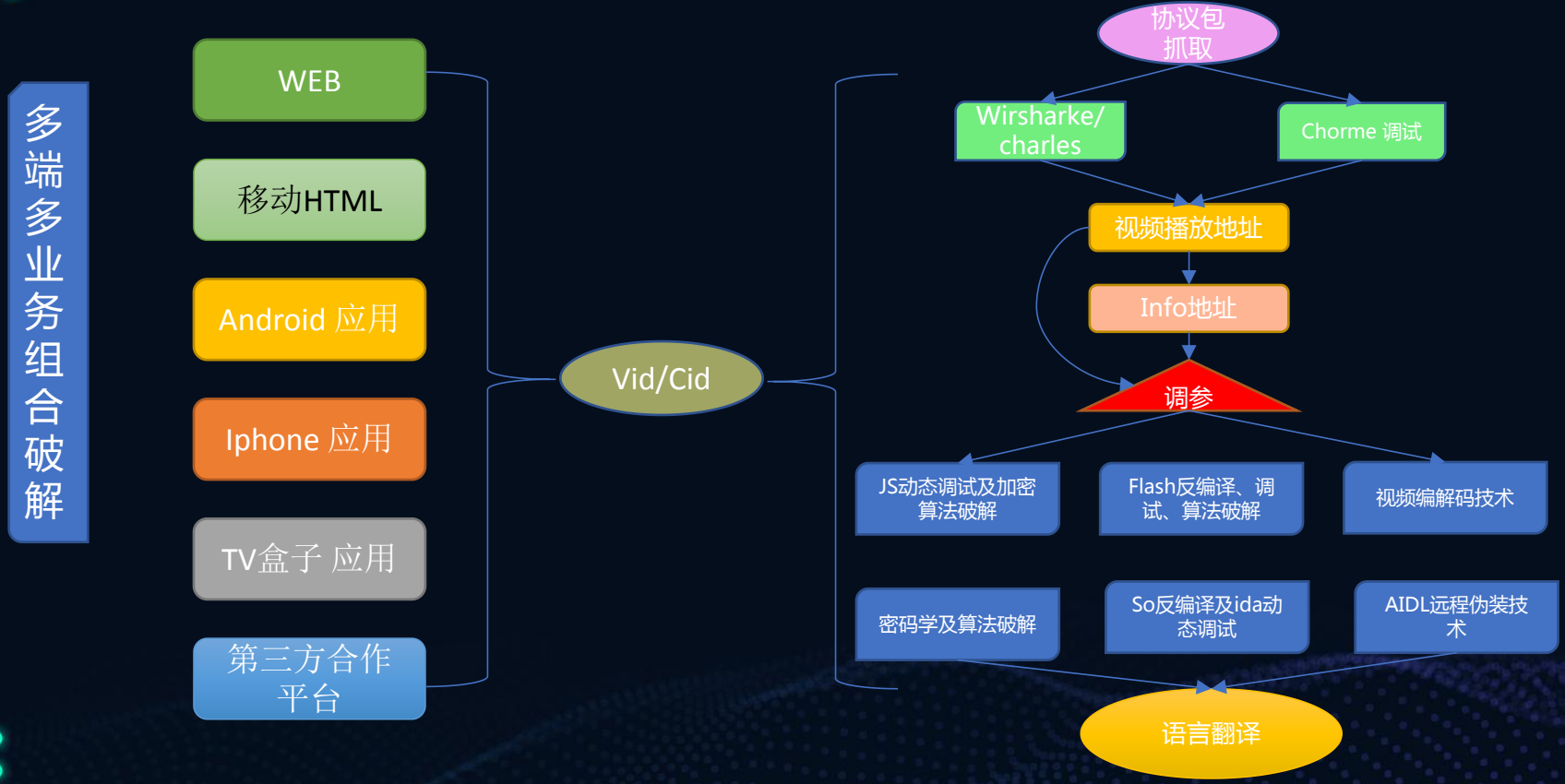
https://*** /wagzbx91asjomnu.html

https://***/g0027ko5qhe.321002.ts.m3u8?ver=4

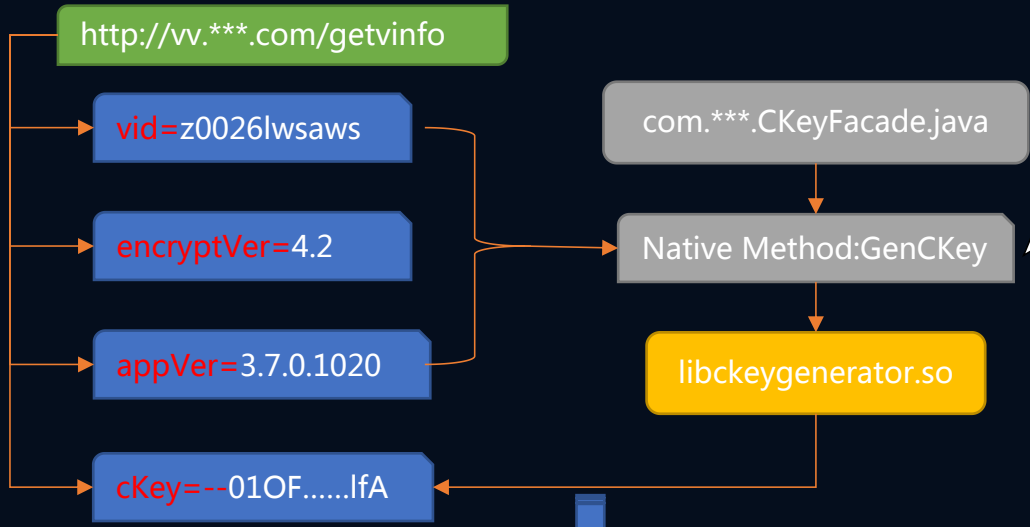




案例：创建视频黑色产业链



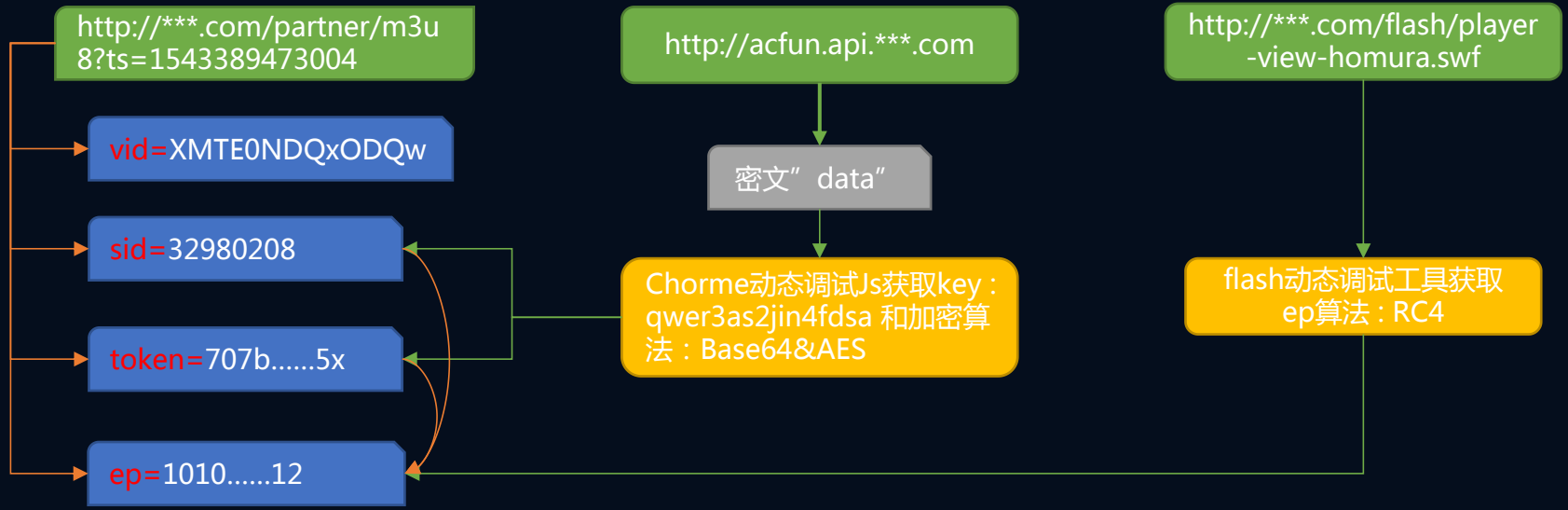
案例：创建视频黑色产业链



贴士：
（加密算法so文件进行了加固、混淆和反调试）
1、调用ckey算法文件，必须使用AIDL模拟原应用远程进程。除了Native方法传入参数，还有context上下文参数。
2、不同参数appVer、encryptVer不同，导致加密算法有所改变。
3、本接口共传入11个参数，任何参数的位置和值错误，会导致ckey值获取错误，或能得到响应结果，但得到视频卡顿。

```
(GenCKey(kPlatInfo.get("kTCSDKVersion"), time_t, vid, i4, Integer.parseInt(kPlatInfo.get("kPlatformId")), i5, RandKey, "fceg", "",
(GenCKey(kPlatInfo.get("KAppVer"), time_t, vid, i4, Integer.parseInt(kPlatInfo.get("kPlatformId")), i5, RandKey,
        kPlatInfo.get("kSdtfrom"), "", getGuid(), iArr, iArr.length));
```

案例：创建视频黑色产业链



打击黑产黑色产业链

FREEBUF | FIT

THANKS