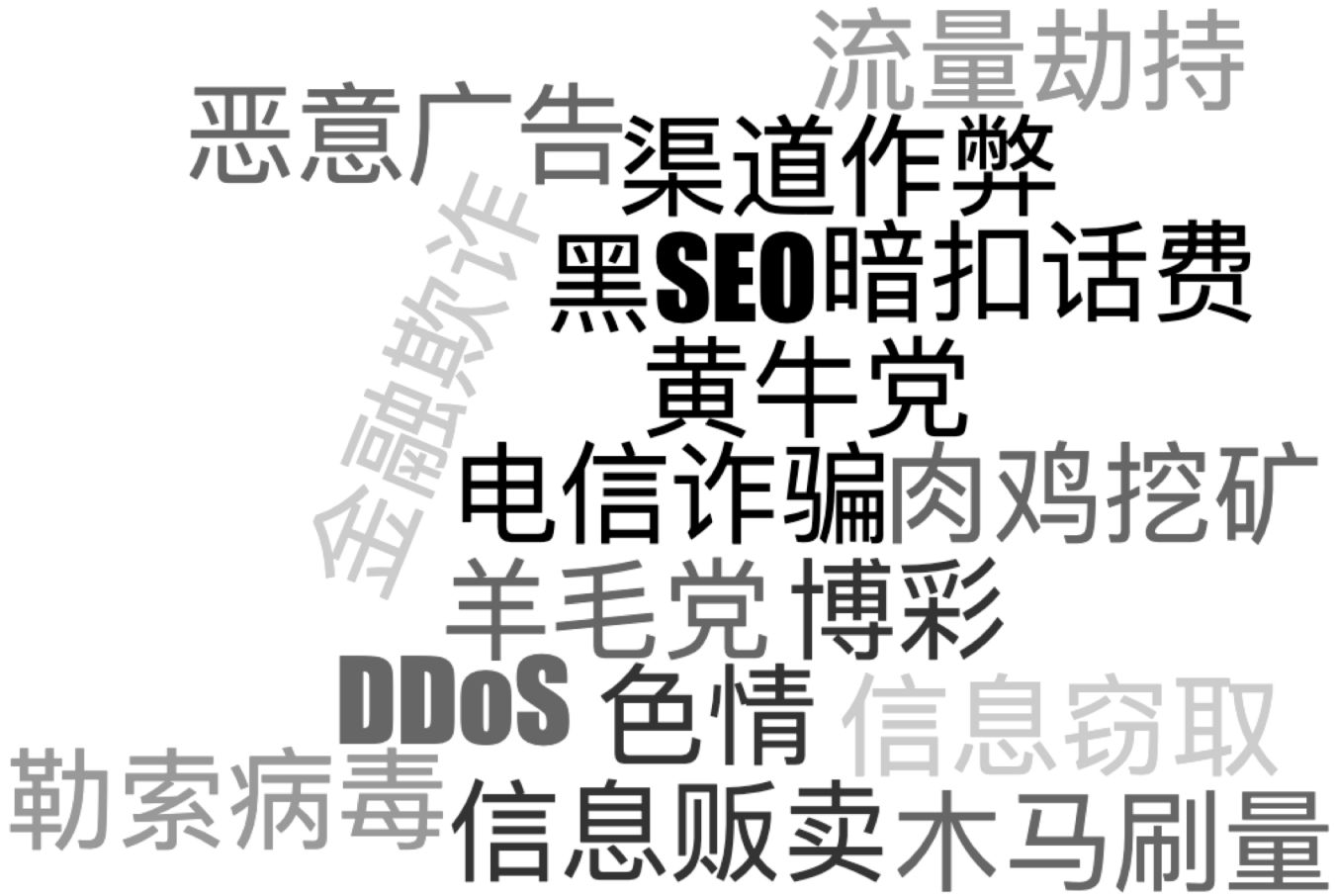
黑灰产对抗的攻守之道

—浅谈黑灰产风险及打击

c0rpse

2019.4.13

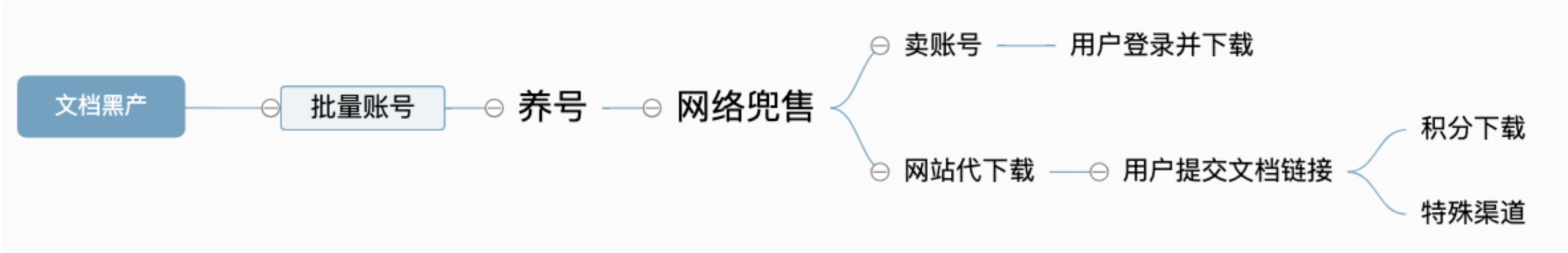

流量劫持
恶意广告
渠道作弊
金融欺诈
黑SEO暗扣话费
黄牛党
电信诈骗
肉鸡挖矿
羊毛党
博彩
DDoS
色情
信息窃取
勒索病毒
信息贩卖
木马刷量

色情：四道贩子的勾结作案史

撞库工具 + 社工数据 + 账号贩子 + 色情贩子

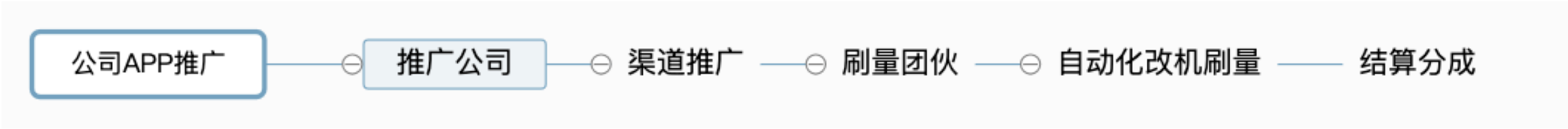
撞库IP -> IDC固证 ->撞库人员 -> 工具作者

生财有道：黑灰产在线文档服务“生意经”



甲方：异常请求 -> 可疑域名 -> 友情检测+固证

似黑非黑：APP刷量羊毛党的覆灭



套路：基础设施->踩点->实施->获利变现->GG

基础设施：自动化攻击工具、漏洞利用工具、IP代理、打码平台、模拟器、分身软件、改机软件、群控牧场、接码平台、猫池卡商、身份认证四件套

踩点：情报搜集分享 + 卧底竞对 + case by case

实施：漏洞脚本攻击、移动场景下的基于硬件设备的批量自动化攻击

获利变现：现金提现、优惠券倒卖、实体货物变现、勾结分成

黑灰产威胁情报的发掘

Q&A

Have a good day!

THANKS

Have a good day!