网络安全创新大会
Cyber Security Innovation Summit

无处不在的黑色产业链

辛巴 Freebuf年度作者

议题大纲一览

一.黑色产业链的收割链条

二.网络犯罪打击的关键点

三.黑吃黑的那些蜜汁操作

四.跟写小说一样的技术犯罪

一.黑色产业链的收割链条

1 诈骗.赌博

1.老少皆宜，四季常青

划分人群，年龄段，外部信息特征，进行针对性的违法犯罪活动。

2.数据提取，精准投放

筛选购买的各种数据进行比对排查自己需要的信息，然后通过短信，邮箱进行投放。

3.开始收割，循环往复

被收割的首要条件，就是你对这个感兴趣，可能是想赚点小钱，也可能是自己本来有这个爱好。

2 刷单. 投资. 彩票=杀猪盘

在这三种诈骗中，分别利用了三种需求，针对性较强，也是目前诈骗成功率最高，受害者最多，损失最大的

刷单诈骗

上当人数较多，诈骗金额相对较小，因为诈骗主体以年轻人为主。

投资诈骗

主要目标主体是各类婚恋，相亲，异性交友平台的男性女性。

彩票诈骗

主要目标主体为社交平台上的人群，无固定目标，通过群刷广告等羊上门。

通过精准信息短信引流

通过盗取社交账号来引流

X音/X探/souX

二.网络犯罪打击的关键点

1. 底层的源头治理

网络实名制，对公账户，银行卡四件套，电话卡，社交平台账户。（断卡行动）

2. 提升犯罪成本

提升犯罪成本，挤压犯罪团伙的生存空间，通过源头治理的方式，在基于所有的犯罪都是用于牟利这一条，斩断或者阻碍该产业链的运行。

3. 提升公民安全意识

对国内的公民进行普法，反诈的宣传力度，在能被人民群众接收到网络安全教育的渠道进行宣传，有意识的去了解各种可能带来的危害后果和套路手段。

二.网络犯罪打击的关键点

4. 黑产的好伙伴

黑帽SEO-黑产的进项保障

入侵大量的国内网站，进行快速排名收录，劫持跳转至违法网站。

【👑👑👑】余生( ) 2020/12/3 14:31:58

引流卖什么产品

【私下被骗不管】等风来。( ) 2020/12/3 14:32:06

- 知识付费的
- 现在用的Q群的，一天能加个几千个群
- 微群，Q群，都有在做
- 想在扩展下别的
- 25吧 私人号好像

【私下被骗不管】等风来。( ) 2020/12/3 14:33:47

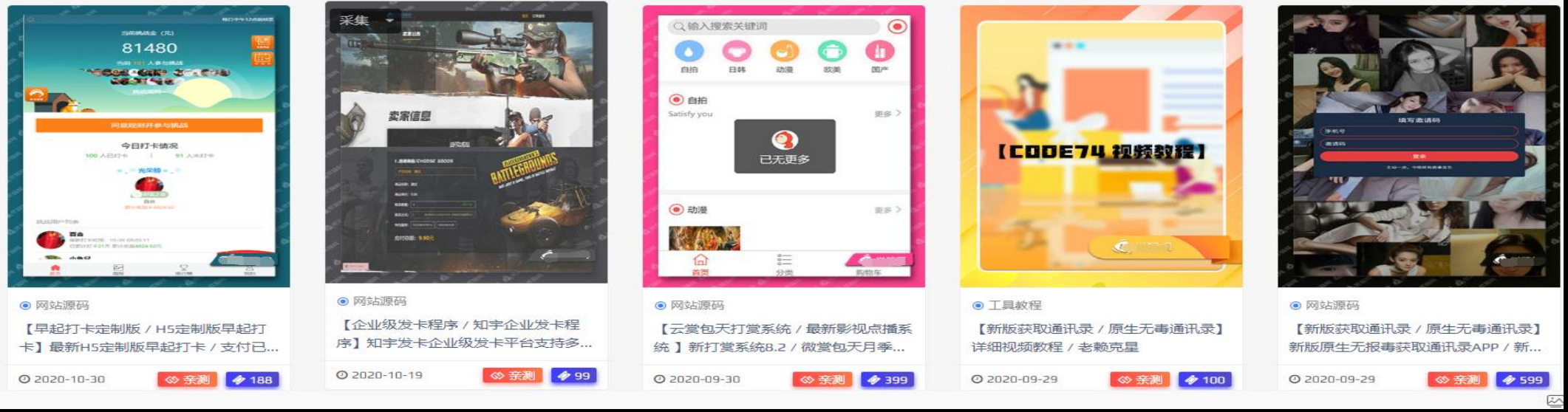
- 我这边快手号才3块钱一个，上去直接点关注，发不了私信
- 找个脚本，能在评论区 关注的
- 直接上号点就行了
- 一个号一天点200个关注，签名改好了，最低加过来5-10个人

【私下被骗不管】等风来。( ) 2020/12/3 14:36:04

- 手机成本一个二手小米4C 200左右，10部 2000块， 算上软件一个月100
- 模拟器组个服务器 一个月400 开10个模拟器跑脚本

二.网络犯罪打击的关键点

5. 网络空间环境治理



网站源码
【早起打卡定制版 / H5定制版早起打卡】最新H5定制版早起打卡 / 支付已...
2020-10-30 亲测 188

网站源码
【企业级发卡程序 / 知宇企业发卡程序】知宇发卡企业级发卡平台支持多...
2020-10-19 亲测 99

网站源码
【云赏包天打赏系统 / 最新影视点播系统 】新打赏系统8.2 / 微赏包天月季...
2020-09-30 亲测 399

工具教程
【新版获取通讯录 / 原生无毒通讯录】详细视频教程 / 老赖克星
2020-09-29 亲测 100

网站源码
【新版获取通讯录 / 原生无毒通讯录】新版原生无报毒获取通讯录APP / 新...
2020-09-29 亲测 599

游戏源码 金币系列
最新旺达棋牌游戏完美境外版本+完...
2020-09-06 131 ¥免费 推荐

程序源码
通讯录获取程序+短信获取+在线定...
2020-09-05 368 ¥688 精品

游戏源码 金币系列
最新天马电玩一夜暴富完美服务器打...
2020-09-05 110 ¥免费 已测试

游戏源码 金币系列
【博乐环球游戏服务端】2020新版...
2020-09-05 77 ¥免费 已测试

游戏源码 金币系列
2020最新网狐UI二开定制版三端齐...
2020-09-05 86 ¥免费 已测试

三.黑吃黑的蜜汁操作

1. 骗子想骗我，没办法，我把骗子骗了

常见的黑产模式，大型的黑色产业链从业者都有稳定的黑色收入，但是还有很多小型的犯罪团队的收入不足以支持其在境外立足，从而转化成了一些小型的，易于操作的违法犯罪手段，例如自己搭建裸聊平台，几人或者多人参与引流到诈骗的整个流程。

而这样的团队成百上千的活跃在QQ，souL，各大婚恋平台上面伺机而动，通过广告群发或者交友功能寻找受害者进一步的为后续的违法犯罪提供铺垫。

三.黑吃黑的蜜汁操作

2. 薅羊毛到BC网站的头上

BC网站的平台充值送彩金，各个不同的平台会有不同的活动，如注册即送188，充值500送300，充1000送500，满足2倍到8倍的流水就可以体现，黑产从业者利用上百套的个人信息注册账号，通过在平台上对刷流水，把一个账户的钱输到另一个账户上面，从而实现薅羊毛的全过程。

1. 利用逻辑漏洞多次重放利用薅羊毛

国内有一些网站，存在逻辑漏洞，部分人组成了FD线报群，通过共享和组织，通过FD以及BP抓包工具，对一些敏感数据包进行数据重放，例如会员折抵卡，通过抓包重放数据，不限次数的使用该卡。

比如某网盘，会员赠送服务，重放数据包数次操作之后，会员时间上升到2999年。

某公司重复某操作，领取积分，通过积分换取某东E卡，各平台VIP会员等。

2. 逻辑支付漏洞套现--一分钱买冰箱

通过逻辑支付漏洞，一分钱或者无需付费购买商城物品套现，虚拟财产，电子物品等等。

国内的跟这个相关的黑色产业链从业者，他们本身没有太强的技术能力，只会逻辑漏洞的三板斧，改参数，负数等等，但就这一个操作，搜索相关的商城网站，也让很多的商家亏损严重。

3. 入侵车管所号牌抽取系统买卖靓号车牌

国内的一些人瞄上了一些可以被变现的渠道，靓号车牌无疑是许多有钱的车主想要的，但是因为预选都看运气，一些不法分子通过寻找相关技术人员，侵入系统通过修改，植入脚本等方式控制选号系统，在联系相关人员下游发展，联系买主进行靓号车牌的选取，然后抽取靓号车牌售卖获利。

4. 入侵全国各地人事考试，建设网，卫生网添加修改数据办假证实施诈骗

该黑色产业链，以上游的技术为主，侵入国内多地的社会资源保障局等网站，在网站数据库添加职业或者技能证书，然后由相关机构和下游从业者进行宣传办理相关证书进行诈骗，而实际上拿到的证书是伪造的，但是受害者在相关网站上进行查询，信息又真实存在，这也让受害者深信不疑。
短短两年时间，该黑色产业链条获利1300万人民币，制作各类虚假证书数以万计。

网络安全创新大会
Cyber Security Innovation Summit

THANKS