基于微信小程序生态体系的黑灰产研究报告

◆ 前言

微信小程序，自 2017 年上线至今，发展迅猛。到 2020 年，微信小程序日活破四亿，MAU 为 8.3 亿，微信小程序的交易规模更是突破 2 万亿，形成了丰富且庞大的商业生态体系。小程序作为一种轻量应用，开发简洁，成本低，迭代快，使用便捷，但安全能力建设却没有及时跟上。因此，基于庞大商业生态的转移，以及相对薄弱的安全防护，使得围绕小程序的黑灰产活动越来越活跃，各种薅羊毛、刷流量的营销欺诈事件层出不穷，企业线上营销活动蒙受巨大损失。

本报告基于永安在线·鬼谷实验室对微信小程序黑灰产的长期监控和研究，从以下几个方面来剖析基于微信小程序生态的黑灰产活动，并提出防护思路，期望以专业、全面的视角帮助企业认知产业、加强防御、避免损失。

媒体合作方：FreeBuf

FreeBuf.COM 是斗象科技旗下国内领先的网络安全行业门户，每日发布专 业的安全资讯、技术剖析，分享国内外安全资源与行业洞见，是深受安全从业者与爱好者关注的网络安全网站与社区。

目 录

一、微信小程序黑灰产活动现状

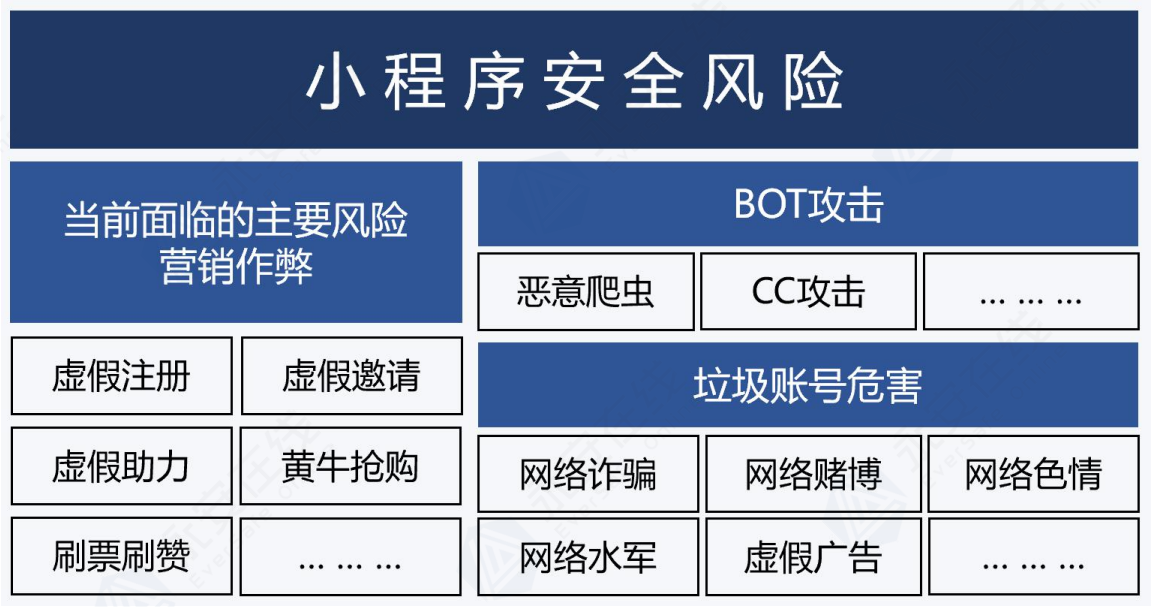
1.1、针对小程序的攻击快速增长，攻击以营销作弊为主

随着微信小程序自身的快速增长，以及依附于小程序的黑灰产业链的成熟，针对小程序的攻击也呈现出快速增长的趋势。基于永安在线业务安全情报平台捕获的黑灰产工具数据，我们统计了从 2020 年 1 月至今小程序自动化攻击工具的数量走势，如下所示：

大量自动化攻击工具的出现，一方面说明小程序给黑灰产带来了足够大的利益，使得专业的黑灰产团伙愿意投入资源和技术；另一方面也说明了目前小程序的安全未能有效阻挡或限制黑灰产，从而导致黑灰产攻击的活跃。

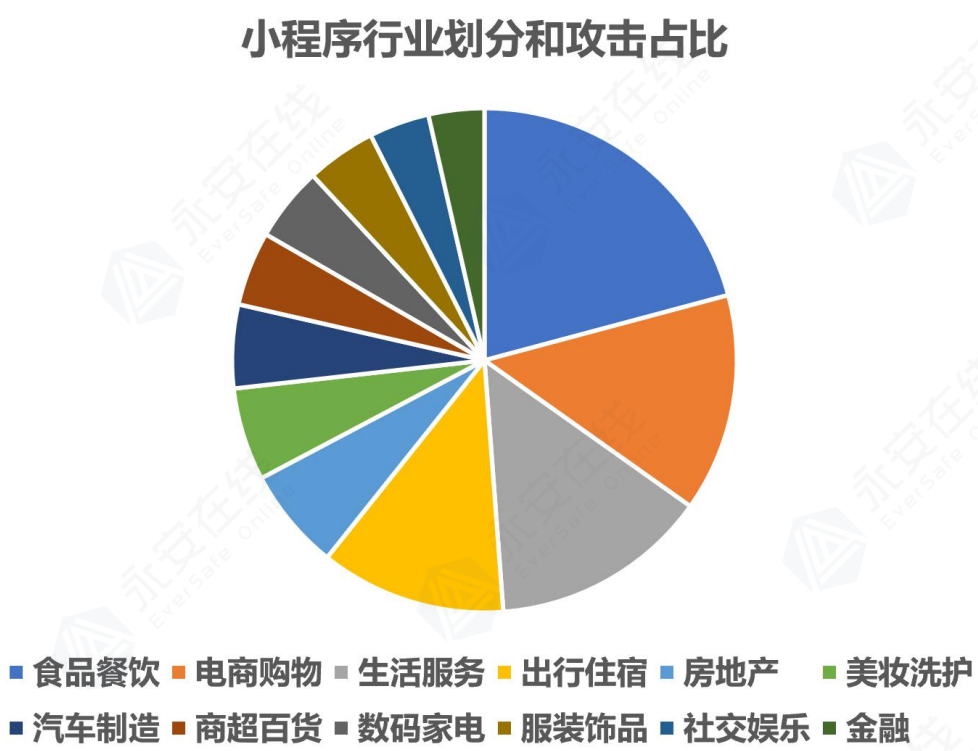
当前的攻击目标以企业在小程序上开展的营销活动为主，通过虚假注册、虚假邀请、黄牛

抢购等方式进行作弊，造成营销费用损失的同时，企业业务也没有得到健康增长。从长远来看，自动化攻击（也称 BOT 攻击）还会带来了更多的安全风险，包括恶意爬取企业数据/用户数据、刷接口、CC 攻击导致服务不可用等，而大量垃圾账号的涌入，对平台的生态也会造成巨大的破坏，包括传播网络色情、网络赌博、网络诈骗等违法行为，网络水军对舆论的操控，发布虚假的广告宣传等。



1.2、传统行业线上业务成为攻击重灾区，攻击遍布各行各业

依托于微信，小程序在便捷性、稳定性、用户触达等方面具备天然的优势，这使得小程序成为了众多传统行业将业务从线下拓展到线上的首选，并发挥出了巨大的作用。另一方面，这些企业相对缺乏黑灰产的了解和攻防对抗的经验，因此在享受小程序带来的红利同时，也成为了黑灰产攻击的重点目标。基于永安在线业务安全情报平台的数据，我们对被攻击的小程序从行业上进行了划分，并统计了攻击占比，如下所示：



可以看到攻击遍布了跟我们生活息息相关的各行各业，我们选择一些行业做简要的盘点。

食品餐饮：“民以食为天”，传统的食品餐饮行业，以酒水、饮料、茶点、零食等为代表，借助小程序从线下拓展到线上，为客户提供更便利更优质的服务，但同时也被黑灰产盯上，成为了被黑灰产攻击最多的行业。针对食品餐饮行业小程序的攻击主要有免单、抢券、秒杀抢购等。

电商购物：电商购物一直是黑灰产攻击的重点行业。除了头部的互联网电商平台，在小程序生态下还涌现出了一些传统企业自建的电商平台，这些平台往往会通过拼团、砍价、积分换购等业务模式来进行社交营销和消费，然而这种业务模式已经被黑灰产熟悉并利用，商家的让利往往被黑灰产攫取了大头。

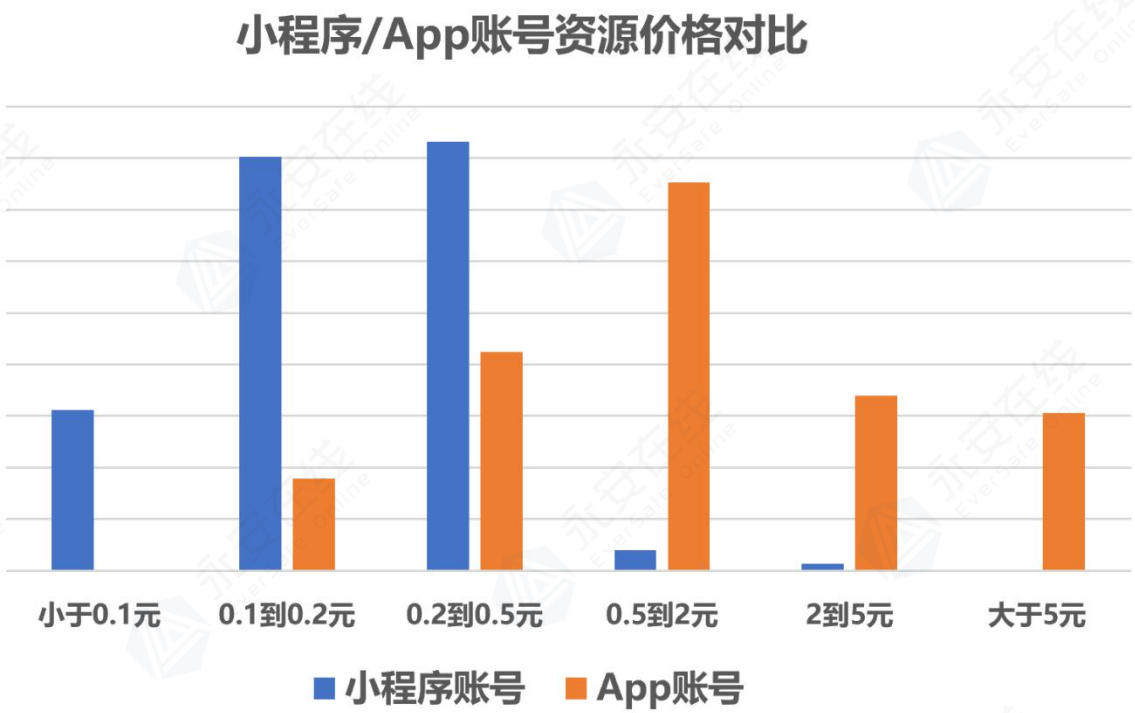
生活服务/出行住宿：互联网服务已经覆盖了我们生活和出行的方方面面，小到外卖、快递、打车、住店，大到婚姻、教育、医疗、养老等。这里面既有大大小小的互联网公司，也有数字化转型的非互企业，还有政府为了提高居民质量或吸引游客而开发的线上服务。在普通民众生活获得便利的同时，黑灰产也从中获取了利益。

房地产/汽车制造：房地产和汽车制造可以说是非常典型的传统行业，在数字化转型的浪潮中，这些企业一方面通过小程序来承载原有的业务，如看房/车、买房/车、租房/车等，另一方面也会通过小程序对业务进行丰富和拓展，如提供业主/车主服务，举行福利活动等。其中福利活动中包含一些线上邀请好友助力的活动，黑灰产可以轻易从中获利。

商超百货/数码家电/服装饰品/美妆洗护：这些行业数字化转型中最大的变化就是将商品买卖从线下的实体店拓展到了线上，其中就包括小程序。大部分企业往往会借鉴电商的营销思路，比如一些国内外知名的运动品牌、化妆品牌等，会在某些时间段（节假日或电商促销日等）推出自己的营销活动，给到用户足够大的优惠。在线下实体店这些优惠给到了真正想要购物的客户，而在线上这些优惠往往落手到了黑灰产手中，比如黄牛党、炒鞋党等。

1.3、小程序攻击成本低，攻击极易规模化

账号资源和设备资源是黑灰产攻击的主要成本。小程序的账号依托于微信授权登录，目前出售的价格，1 个账号仅需 0.1 到 0.5 元；与之对比的是 App 的账号，主要依托于手机接短信验证码，价格普遍要高出不少，一些热门的业务价格则更贵（注：这里仅限于单次授权/接码的价格对比，不包含养号或老号出售）。



黑灰产攻击的规模越大，需要的账号越多，小程序在账号资源上的价格优势就越明显。

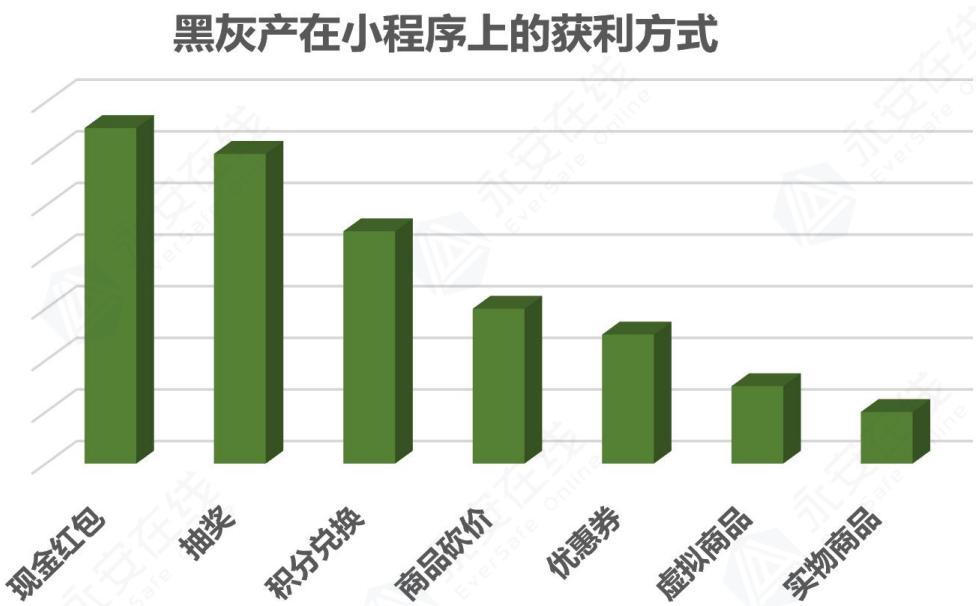
此外，根据永安在线-鬼谷实验室安全专家的分析，目前针对小程序的攻击工具几乎都是协议攻击，而协议攻击不需要手机、群控等设备资源，因此攻击成本大大降低。几种黑灰产实施自动化攻击的常见方式，对比如下：

攻击方式	技术原理	设备需求
协议攻击	破解接口协议，直接伪造接口请求发起攻击	不需要
模拟操控攻击	使用按键精灵、Autojs等编写脚本模拟操控应用界面；对于Web应用，也可以使用Selenium等Web自动化测试框架	需要
注入hook攻击	使用Xposed、Frida等框架，编写插件注入应用并hook关键代码，监听并篡改应用的内部数据或执行流程	需要

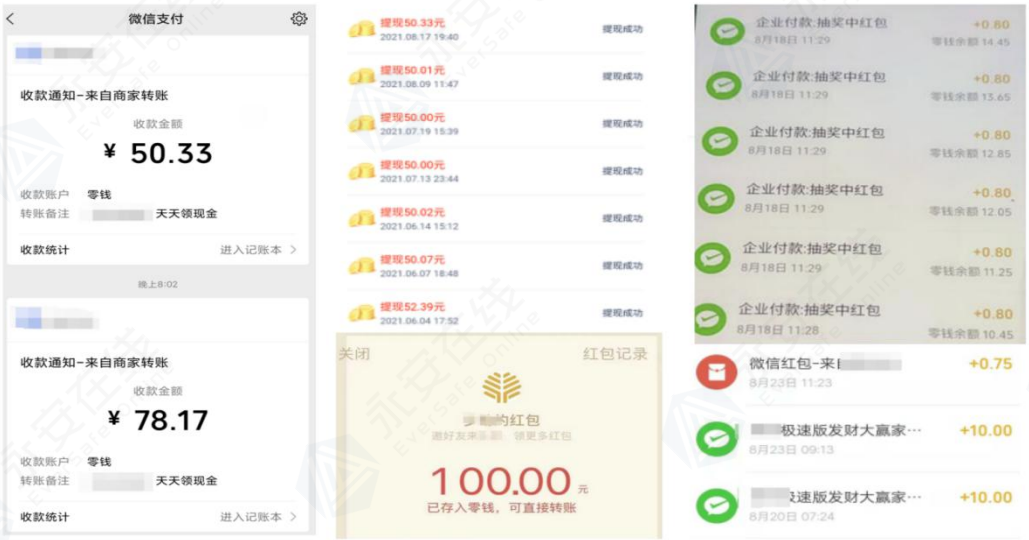
一旦脱离了设备的限制，即使是初级的黑灰产团伙，可以非常轻易的实施规模化的攻击。

1.4、获利方式多种多样，现金红包最受黑灰产青睐

微信好友之间的传播，是小程序最简单也是最好的营销裂变手段。为了刺激用户更多转发和分享自己的小程序，企业会给到用户有足够吸引力的各种奖励方式，而这些往往也成为了黑灰产的获利方式，主要的获利方式有以下这些：



现金红包：微信红包融入了我们的生活，很多企业在小程序上也采用现金红包的形式进行营销获客。由于可以通过微信支付快速变现，因此现金红包成为了黑灰产最为青睐的获利方式，黑产人员也最喜欢用微信提现记录来炫耀自己的“战绩”：



虽然单个账号获取的现金金额往往并不高，但由于攻击小程序可以轻易实现规模化，因此黑灰产获得的总体收益会很高。

抽奖：虽然抽奖是概率事件，但由于黑灰产在“人头”上拥有优势，基本可以保证到稳赚不赔；而且有些抽奖的奖品本身就是现金红包，甚至会有一些高价值的商品，比如iPhone、品牌运动鞋等，这些都会让黑灰产趋之若鹜。

积分：做任务赚取积分，然后积分可以兑换奖励。有些奖励中会有现金红包，或者容易变现的商品，比如充话费，因此也会吸引不少黑灰产。

商品砍价/优惠券：主要来自小程序上的众多电商平台，通过这两种方式来营销自己的商品。黑灰产会重点关注其中的优质或热门商品，以及满减额度高的优惠券和无门槛优惠券。

虚拟/实物商品：常用于营销活动的虚拟商品比较容易出手，比如各大视频网站的会员卡、电商平台的购物卡、线下商品兑换券；实物商品虽然可以通过咸鱼、转转等平台出售，但变现周期长，以及收发囤货的成本，黑灰产会相对谨慎，一般会选择生活必需品（比如纸巾、食用油等）和网红流行物品（比如爆款盲盒、星巴克杯子等）。

1.5、围绕小程序的黑灰产已经形成了一个成熟的产业链

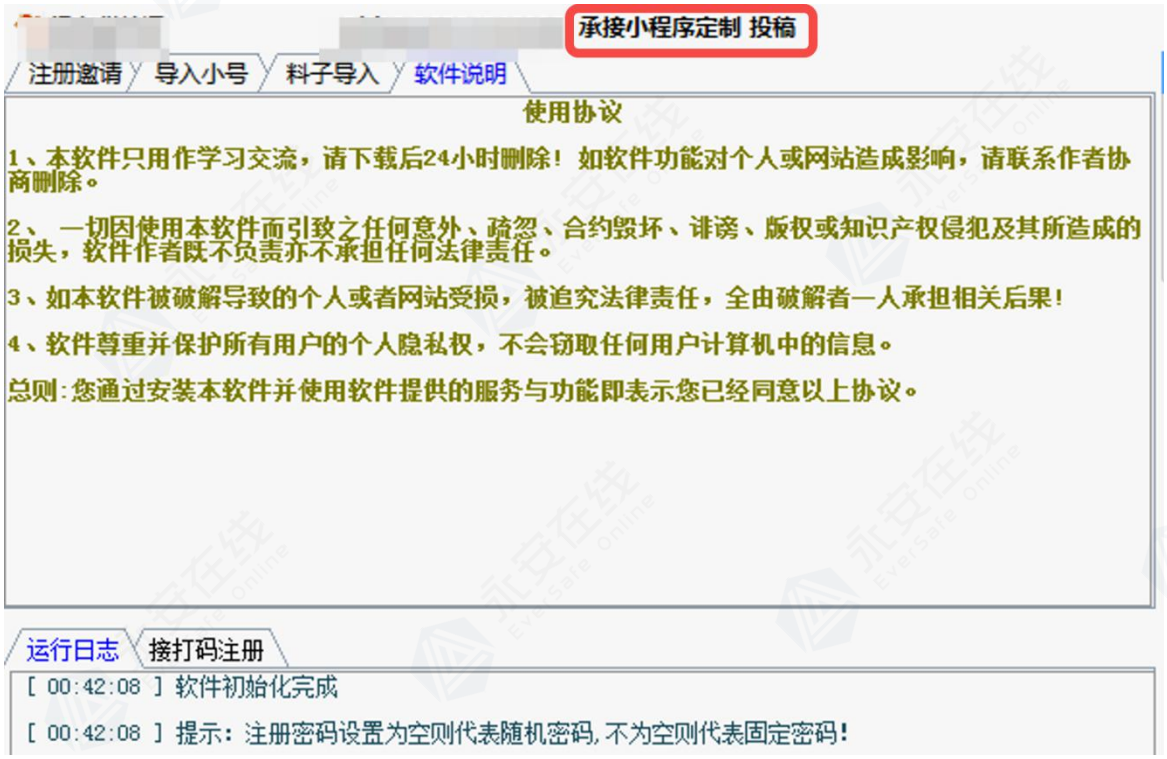
判断一个产业链是否成熟，可以从两方面来评估：1、是否有稳定的从业人群；2、是否形成了稳定的供给关系。而围绕小程序的黑灰产业链条中，账号供应和自动化工具开发是其中比较关键的环节，目前都已经形成了比较稳定的从业人群和供给关系。

账号供应：小程序的账号资源，早期主要通过发卡平台或Q群打广告来出售，触达少，

数量和稳定性也无法保证；而目前已经有了专门提供小程序授权登录的黑灰产：微信授权平台，一方面账号资源得到了充分的保证，另一方面也更好的连接了上下游。根据我们的统计：

- 目前活跃的微信授权平台已经超过 10 家
- 头部平台可用于小程序登录的微信账号超百万
- 大多数平台均支持 API 对接，可快速集成到自动化攻击工具当中

自动化工具开发：越来越多的黑灰产工具作者参与到小程序的攻击工具开发当中，一些工具作者还会在程序界面上打广告，承接小程序攻击工具的定制开发：



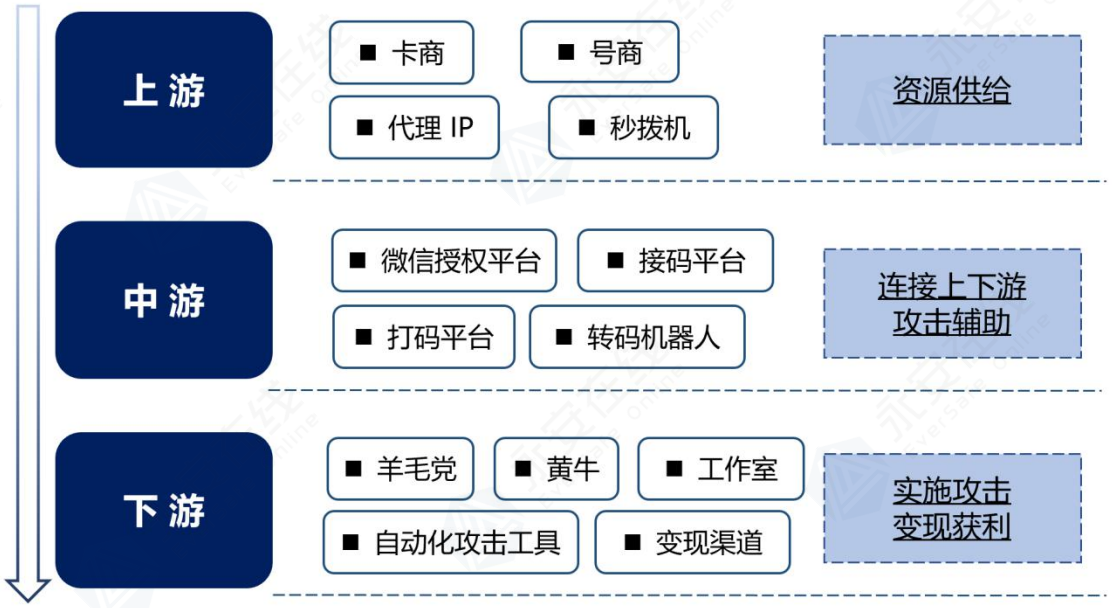
根据我们的统计，过去 1 个月：

- 有超过 **90 个**工具作者发布过针对小程序的攻击工具
- 排名**前 10** 的工具作者发布都超过了 **10 次**
- 排名**第 1** 的工具作者发布了 **57 次**，将近 **2 次/天**

接下来的一个章节我们对产业链做进一步的分析，揭露更多的细节。

二、小程序黑灰产业链分析

围绕小程序的黑灰产业链，按照角色和分工的不同，也可以大致分为上游、中游和下游。上游供给资源，下游实施攻击和变现，中游则连接上游和下游以及为攻击提供辅助。如下所示：



部分角色是小程序黑灰产业链所特有的，我们来重点讲述。

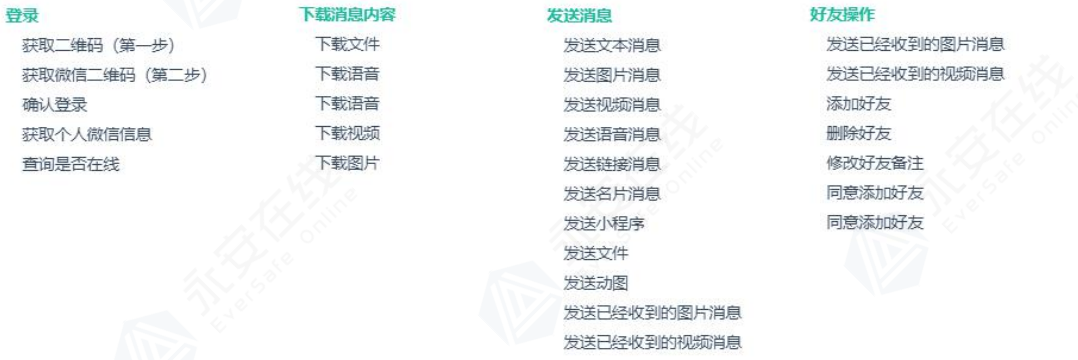
2.1、产业链上游

- **号商**

小程序的登录必须通过微信账号，因此小程序账号资源本质上就是微信账号。黑灰产出售的微信账号主要有 2 类：

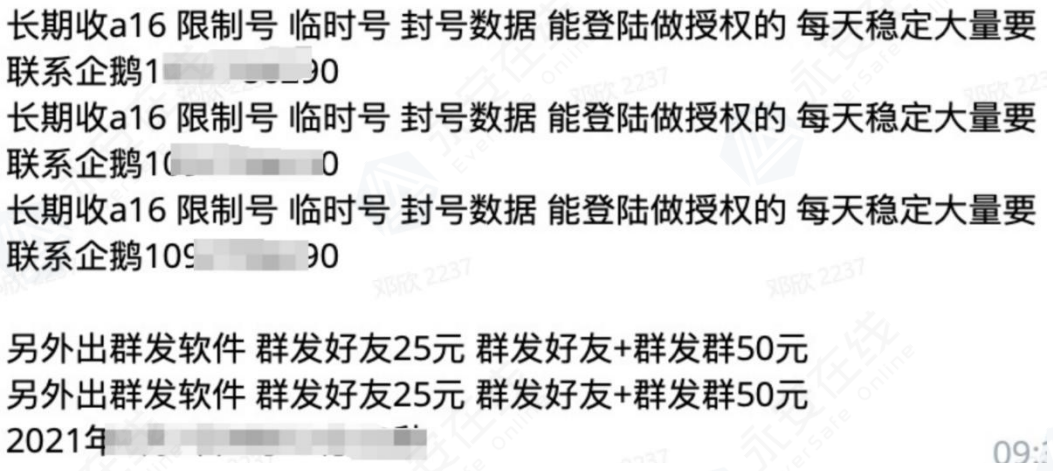
1、**真人账号：**这类账号大多来源于一些经济不宽裕的人群，在经济窘迫时将个人微信号出租或出售。由于是真人使用的账号，因此这类账号流入到黑灰产初期基本不会被微信限制，常被黑产用于一些暴利或非法行为，比如广告引流、网络赌博、网络诈骗等。当然这类账号的出售价格也非常高，1 个账号通常需要上百。

2、机器账号：这类账号主要来源于微信养号工作室。如今黑灰产也与时俱进，出现了专门提供养号服务的平台。养号工作室通过调用平台提供的接口，实现云端养号。比如某云端养号平台就提供了非常丰富的养号接口：



工作室方面只需购买云端平台的服务，无需投入设备，风控对抗也全由云端平台来做。专业的事交给专业的人，分工更加细化。

无论是真人账号还是机器账号，后期由于违法违规行为被微信限制之后，仍然可以用于登录小程序。而黑灰产市面上有大量的被限制的微信账号，出现了专门**收微信 a16 或者 62 数据的号商**，授权登录第 3 方，其中包括小程序、公众号等：



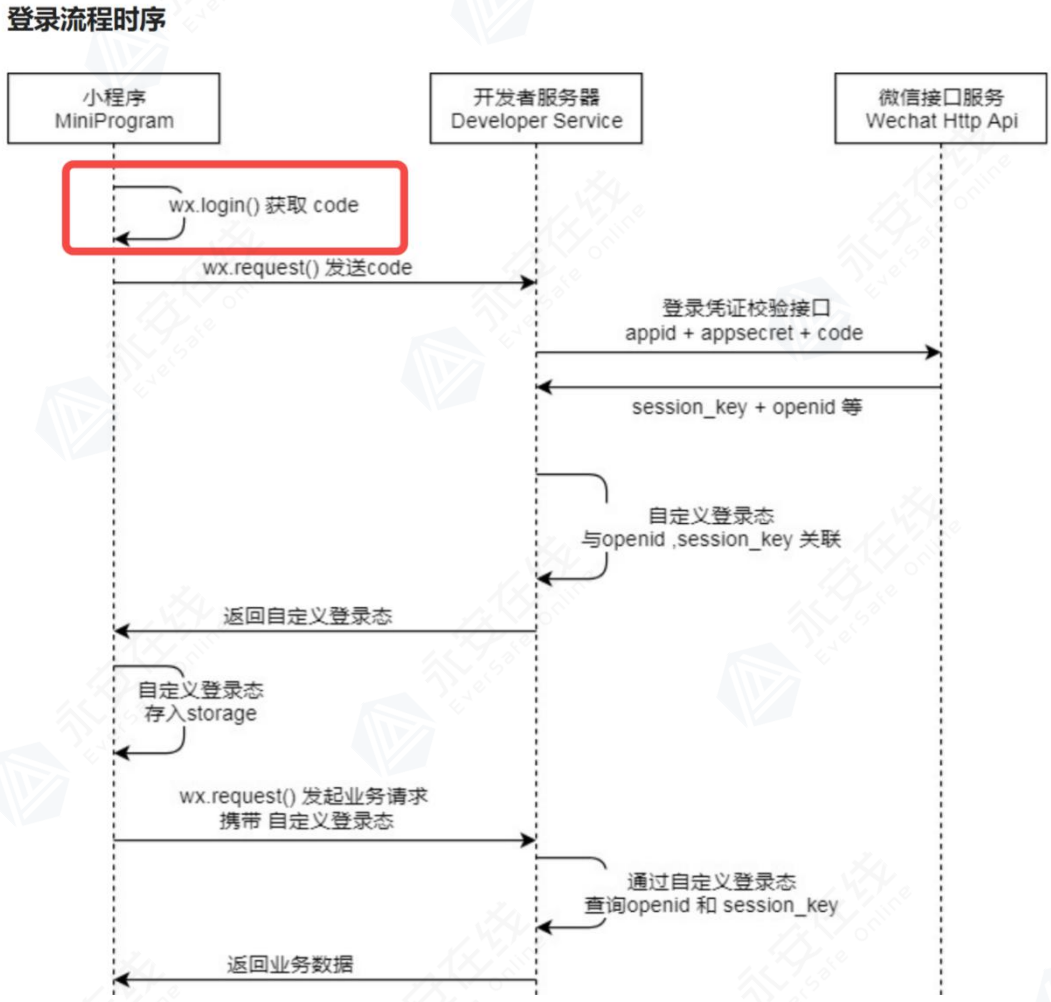
a16、62 数据是微信登陆后产生的身份凭证数据，有了 a16 或者 62 数据就可以实现免账号密码，免验证登陆微信。

2.2、产业链中游

- **微信授权平台**

号商和下游直接对接是低效的，因此出现了连接号商和下游的平台：微信授权平台。

理解微信授权平台，我们首先要清楚微信授权登录的原理。微信官方文档给出了小程序登录的流程：https://developers.weixin.qq.com/miniprogram/dev/framework/open-ability/login.html，流程图如下：



总结起来可以分为 2 步：

1、调用 wx.login() 获取**临时登录凭证 code**，并回传到开发者服务器；

2、开发者服务器拿到 code 后，转而向微信接口服务发起登录请求，微信接口服务返回 session_key、openid 等重要数据给开发者服务器，据此完成登录，并返回自定义登录态。

微信授权平台的作用在于第 1 步，黑灰产可以**通过微信授权平台获取 code**，而无需调用 wx.login() 。一方面针对小程序的攻击完全脱离了小程序的运行环境，另一方面微信授权平台储备了大量的微信账号，可以为攻击提供了大量的账号资源。绝大多数微信授权平台都提供 API 接口，可方便集成到自动化攻击工具中。如下是其中一个平台的 API 接口说明：

接口地址 /prod-api/syste authorizationUser

请求方式 GET

consumes

produces ["*/*"]

接口描述 判断状态码=200 超时- 1跳出循环

miniAuthType	小程序授权类型 1.只返回code 2.code,encryptedData,iv,nick_name,avatarUrl,signature 3.小程序绑定任意手机号，返回code,encryptedData,iv,mobile 默认 1	query	false	string

可以看到除了 code 之外，绑定的手机号、昵称、个性签名等信息，也都可以获取到。目前活跃的微信授权平台已经超过 10 家。这些平台累计支持的 App、小程序数量多达上万个，但凡能给到黑灰产利润空间的 App、小程序等，基本都在支持列表中。

• 转码机器人

转码机器人也是小程序黑灰产的一个特有产物：对于攻击者而言，需要指定受益者，比如攻击助力邀请活动，需要在攻击参数中指定邀请的发起人，这时就需要用到转码机器人。以某品牌汽车制造商的小程序拉新助力活动为例：

1、黑产收益账号登录小程序，将邀请链接发送给转码机器人。

2、转码机器人则可以自动提取出链接信息，主要是打开小程序后跳转的页面以及参数，其中就包含了邀请人的身份信息。

3、部分黑产还会通过真人作弊平台（关于真人作弊平台，可以阅读永安在线之前发布的《真人作弊黑灰产研究报告》：https://zhuanlan.zhihu.com/p/160828150），邀请真人协助作弊。因此转码机器人还会将链接信息转换为一个小程序码，便于微信扫码操作。转码机器人一般是按次收费，也有一些免费的转码机器人，甚至一些黑灰产技术论坛还开源了代码。我们这里简单介绍一下利用微信 PC 客户端实现的转码机器人，原理如下：

1、启动 PC 微信，并注入消息拦截模块到微信进程当中；

2、消息拦截模块 hook 微信接收消息的关键函数；

3、判断接收的消息类型，如果是小程序转发消息，解析并提取出链接信息。

我们发送的文字、图片、表情包、小程序等消息，在消息格式上是一致的：

不同类型的消息，其消息正文会不一样。对于小程序而言，消息正文是一段 XML 格式的文本，其中标签<weappinfo>中包含了相关的信息，如下所示：

```
<weappinfo>
    <pagepath>
    <![CDATA[packageCommunity/pages/copartner/passiveReferredInfo/passiveReferredInfo.html?shareId=7065
    8&activityType=2&clueName=          合伙人&shareVin=LGBH52J          6&shareUnionid=oMiuet_9uAxfau7U8N
    FoeTgb2ZuE&_smwt_ks=16247795348205521 9&_smwt_kn=1&_smwt_kr=16247795348205521 9]]></pagepath>
    <username>gh_e574c29a84d2@app</username>
    <appid>wxe3fd49854884240e</appid>
    <version>111</version>
    <type>2</type>
    <weappiconurl>
    <![CDATA[http://wx.qlogo.cn/mmhead/Q3auHgzwzN                                    51r4Ptib7KDg/96]]>
    </weappiconurl>
    <weapppagethumbrawurl>
    <![CDATA[https:/                    /resources        wxmp-site/images/packageCommunity/asst
    es/images/recommend_main_pic.png]]></weapppagethumbrawurl>
    <shareId><![CDATA[1_wxe3fd49                                  5fa6cf27f31ae_1626309630_0]]></shareId>
    <appservicetype>0</appservicetype>
    <secflagforsinglepagemode>0</secflagforsinglepagemode>
    <videopageinfo>
        <thumbwidth>720</thumbwidth>
        <thumbheight>576</thumbheight>
        <appthumburl><![CDATA[(null)]]></appthumburl>
        <fromopensdk>0</fromopensdk>
    </videopageinfo>
</weappinfo>
```

2.3、产业链下游

- **破解小程序**

下游是攻击的直接发起者，而对于专业的黑灰产而言，会开发工具实施自动化攻击，以获取更大的利益。其中第一步是破解小程序，搞清楚小程序的业务逻辑和核心算法。

破解步骤如下：

1、提取小程序包：手机微信的小程序包位于：

/data/data/com.tencent.mm/MicroMsg/{{用户哈希值}}/appbrand/pkg 目录下，后缀

为.wxapkg 的文件；PC 微信的小程序包则位于：{{我的文档}}\WeChat Files\Applet\{{小程序 AppID}}\{{小程序版本}}目录下，名为__APP__.wxapkg 的文件；

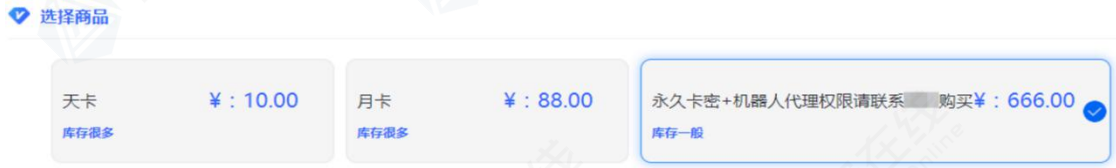
2、解包小程序包：小程序包的文件结构已经被研究清楚并公开，网上也有公开的开源项目和工具，可以从小程序包中解出源代码文件；

2、分析代码：将源代码导入到微信开发者工具，方便阅读和调试，同时结合动态抓包定位并分析关键代码，比如业务接口请求的构造。

- **开发工具**

完成小程序的破解后，工具开发者通常先手动测试完成攻击流程，然后再编写工具代码实现自动化操作。开发者会在工具中接入多个微信授权平台的 API 接口，同时也会接入接码平台、打码平台、代理 IP 平台的 API 接口。这些都是可以复用的，对于不同的小程序，工具开发者需要修改的代码并不多，因此开发一款新的小程序攻击工具对于他们来说成本并不高。

工具开发完成后，开发者会通过一些渠道将其出售给实施攻击的人。部分工具是公开出售的，通常会使用 QQ 群来保持联系和交流，包括使用教程、工具更新通知、下载和购买地址等。其中购买地址一般会指向某个发卡平台的店铺，开发者通过出售卡密的方式来获取收益，而卡密则根据工具的使用时长来定价：



有些工具开发者会通过发展代理的方式，来获取更多的使用者从而扩大其收益；有些工具开发者自己也会发起攻击，为了降低风险，他们会在一段时间之后将工具免费提供出来，借此达到“法不责众”的效果。

三、小程序攻击案例分析

了解了产业链之后，我们选取几个典型的案例，让大家对于小程序的黑灰产攻击有一个更加直观和现实的感受。

3.1、某金融服务平台一元购活动被攻击

某头部金融服务平台的小程序在 8 月 20 日-8 月 27 日推出了“邀好友，千元好物一元购”的活动，可以邀请好友给自己助力砍价，商品价格最多可以砍到一元，这对于黑灰产来说具备了足够的吸引力。在 20 日早上 7 点多，也就是活动开始后 7 个多小时，就有工具作者完成了自动化攻击工具的开发，攻击成功之后，也有黑灰产对收益进行炫耀：

邀请好友助力砍价可以通过小程序的分享转发快速实现用户裂变，因此是小程序上最为常用的营销获客方式之一，同时也是一个非常典型的小程序攻击场景。我们以其中一款工具为例，来看看黑产是如何实施自动化攻击的。首先从工具界面导入需要助力的邀请人列

表：

然后通过微信授权平台获取助力账号 code，授权登录小程序：

```
aWechat_6       db ']WeChat授权获取失败|未获取到授权',0
aWechat_5       db 'WeChat授权获取失败|未获取到授权',0
aHttpsGugujiZgp db 'https://          com.cn/usr/getToken',0
aCode_0         db '{"code":"',0
aHostGugujiZgpa db 'Host:                    ',0Dh,0Ah
                db 'Connection: keep-alive',0Dh,0Ah
                db 'Content-Length: 43',0Dh,0Ah
                db 'User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.3'
                db '6 (KHTML, like Gecko) Chrome/53.0.2785.143 Safari/537.36 MicroMes'
                db 'senger/7.0.9.501 NetType/WIFI MiniProgramEnv/Windows WindowsWecha'
                db 't',0Dh,0Ah
                db 'content-type: application/json',0Dh,0Ah
                db 'Referer: https://servicewechat.com/wx          5b3b/121/page-fr'
                db 'ame.html',0
                db ']登录成功|正在助力',0
                db '登录成功|正在助力',0
                db ']登录失败|失败原因：',0
```

登录接口

传入从授权平台获取的code

伪造请求头

登录成功后，攻击助力接口，完成对黑产邀请者账号的助力：

```
aHttpsGugujiZgp_3 db 'https://          .com.cn/groupGamePrizeCutRecord/cut',0
aRecordid         db 'RecordId=',0
asc_9B459B        db '&',0                ; DATA XREF: sub_49055D+139↑o
                                          ; sub_4A245C+38↑o ...
aShareusrid       db 'shareUsrId=',0
aShareusrid_0     db ', shareUsrId : ',0
aGroupgameprize   db '{"groupGamePrizeRecordId":',0
aDataMsg          db 'data.msg',0
aDataResult       db 'data.result',0
aTrue             db 'true',0             ; DATA XREF: sub_48C9AD+22E↑o
                                          ; sub_48C9AD+2F8↑o ...
aDataGroupgamep   db 'data.groupGamePrizeCutRecord.cutPrice',0
                  db ']登录成功|助力成功|',0
                  db '登录成功|助力成功|',0
                  db ']登录成功|助力失败|失败原因：',0
                  db '登录成功|助力失败|',0
```

助力接口

传入邀请者ID

根据返回结果判断是否助力成功

3.2、某生活服务平台现金活动被攻击

某生活服务平台为了吸引用户推出的现金活动，每周 1 个活动周期，在 1 个活动周期内，1 个账号可以通过签到、邀请好友、下单等方式赚取现金，满 50 可提现。前面提到现金活动可以通过微信支付快速变现，是黑灰产最为青睐的获利方式，这个活动也不例外：

虽然每次赚取的现金并不多，但对于黑灰产来说，可以通过微信授权平台获取大量账号，并配合自动化工具实施批量攻击，最终的整体收益会非常可观。

3.3、某品牌茶饮厂商抢购活动被攻击

这是小程序上的一个限时抢购活动，推的是买 1 送 1 优惠，可以用 1 张卡券的价格购买 2 张卡券。由于该茶饮的卡券非常容易出手变现，因此被黑产盯上，活动期间出现了大量的羊毛党交易信息：

@全体成员　　昨天买的[redacted]32+29　　51回收　　[redacted]礼品卡13/20的73折回收

[redacted]　　发布渠道：玩卡撸羊毛2群小神　Q群　发布人：[redacted]

[redacted]不好意思哈，确认有点慢。第二期价格崩了，还是按50回，别催别急，我也一直在催别人多的也知道我很稳[emoji=F09F9882][PicUrl:http://gchat.qpic.cn/gchatpic_new/1/1-1-61

[redacted]　　发布渠道：小肥羊线报群　Q群　发布人：[redacted]

48收1000套[redacted]

[redacted]　　发布渠道：全网最大群友聚集地　Q群　发布人：[redacted]

50出一套[redacted]

[redacted]　　发布渠道：抢购线报VIP交流群　Q群　发布人：[redacted]

[redacted]全部结账了，今天出了点意外卡了点壳，还好最后全部都处理完了，最后感谢大家的支持

[redacted]　　发布渠道：游戏项目群　Q群　发布人：[redacted]

同时也出现了自动化的攻击工具，活动开始之前在工具界面上设置好攻击的时间、次数以及延迟：

等活动时间一到，自动触发访问抢购接口：

四、小程序攻防难点和防护思路

4.1、小程序的攻防难点

随着小程序的攻击案例越来越多，小程序安全已经逐渐引起业务方和安全行业的重视。相比于 App 和 Web 应用，小程序带来了一个新的攻防平面，**其难点在于：已有的一些防护方案不能有效的运用到小程序上，导致达不到理想的防护效果，例如以下方案：**

- **设备指纹**

设备信息是业务安全风控的重要输入参数。设备指纹能否取得比较好的效果，取决于采集的信息是否可以形成该设备的唯一 ID，以及可以判断该设备是否存在风险。出于权限和

隐私等安全方面的考虑，小程序可以采集到的设备信息并不多，能采集到设备信息，比如品牌型号、屏幕大小、分辨率、电量、网络类型等，无法形成唯一性强稳定性好的设备ID，也无法借助这些信息来判断设备是否存在风险。

同时，由于目前黑灰产攻击小程序基本采用的都是协议攻击，黑灰产可以在发起的业务请求中随意伪造设备信息，这使得设备指纹在小程序防护上的效果微乎其微。

- **安全扫描**

通过人工或自动化的方式对小程序前端和后端进行扫描，检查是否存在 SQL 注入、XSS 跨站脚本、目录遍历、信息泄露等应用漏洞。然而当前黑灰产针对小程序的攻击，几乎都不是通过应用漏洞进行攻击。黑灰产伪造业务请求发起的自动化攻击，其产生的机器流量，没有携带任何漏洞特征或恶意代码，和正常的请求并无差异。

安全扫描可以提早发现小程序中的漏洞，避免遭受漏洞攻击；但对于非漏洞的攻击，则起不到任何防护作用。

- **安全加固**

安全加固指的是对小程序的前端代码进行一系列的混淆和变换，在执行逻辑不变的前提下，降低其可读性，提高攻击者分析前端代码逻辑的难度，从而保护小程序的安全。常见的变换手段有：字符串加密、变量名混淆、插入垃圾代码、调用等价变换、控制流平坦化等。

安全加固确实可以在一定程度上提高攻击门槛，劝退菜鸟级黑灰产，但仍然难不倒技术实力强的黑灰产。而且小程序主体的代码逻辑基本上不会发生大的变化，所以破解是一次性的，只要收益足够大，破解所需要的时间成本对于黑灰产来说是可以接受的。

此外，安全加固必然会带来一定程度上的性能损失和稳定性下降，也不方便调试，因此目前并没有被广泛使用。我们随机选择了 30 款小程序作为分析目标，对这些小程序进行反编译后，发现没有 1 款小程序对代码做了混淆加固，情况不容乐观。

- **接口保护**

对于重要业务接口的访问进行签名校验，是抵御机器流量的有效手段之一。最常见的方法是在接口请求参数或者请求头中携带一个签名 signature（或者叫令牌 token），签名在小程序前端由具备一定强度的算法生成，小程序后端根据对应的算法校验签名的合法性，若校验失败则拒绝响应本次请求。对于小程序主要面临的协议攻击来说，确实可以提高攻击门槛。**但问题在于攻防的不对等。**

由于小程序代码无法实时更新，签名算法一旦被破解，需要等到小版本发布新的版本才能升级新的签名算法。发布新版本很多时间需要服从产品计划，而且需要经过完整的测试，这往往会给黑灰产留下足够的攻击时间，防护效果大大折扣。

由于已有的这些防护方案，防护效果都比较有限，因此我们需要考虑小程序自身的特性，结合黑灰产攻击情报和案例的分析，量身打造适用于小程序的安全防护。

4.2、小程序的防护思路

- **重视情报的价值**

“未知攻，焉知防”，无论哪种产品形态，情报对于安全攻防来说都是非常重要的。通过情报可以第一时间感知到是否存在针对己方小程序的攻击以及攻击规模，并从情报中提取出黑灰产所使用的技术和攻击逻辑，进行针对性的反制。

这里举一个实际的案例：去年某个出行企业在小程序上，以过关游戏的方式拉动用户，并给予通关者较高的现金奖励。正常情况下玩家在规定时间内无法通关，需要依靠邀请好友来延长游戏时间。然而分析从永安在线业务情报平台捕获的攻击工具得知，黑产只需伪造通关成功的接口请求，可以跳过游戏关卡直接拿到现金奖励。根据这条情报，业务侧很快进行了修复，从而避免了进一步的损失。

- **设计合理的规则**

合理的规则，一方面需要对正常用户有足够的吸引力，确保业务正常开展；另一方面则需要提高黑灰产的攻击成本，或者降低其收益。这里提供一些规则设计上的建议，供大家参考。

①现金红包：

不建议秒提现，给审查留下时间；

②优惠券：

如果平台上有一些低额易变现的商品（比如 10 元充话费），不建议无门槛优惠券；

③抽奖：

对于一些可能有问题的账号（比如 IP 地址来源于 IDC 机房，缺乏埋点行为的上报等），降低其中奖概率。

④助力邀请/砍价：

这是最具小程序特色的营销方式。由于往往需要邀请多个人，黑灰产在攻击时会使用代理 IP 来规避 IP 地址单一的问题。不过无论是基站 IP 还是 ADSL 拨号 IP，都存在好人和坏人混用的情况，从而产生一定比例的误报。超过多少人都命中风险 IP 才进行判定，可以大

幅度降低误报率。

比如助力需要邀请 5 个人，只有 1 个人命中风险 IP 时，误报率为 1%；而 2 个人同时命中风险 IP，误报率则降低为 0.01%，而 5 个人同时命中风险 IP，误报率直接可以忽略不计。可以结合实际情况来设置人数的阈值。

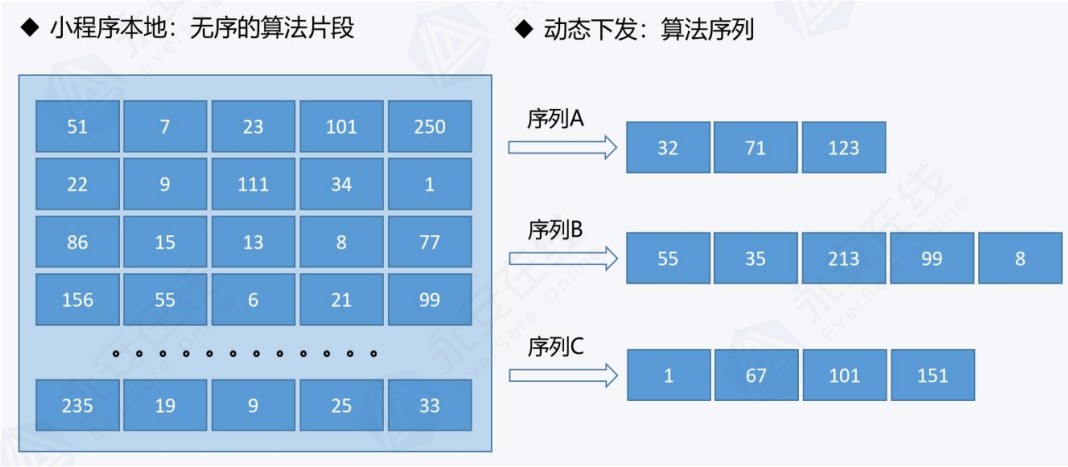
- **基于小程序的动态防护**

动态防护的思路在 App 和 Web 应用上已经得到了广泛的运用，其核心思路是：跟黑灰产攻防对抗比较激烈的攻击面，比如接口保护的签名算法，其代码不是固定的，而是动态变化的，这样黑产很难找到攻击锚点，无法实施稳定的攻击。

对于小程序而言，这个方案的难点在于小程序的代码只能在小程序发布新版时才能更新，无法动态下发，理论上只能执行固定的代码。不过我们可以转换一下思路，以签名算法为例：

一个算法 = 若干个算法片段 + 固定的执行序列

我们将所有签名算法的算法片段无序的放在小程序前端的代码文件中，然后在后端动态下发执行序列，如下所示：



如果有 100 套算法，对应的就是 100 个执行序列，每次随机下发其中 1 个执行序列，从而达到动态签名的效果。不过由于所有的算法片段都暴露在本地，即使做了乱序和混淆加密，时间长了难以保证不被破解，因此仍然需要跟黑灰产保持住攻防对抗。而借助情报可以有效感知到黑灰产是否绕过了防护，从而针对性的对算法进行升级。

这个也是我们目前主推的小程序防护方案。

• 写在最后

没有一个技术方案可以一劳永逸的解决某类安全问题，小程序安全也是如此，需要有更多的人参与进来，大家集思广益，加强交流与合作，共建安全。我们发布这篇报告，也是希望抛砖引玉，能引起行业更多的思考和探讨，护航小程序生态的健康发展。