



永安在线
EverSafe Online

· 业务安全情报专家

2020年 黑灰产攻防研究 年度总结报告

出品方：永安在线业务安全情报团队



A N N U A L S U M M A R Y R E P O R T

摘要

进入21世纪，智能手机的普及开始把曾经存在于PC上的媒介、市场逐渐招揽到移动端来。很快，互联网承载的业务场景因为移动属性呈现出爆发式增长，商业模式上个人付费能力及意愿也在快速增强，越来越多的人愿意享受内容付费带来的服务，如，开通VIP会员，购买线上课程等等。这时互联网产生的连接已经不再只是内容和设备的连接，而是场景和个体的连接。

互联网的核心资源也从设备变成了个体，存在于互联网中的每一个网民就是新互联网时代的争夺对象。与此同时，黑灰产也逐渐向移动互联网的场景转移。

基于这一认知，永安在线对移动互联网端内黑灰产的攻防进行了很长一段时间积累。近期，我们将2020全年的案例积累进行了总结分析，凝汇成了此份报告。我们期望这些经验分享，能为企业、机构和从业者在未来互联网的业务安全建设上提供前瞻性的参考，助力企业夯实业务安全底座。

本报告的主要内容如下：

第一部分，我们将围绕企业的核心风险场景，介绍业务安全情报在企业安全中的重要性和价值体现，并展示永安在线相对应的解决方案；

第二部分，我们将介绍黑灰产这条产业链的宏观和微观层面的演变趋势，从攻击方式、攻击渠道、人群画像等维度进行案例式解析；

第三、四部分，则主要分享攻防技术的迭代和黑产工具、案例，并给出相应的攻防建议。

目录

摘要	1
一、永安在线业务安全情报能力	3
1. 业务安全情报平台	3
2. 风控基础数据标签	4
3. 业务安全服务	5
4. Karma业务情报搜索引擎	5
二、黑灰产攻击的演变趋势	6
1. 商业模式转变带来黑灰产核心资源变化	6
2. 虚假账号的生产和流转呈规模化趋势	7
3. 作恶方式从自动化工具向真人众包演变	15
4. 真人作弊深度剖析	22
三、攻防技术的迭代	34
1. 黑产群控进化史	34
2. 黑产IP资源进化史	42
3. 秒拨IP识别技术案例分析	50
4. 新工具“IP魔盒”案例分析	55
5. 定制ROM改机案例分析	58
6. 黑产攻击流程自动化体系	62
四、黑产工具情报分析	86
1. 工具样本的快速分析和有效性验证	86
2. 工具分析及案例	92
2.1 恶意爬虫工具	92
2.2 抢券工具	99
2.3 注册机工具	108

一、永安在线业务安全情报能力

永安在线基于业务安全情报的三大产品服务线：

1. 业务安全情报平台

帮助企业监控、预警和发现未知风险



业务安全情报平台围绕企业的核心风险场景：账号安全、营销活动薅羊毛、私信/动态恶意引流、刷量作弊、真人众包等业务问题。分析每个风险场景黑产的产业链结构、团伙特征，各级黑产人员传递消息、黑产物料及黑产服务的渠道和方式方法。最终将网络黑产按照产业链的供给结构分为资源、服务、变现三类群体，分别针对不同阶段的黑灰产进行，进行情报渠道挖掘和监控。



搭建对业务场景与黑产攻击链路全景式覆盖的风险情报平台，通过为黑产线报监控、黑产工具监控、黑产成本监控和数据资产安全四大情报板块为企业业务安全赋能。



2. 风控基础数据标签

帮助企业建立对黑灰产的三大基础资源的风险情报库,风险识别准确率高达99.5%，可直接用于业务判定；风险召回率高达60%，极大的帮助客户减少风险与损失。

- 1) 风险手机号识别——识别手机号是否是黑灰产团伙所持有的虚假手机号或是被黑产所劫持的真人号码
- 2) 动态风险IP识别——实时识别代理、秒拨、混拨、代理秒拨等动态的风险IP
- 3) 风险设备环境——识别群控、云控、箱控、云手机、模拟器、多开分身、Root越狱、设备调试、虚拟定位、挂机行为等30多种风险设备环境

3. 业务安全服务

帮助企业落地情报的应用与监测

- 1) 黑灰产调研服务
- 2) 黑灰产工具分析
- 3) 业务安全蓝军

4. Karma业务情报搜索引擎

永安在线推出的业内首个业务情报搜索引擎



关于这款业务情报搜索引擎，我们将始终围绕着三大能力为客户提供价值——

业务情报调查和分析能力：可以通过Karma业务情报搜索引擎发现并分析最新黑灰产工具、查询手机号风险画像、IP风险画像等等。未来Karma还将围绕搜索，连接更多风险场景和情报数据，并借助AI机器学习提供更深入的分析能力，持续帮客户提高查询覆盖率和分析效率。

业务风险感知能力：现在Karma已经提供了一些基础的情报预警能力，比如发现攻击您业务的黑产工具、监测到暗网的数据交易及黑产变现交易价格波动等。一方面我们会继续拓展预警能覆盖的场景，另一方面我们会在后续提供更多的风险感知能力，很多迭代中的功能都可能是业内第一家做的，敬请期待。

业务情报数据API能力：API作为产品的扩展，包括手机号画像API，IP画像API，情报监控API。手机号画像和IP画像可以在Karma发现风险后给客户提供识别/拦截的落地能力；而情报监控API可以方便自建情报分析系统的客户灵活接入外部能力。

二、黑灰产攻击的演变趋势

1. 商业模式转变带来黑灰产核心资源变化

黑灰产这条产业链伴随国内互联网发展二十余载，早些年，黑灰产就开始控制个人电脑做为肉鸡来进行Ddos、刷广告、安装流氓软件等变现。一台台实际的物理电脑就是黑灰产的核心资源，谁控制的越多，谁就赚的越多。

这个时代下的互联网黑灰产之所以是这种逻辑，也是因为互联网早期的商业模式非常集中在线上广告，在PC互联网时代这种线上广告的结算逻辑是以电脑设备为单位，各个互联网厂商也是以安装量、激活量及活跃量等来构建自己核心商业逻辑。

彼时，设备数量不只是当时互联网黑灰产的核心资源，同时也是当时整个互联网的核心资源。

进入21世纪，智能手机的普及开始把曾经存在于PC上的媒介、市场逐渐招揽到移动端来。很快，互联网承载的业务场景因为移动属性呈现出爆发式增长，商业模式上个人付费能力及意愿也在快速增强，越来越多的人愿意享受内容付费带来的服务，如，开通VIP会员，购买线上课程等等。这时互联网产生的连接已经不再只是内容和设备的连接，而是场景和个体的连接。

互联网的核心资源也从设备变成了个体，存在于互联网中的每一个网民就是新互联网时代的争夺对象。与此同时，黑灰产也逐渐向移动互联网的场景转移。

2. 虚假账号的生产和流转呈规模化趋势

基于互联网核心资源的变化，我们观察到，互联网黑灰产从之前的通过色情流量下发木马到用户电脑，取得电脑控制权后变现的模式，变成了通过大量手机号在各个互联网核心业务场景注册恶意账号，并通过这些账号在业务场景中变现的方式。

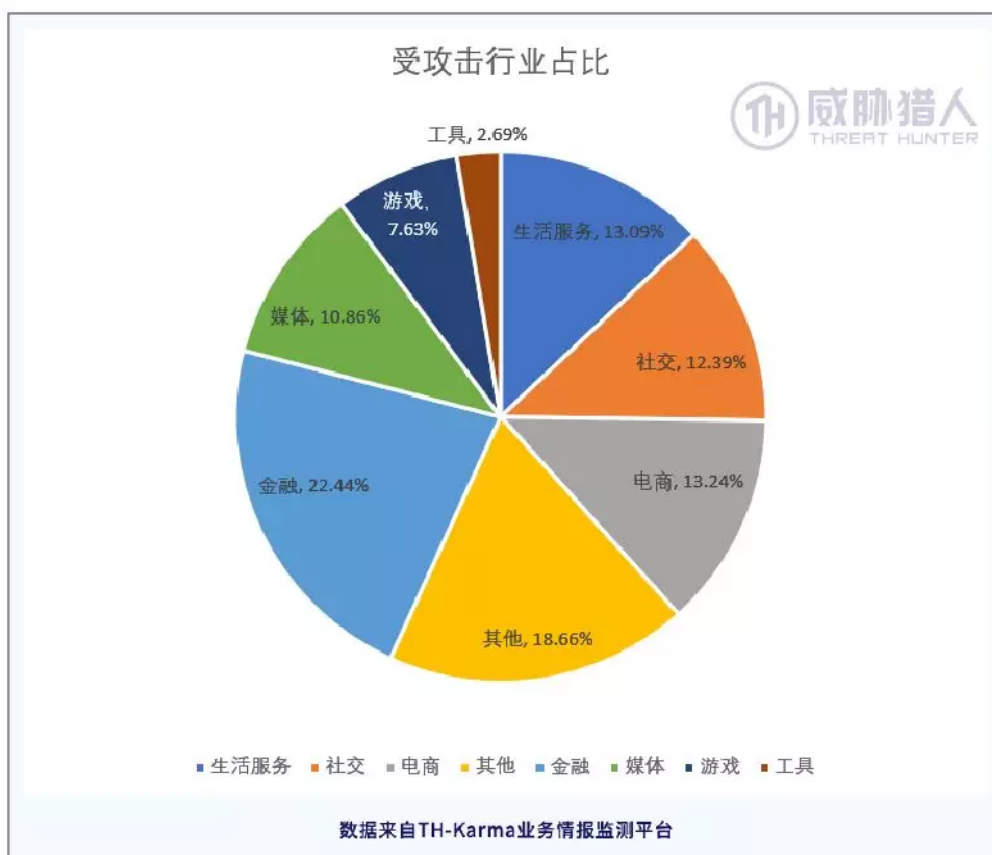
恶意注册是业务风险的起点，也是企业风控的核心关键点。当今黑产以恶意注册为代表的各类攻击资源已经高度的模块化和市场化，产业链不同层级的团伙专注于不同的任务而又配合严密。而究其根本，是强自动化使得攻击变得可复制，进而形成套路化的盈利模式，对企业资产造成威胁。如果企业无法及时发现问题，采取有效对抗策略，将在业务上面临巨大损失。

2.1 以恶意注册为核心资源的黑灰产作恶场景

随着商业模式的变化，电商平台薅羊毛、直播平台刷量、社交平台刷粉、网络诈骗等各种以虚假账号为核心资源的黑灰产攻击开始涌现。

以直播平台刷量为例，通过刷量可以帮助主播上各种排行榜；给主播购买僵尸粉，可以增加主播的粉丝数；在主播的直播间购买水军，可以增加直播间人气等等。一方面，这些数据可以直接在平台折现成现金奖励，由此获利；另一方面，伪造人气可以吸引更多的粉丝，进而通过粉丝打赏获利。

根据永安在线鬼谷实验室统计，全网恶意注册发起的攻击每日就可达8327380次。这背后涉及到的黑卡资源，平均每日活跃量可达1389107张，平均每张黑卡每日进行6次攻击。其中，受恶意注册影响最严重的行业有金融、电商、媒体、社交和生活服务。可以明显发现，恶意注册攻击的目标一般具有高盈利性质或是高流量性质，可见下游的变现需求是驱动恶意注册进行的根本。



图为：受恶意注册攻击行业占比

每张黑卡的重复使用率都非常高，因为在中国国情下的黑灰产攻击具有明显的流动性，即同一行业往往面临共通的黑灰产攻击，攻击门槛更低、防护较弱的企业产品更容易吸引攻击。当某厂商攻击难度提高后，相关人员会迅速的转向同类别的其他厂商。各大企业在解决问题上的思路与措施有一定的相似性，也造成了黑产绕过方式与攻击工具的可复制性非常高。

在这样的情况下，如果企业不了解的黑灰产的攻击手段，无法识别其掌握的大量虚假账号，就不能结合企业自身情况制定最低成本与最低损害正常业务的策略进行防守。

2.2 恶意注册规模化的背后是效率平台的发展

当今黑产以恶意账号为代表的各类攻击资源已经高度的模块化和市场化，产业链不同层级的团伙专注于不同的任务而又配合严密，而究其根本，是强自动化使得攻击变得可复制，进而形成套路化的盈利模式，对企业资产造成威胁。

根据永安在线鬼谷实验室的研究分析发现，恶意注册所得账号为消耗型商品，各厂商通过各式安全策略处理作恶账号的同时，新生的恶意注册账号会不断填充被处理作恶账号缺失的部分。虽然有些账号在封禁后，可以通过发送短信、接收语音验证码等方式对账号进行解封，但实际解封率极低，原因有两点：

- 一是黑产解封一个账号花费的时间远长于注册账号所需的时间；
- 二是在很多场景下，黑灰产在账号封禁前已经完成了变现，此时解封一个封禁账号的价格成本远高于注册一个新账号。

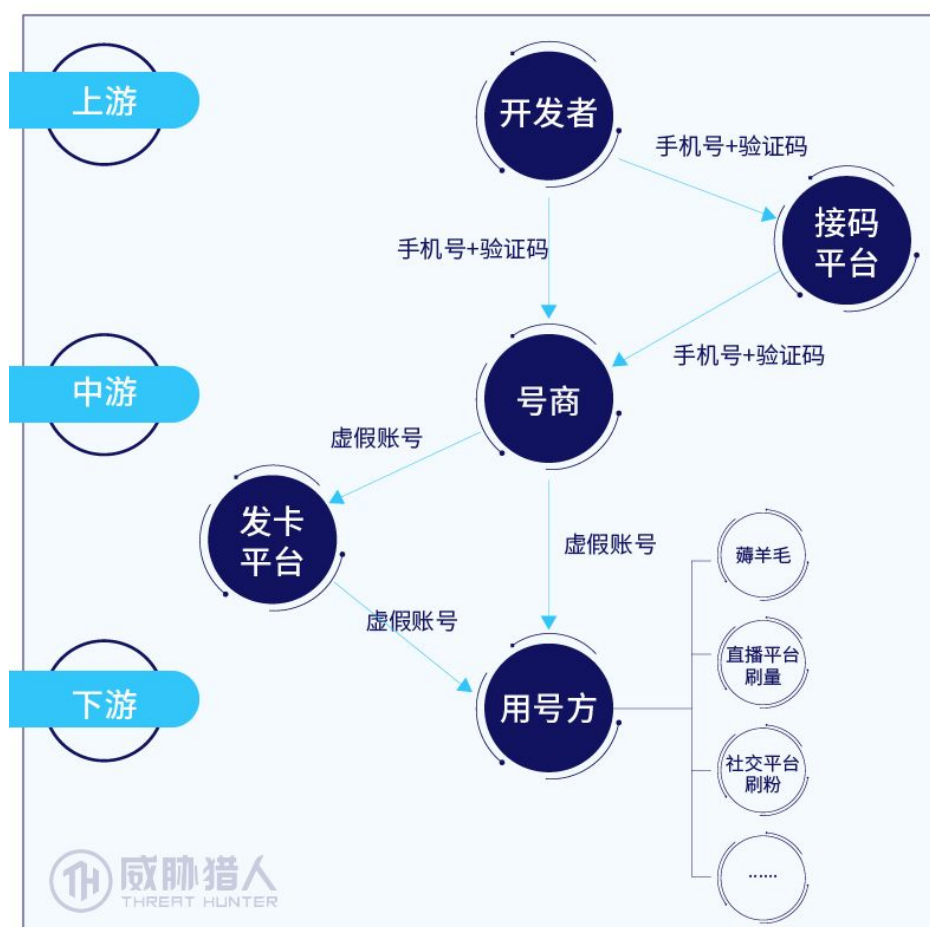
如下图，是同一时期内，新生恶意注册账号和二次解封账号的比例：



图为：恶意注册账号新生量与解封量对比

可以看出，在同一时期内，恶意账号的新注册量远远大于解封量。于是，在整个大批量恶意注册的过程中，如何提升整个运作过程的效率和降低恶意注册的成本，是作恶的核心关键点。

于是在整个黑灰产的发展过程中，“接码平台”“发卡平台”及其相关产业成为了恶意注册产业链中至关重要的一环。



图为：利用接码平台、发卡平台完成的产业链协助

2.2.1 接码平台-提升黑灰产虚假注册的效率

接码平台实际上是一个接收短信验证码平台，它诞生在移动互联网早期。当时黑灰产购买猫池设备，再插上上百张手机卡来模拟上百个自然人，完成对业务场景的恶意注册。恶意注册完之后再把设备和电话卡转卖或者租用给另外一个黑灰产团队用于不同业务场景的恶意注册。

这个过程其实非常低效。因为一个黑灰产要负责三个环节：



图为：过去利用猫池完成恶意注册

接码平台的诞生就像是一个黑灰产的“交易平台”，它的价值产生在特定两个互联网黑灰产业链节点之间。

账号资源是众多黑产业链最上游、最基础的需求，而数量众多的卡源卡商，通过接码平台可以直接在线上把手机卡的价值卖给处于中游的大量号商，取得高回报。

号商，通过接码平台的网页端，可以直接获取手机号和验证码，完全不需要买入手机卡及相关设备，就能完成账号的注册。



图为：利用接码平台完成恶意注册

接码平台负责连接卡商和有手机验证码需求的群体，提供软件支持、业务结算等平台服务，通过业务分成获利，一般为30%左右。

2016年11月，当时规模最大的接码平台爱码被警方查处，缴获黑卡700余万张，自此很多接码平台转入地下，有些平台也通过关闭新用户注册等措施来降低风险。以接码平台爱乐赞为例，在2018年1月关闭了新用户注册，导致平台一号难求，其平台账号甚至达到每个100元。目前市场已有的接码平台非常多，比较活跃的有：火云、爱乐赞、ema666、60码、thewolf、玉米等。

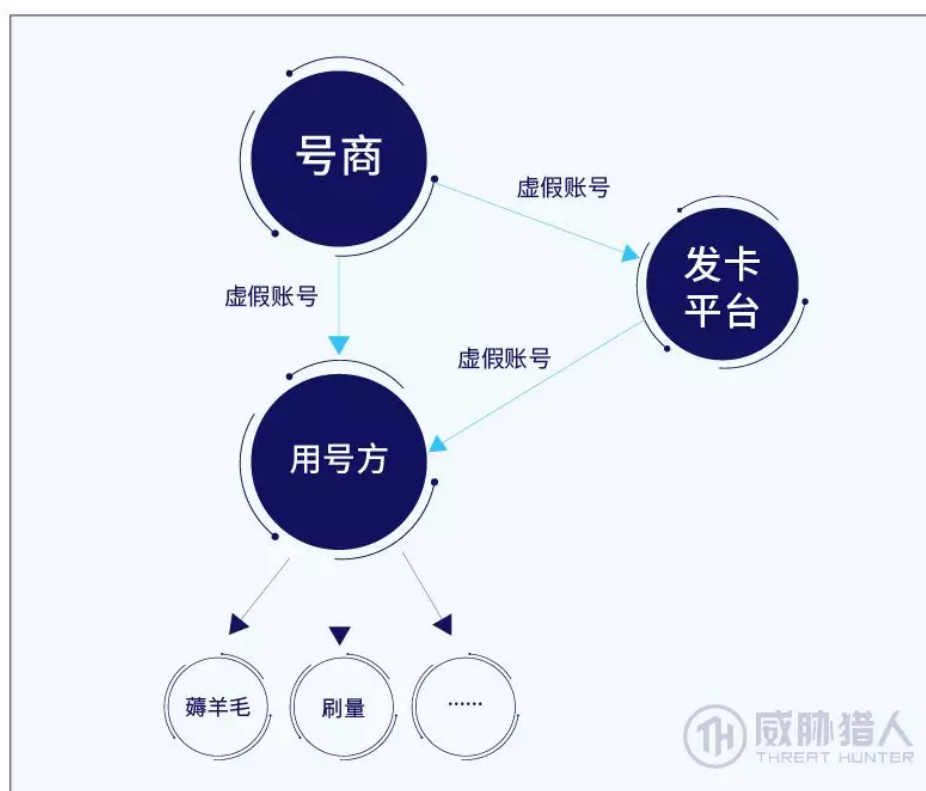
随着验证码对抗的升级，注册项目不再是通过单一的短信验证，有些需要语音验证，有些则需要二次验证，即需要注册用户使用注册的手机号向指定号码发送一条验证短信。接码平台也紧随市场变化不断升级，衍生出接收语音验证码、二次取号、发送短信的服务。

2.2.2 发卡平台-提升黑灰产账号流转的效率

发卡平台是把数字商品做自动化交易的平台，在号商完成大量账号的注册后，他们会把恶意账号整理后集中在发卡平台中列出，供处在产业链下游的用号方直接线上批量采购。

这就像在淘宝买一张话费充值卡一样，只是在应用的场景上，发卡平台现在已经是互联网黑灰产的主要交易通道和协作平台。

用号方会根据自身作恶场景，通过发卡平台买入对应的虚假账号，用以薅羊毛，平台刷量，账号诈骗等场景。



图为：利用发卡平台完成账号交易

根据永安在线对黑灰产的长期监测和资源统计，目前参与到发卡平台交易的黑灰产从业人员超过1万人，涉及的商品种类将近数千种，商品数量超过百万，年产值数亿元。

此外，通过追踪发卡平台上灰色商品的价格，我们发现，价格是体现企业风控策略有效性和市场需求变化的一个非常直观的因素，商品价格越高，代表企业风控策略越有效，使得黑灰产作恶成本变高。此时配合其他数据，若发现黑产发起攻击没有减少，那么原因是收益仍然高于成本，那么企业就需要继续进行对抗。

2.3 企业应对恶意注册的主要措施

2.3.1 防控-及时捕获黑灰产行为

在整个企业与黑灰产攻防战中，不同企业的业务场景不同会让整个攻防格局有区别。但黑灰产的核心资源始终是其控制的虚假账号，只要能在恶意注册这个点上对黑灰产施加有效的控制，对企业业务风控整体的风险就是相对可控的。

识别黑灰产资源

黑灰产在作恶和变现时都重度依赖于其手中持有的基础资源，包括但不限于手机号、IP、设备等。而这些黑灰产资源对于企业方来说，是全黑的数据，如果能将这些数据与自身业务数据进行匹配，就可以直接识别出恶意帐号或黑灰产恶意行为，针对性的进行相应的风险控制。

分析黑产工具

黑灰产的攻击工具承载着黑灰产的攻击逻辑和利用的企业业务漏洞，通过对工具的监控和逆向，企业可以了解到自身存在哪些业务逻辑漏洞或者是哪些风控策略已经失效，从而提升整个攻防对抗的效率。

监控黑灰产交易变化

黑灰产交易品类和价格的变动，能够反映出企业一定周期内风控策略的有效性。例如，即使企业上线了风控策略，但是黑灰产仍然能够以很低的成本完成恶意帐号的注册，则表示企业的风控策略失效了；另一方面，如果发现黑灰产交易价格变高，反映出黑灰产攻击成本的上升，则可以看出企业的风控策略有了一定的效果。有效的风险评估，能更好地推动业务安全的落地和迭代。

2.3.2 预警-对虚假账号进行风险预警

永安在线业务情报预警平台从黑灰产恶意注册的整个产业链出发，能对恶意注册的不同阶段进行监控和预警，帮助企业发现和掌控自己面临的虚假账号现状。

新增的恶意注册项目：黑灰产在实施恶意注册行为之前，首先要在相应的平台上创建一个新的项目。而这个创建项目的行为就是黑灰产即将发起攻击的信号。我们通过对这一情报的监控，可以随时获取黑灰产的最新动向。

正在发生的恶意注册行为：黑灰产发起恶意注册时使用的自动化工具、利用的恶意资源、攻击的接口等，都是暴露攻击逻辑的路径。这些情报可以用来及时的还原黑灰产攻击逻辑，进行有效的风险控制。

恶意账号倒卖风险：在黑灰产完成注册之后，通常会将虚假的账号放在发卡平台进行交易。永安在线情报预警能够实时监控到黑灰产虚假账号新增或下架交易信息及价格的变动，帮助企业了解黑灰产攻击趋势的变动及自身风控的有效性。

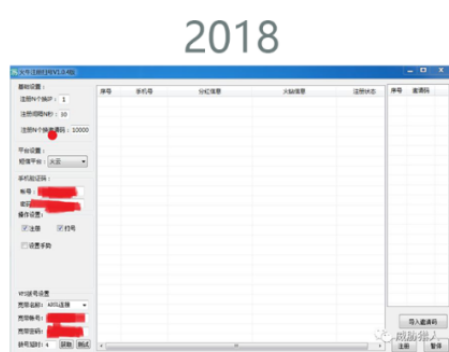
3. 作恶方式从自动化工具向真人众包演变

3.1 黑灰产作恶方式的趋势演变

站在2020年时间点上，我们回顾过去两年黑产的动向，发现黑产攻击的趋势：

3.1.1 黑产工具与产业链的整合程度加深

黑产工具在经过长期的技术升级，相较于仅将接码平台与网络代理模块进行组合，已经实现了在单个工具中可以集成接码、打码、宽带秒拨、网络代理等多个针对绕过业务安全风控节点的功能。通过集成多个功能，黑产可利用工具实现定制化更强、功能更多的作恶行为。现在的黑产工具集成度更高，造成的影响也更大。



工具功能单一

只集成短信接码和代理连接



工具功能较多

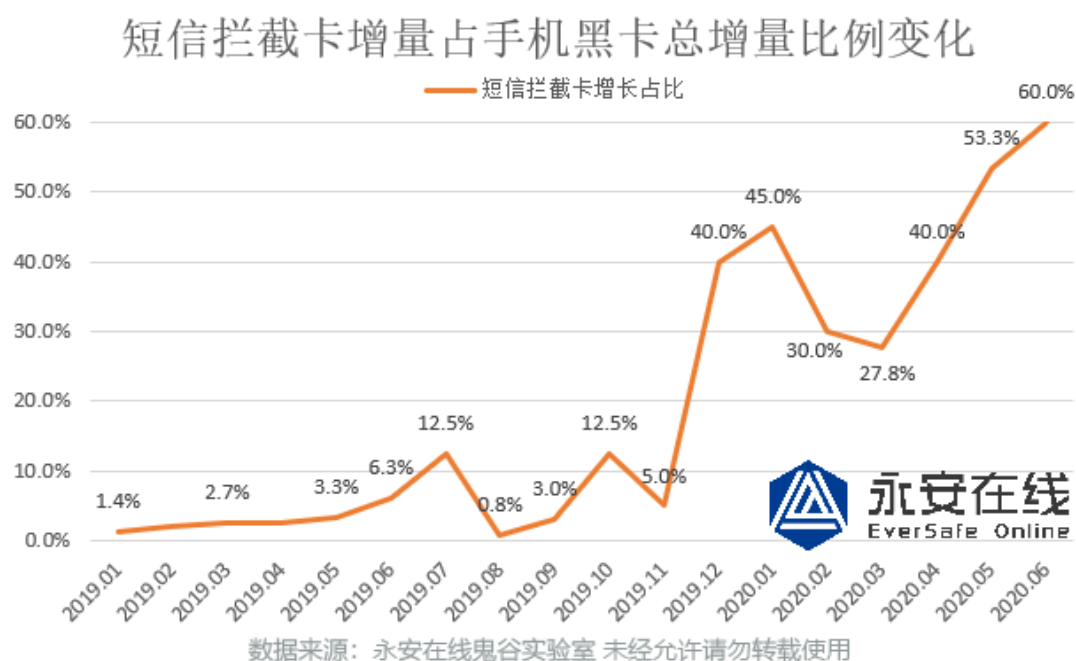
集成接码打码、IP代理伪装等功能

还可控制攻击线程数

图为：黑产工具的变化

3.1.2 将攻击行为隐藏于正常用户行为中

相较于以往，黑产已开始利用手机短信拦截卡和秒拨IP的方式去绕过业务安全风控模型以实现攻击。这两种攻击方式有一个共同点，就是使用的资源是与正常用户共用的，这导致在一般的风控模型下不会被判定为黑产行为。



图为：短信拦截卡增量占手机黑卡总增量比例变化

对于可以获得高利益的攻击，黑产还开始利用众包任务的方式，发布注册任务，用相对较低的价格获取到大量真人实名认证的账户。

本质上，真人作弊源于人的贪婪和惰性，驱动因素是互联网技术和企业与黑灰产长期攻防对抗，从而演化出了此类比较高级的作恶形态。下章将对真人作弊进行深入剖析，此处不做赘述。

3.2 黑产作恶方法的转变

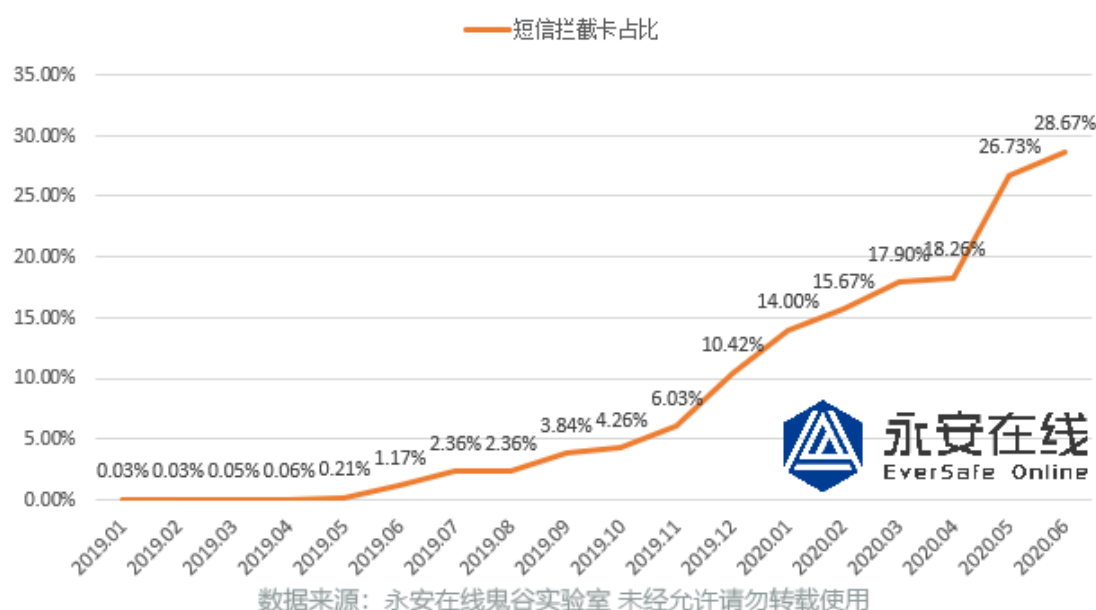
3.2.1 手机号的转变-短信拦截卡比例增高

在业务安全层面，识别黑产持有的恶意手机号码是一个持久战。利用现有的黑产手机号情报，一般都可以实现对黑产手机号的拦截。黑产面对来自业务安全的防御，也对持有的手机号进行了或多或少的改进：新采购的手机号先利用其“干净”的身份去注册高利润的账号，对高净值的账号注册结束后再打包给下游进行中低净值黑产进行利用，从而压榨一个手机号中的价值。但是这种由于黑产仍然需要去进行养号的工作，再加上运营商对这些号段的回收利用效率的提升，导致新采购手机号的可利用价值逐渐贬值。

伴随着近几年国内一些手机厂商推出大量面向低端市场和海外市场的产品，黑产在其中发现了可利用的机会。黑产通过在这些机型中植入可以拦截手机短信的木马，利用手机持有者的手机号进行短信的获取，再通过网络传输给黑产，从而实现利用该手机号进行牟利。

短信拦截卡这种黑卡从2018年底首次发现，由于其隐蔽性相对其他渠道更高，实际出现时间可能早于首次发现时间。2019年5月拦截卡数量出现一次增长爆发，平台聚集。得益于恶意注册市场需求的激发，拦截卡的增长速度迅猛，之后黑产持续补充相关“卡源”，使得拦截卡在手机黑卡产业中占据了自己的一席之地。

手机黑卡中的短信拦截卡占比统计



图为：手机黑卡中短信拦截卡占比统计

在这种作恶场景中，由于该手机号持有者为一般用户，导致该手机号在正常情况下不会被判定为黑产持有的手机号，当黑产利用其手机号进行恶意注册时，一般的业务安全体系不会将其判定为黑产注册行为，黑产就可以通过这种“漏洞”去进行获利。

3.2.2 真人作弊乱象-新客福利被黑灰产和羊毛党恶意赚取

除了用手机号黑卡批量注册需要被防范，一些平台的新客福利也有可能被黑产赚取。

很多的垂直领域平台为了更好的吸纳新用户，会在平台内给这些新用户发放一些礼品卡、话费、平台礼金等高价值福利。部分平台为了防御黑产针对新用户福利的恶意攻击，会采取强制用户领取礼包前进行实名认证，这种方式确实直接避免了黑产利用工具自动化注册牟利，但是却拦截不了来自真实用户认证后再转售帐号的真人作弊行为。

从根源上讲，薅新用户福利一般都是由一些常见的羊毛党用户发现，然后发布到类似赚客吧等“专业薅羊毛”社区进行分享，到这里平台的损失还是可控的。如果发放的福利是第三方礼品卡或平台礼券这种可通过下游进行变现的，就会吸引黑产投入成本，利用真人众包的方式去进行牟利。

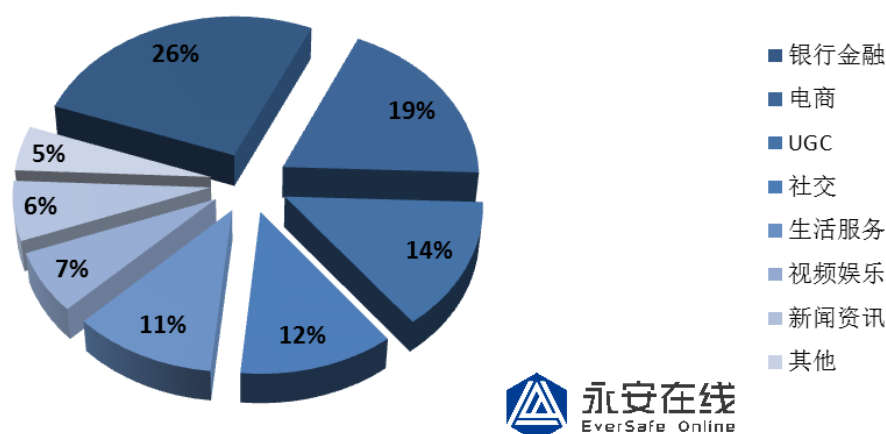


图为：某真人众包应用截图

根据Karma上的检测，真人作弊目标行业类型主要有以下几个部分，银行金融、电商、UGC平台和社交平台成为了黑产盯上的主要目标。按永安在线的预估，真人作弊产业每年产生约

20亿元的悬赏金额流水、10亿元完成金额流水，直接对目标平台造成数十亿甚至百亿的损失。

真人作弊目标行业类型占比



图为：真人作弊目标行业类型占比

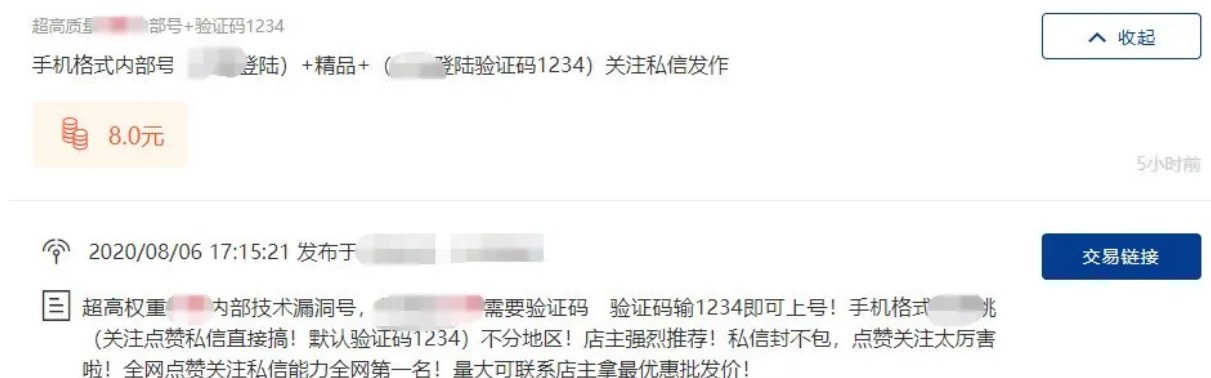
3.2.3 刷量方式隐蔽升级-从假肉鸡到真肉鸡

流量造假一直困扰着互联网广告行业，这是因为互联网广告的按量付费结算方式决定的，这个量既包含点击量，又包含曝光量。因为这些量化的指标，有些不法的广告平台采取一些手段，在广告点击和广告曝光上做手脚，通过造假的方式去完成广告触达指标，从而获得广告投放费用。

以前互联网广告流量作弊一般就是由专门的刷量工作室去接单，利用分身工具和IP代理工具伪装成大量设备进行刷量，这种刷量方法在现在的风控体系里通过IP画像可以很明显的发现，其IP一般为代理IP。

现在广告刷量花样就比较多了，有网页广告采用隐藏浮层的方式进行刷量，有软件广告通过恶意弹窗进行刷量，还有利用小众宽带进行宽带劫持弹窗刷量。通过这种方法，这些刷量平台和广告公司可以挣得盆满钵满，只有广告主成为冤大头。

而随着社交媒体的发展，广告刷量在社交媒体上又掀起了新的风潮，在Karma业务情报平台上我们可以看到有些黑产在售卖一些社交媒体帐号，声称帐号为平台内部漏洞号，刷量可快速上趋势榜前位。



图为：与社交媒体刷量相关联的黑产情报

3.3 新型黑产的可行应对方案

3.3.1 拦截卡黑卡作恶方式

业务安全的攻防在过去长期是围绕着“人机识别”为基础的。黑产用的是假人、假设备、假号码。逐渐的黑产开始用真实的手机设备，现在也大规模的应用的真人手机号码和IP资源。这无疑为业务安全攻防带来更多挑战，当判定对象已经被好人和坏人同时持有，识别的难度及误判的风险、客诉问题就都更加严峻。

面对拦截卡这种黑卡作恶，需要以“是否为持卡人本人操作”来区分是不是被黑产利用，这需要根据拦截卡本身特点和使用拦截卡攻击过程中的特征进行判定：

- 1) 通过自身业务场景设置判断规则
- 2) 根据拦截卡的出现频次，以及手机黑卡、黑IP的命中次数进行判定。

3.3.2 真人众包作恶方式

真人众包的作恶主要为通过发布众包任务的方式进行作恶，我们如果要应对的话首先需要知晓其作恶流程。上面对真人众包作弊流程进行了文字性描述，为了方便起见这里拿了某短视频应用真人作弊众包任务，可直观感受下黑产在下发真人众包作弊任务时的流程。



图为: 某短视频众包任务流程

真人作弊的作恶可以通过情报维度和数据维度两个方面共同分析, 对真人作弊帐号进行精准的定位:

- 1) 情报维度的信息, 获知哪里记录了礼品最快领取流程, 可以帮助我们直接抹去和黑产之间的信息差, 并在最短的时间夺取主动权.
- 2) 数据维度可以用是否有异地登陆、异地登陆设备等特征去进行复合判断, 以发现黑产动作特征, 及时发现被黑产控制的帐号。

3.3.3 刷量方式的应对措施

对于广告投放商来说, 一般都会对相关的广告投放加以统计代码进行数据统计。此时通过统计代码自带的页面统计功能发现恶意刷量的行径:

- 1) 通过停留时长发现刷量的请求

2) 可以通过对IP的检测发现是否是来自于刷量工作室的访问，从而清洗出相对干净的用户访问列表。

社交平台的刷量解决方案更倾向于结合真人作弊的定位方式进行分析，通过情报维度和数据维度发现被黑产控制进行刷量的帐号，然后根据特征进行一网打尽：

1)情报维度的信息，通过了解黑产可以进行刷量的操作点，对相关环节进行监控，拦截来自恶意手机卡和恶意IP的请求。

2)数据维度可以用是否有异地登陆、异地登陆设备等特征去进行复合判断，以发现黑产动作特征，及时发现被黑产控制的帐号。

4. 真人作弊深度剖析

真人作弊俨然已经发展成为目前黑灰产最常见、最难以防御、同时也对风控体系破坏极大的一种侵害平台整体安全性及稳定性的作恶形式，在隐秘的角落里，它无时无刻不给平台带来伤害。永安在线基于长期对真人作弊产业的调查和研究，深入剖析这个产业的方方面面，解析真人作弊产业的发展、现状、危害以及防御思路，力求以最专业、最全面的视角呈现它的全然样貌。本部分主要分为以下几个要点：

- 1) 真人作弊黑灰产经过数年发展，模式和形态越发多元和丰富，已渗透至众多场景、众多行业；
- 2) 真人作弊黑灰产发展迅猛，自2014年至2020年，真人作弊平台（app）的数量在增长了近40倍，参与人数增长了近百倍；
- 3) 相较于机器作弊，真人作弊对甲方的风控和安全能力提出了更高的要求，带来了新的挑战；
- 4) 以情报能力和数据能力为风控赋能，是识别新型欺诈模式的有效方式方法。

4.1 发展与现状

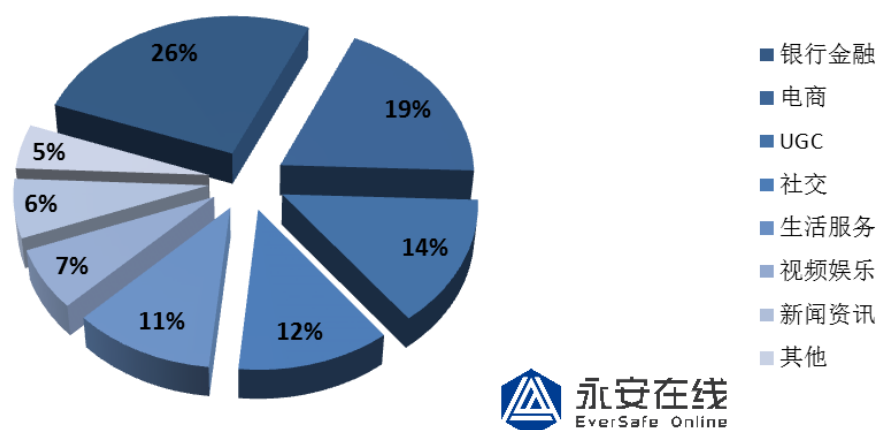
本质上，真人作弊源于人的贪婪和惰性，驱动因素是互联网技术和企业与黑灰产长期攻防对抗，从而演化出了此类比较高级的作恶形态。近年来，这种模式和形态越发多元和丰富，从早期单一的兼职刷单，到如今的多行业、多场景、多任务的广泛渗透；从早期的只在PC端进行的单一手法的兼职，到如今以移动端为主；从早期的线上群组媒介（QQ群、YY语音等），到如今平台化、裂变变化。

4.1.1 多行业、多场景、多任务广泛渗透

1) 多行业涉及

真人作弊涉及的行业极其广泛，从金融领域到UGC娱乐，从生活服务、视频音频到新闻资讯、社交聊天等，无所不涉。如下图所示，是真人作弊的目标行业类型占比：

真人作弊目标行业类型占比

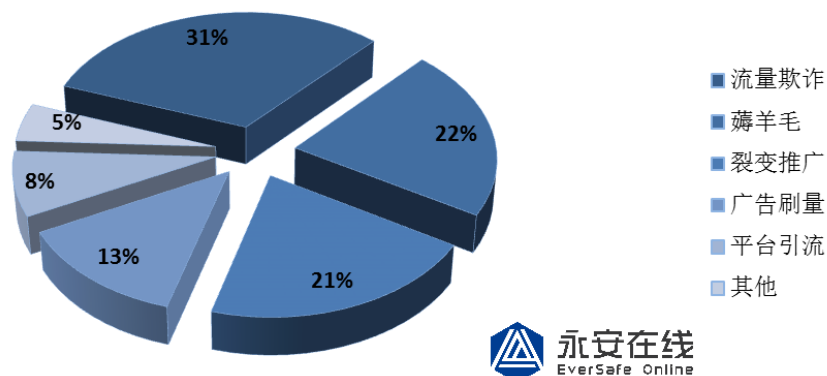


图为：真人作弊目标行业类型占比

2) 多场景渗透

在业务范围方面，真人作弊也几乎涵盖了所有黑灰产作恶场景，无论是薅羊毛、流量欺诈，还是广告刷量、平台引流、裂变推广等场景，真人作弊都参与其中。具体占比见下图：

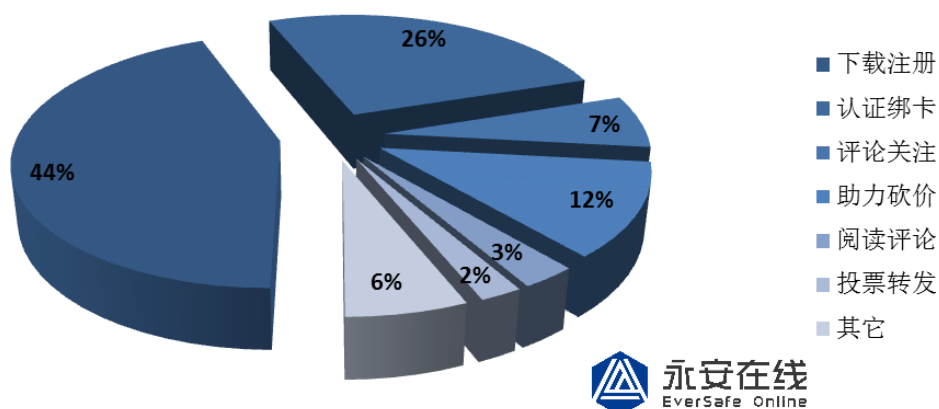
真人作弊场景类型占比



图为：真人作弊场景类型占比

3) 多任务参与

真人作弊任务类型占比



通过统计长期监控到的真人作弊任务标题、内容和关键词，形成以下词云图，从中也可看出真人作弊的主要关注任务是：下载注册、认证绑卡、评论关注等。



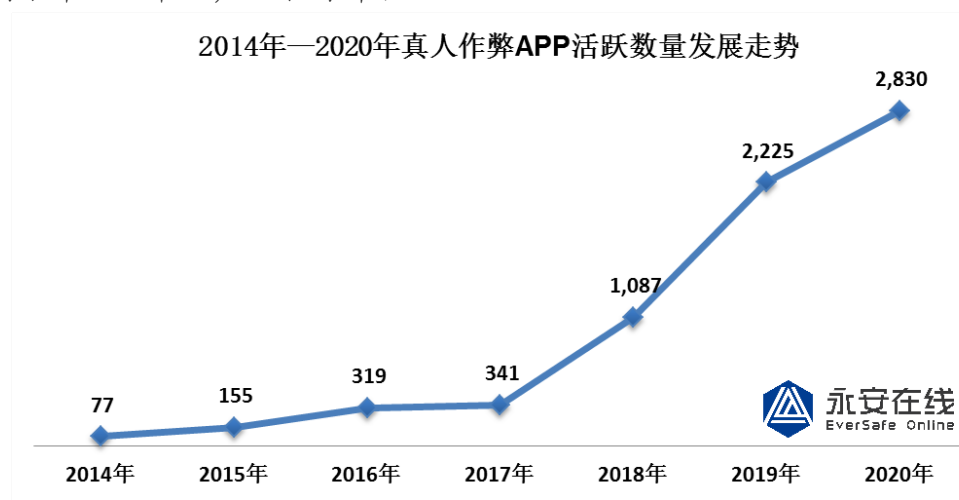
图为：真人作弊任务类型词云图

4.1.2 真人作弊APP近年发展迅猛

1) 2014年-2020年APP活跃量及下载量指数级增长

在最早期，真人作弊还是以“线上群组”的方式为媒介进行交流和信息传播，典型的有YY语音群组、QQ黑灰产交流群、论坛聊天等，但是当互联网走向移动化之后，真人作弊也紧跟时代发展的步伐。

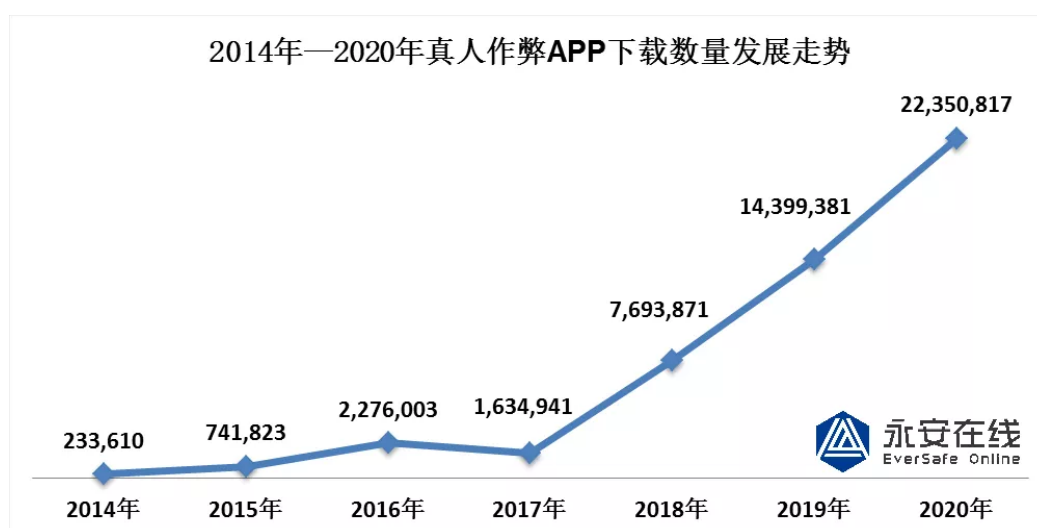
永安在线监控到，从2014年到2020年，真人作弊APP数量呈现几何式增长：2014年的时候不到百款，到今年近三千款，如下图所示：



图为：2014年—2020年真人作弊APP活跃数量发展走势

（注：2020年上半年整真人作弊APP的活跃数量为1,415款，基于2019年的数量，以及真人作弊的发展现状，我们合理推测：2020全年活跃的真人作弊APP可达2,830款。）

在真人作弊APP活跃数量呈几何式增长的时候，相关的下载量也增长迅猛：

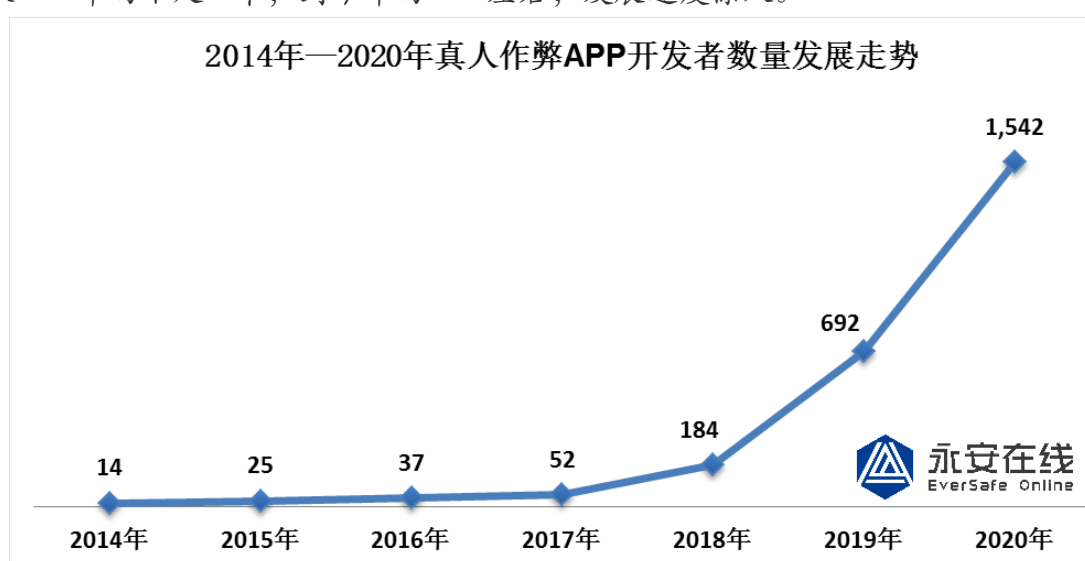


图为：2014年—2020年真人作弊APP下载数量发展走势

(注：2020年上半年整监测到的真人作弊APP下载量为12,350,817次，基于2019年的下载数量，以及真人作弊的发展现状，我们合理推测：2020下半年真人作弊APP的下载量可以再增加10,000,000次，最终至全年下载量为：22,350,817次。)

2) 2014年—2020年开发者增长迅速

真人作弊参与人数爆发式增长的背后，离不开资源的支撑，其中一个重要资源就是平台：真人作弊平台——即真人作弊APP，这一方面可以从真人作弊APP的开发者数量中体现，在永安在线监控到的数据中，我们可以发现真人作弊APP的开发者数量同样呈现指数形式的增长：从2014年的不足20个，到今年的1500左右，发展速度惊人。

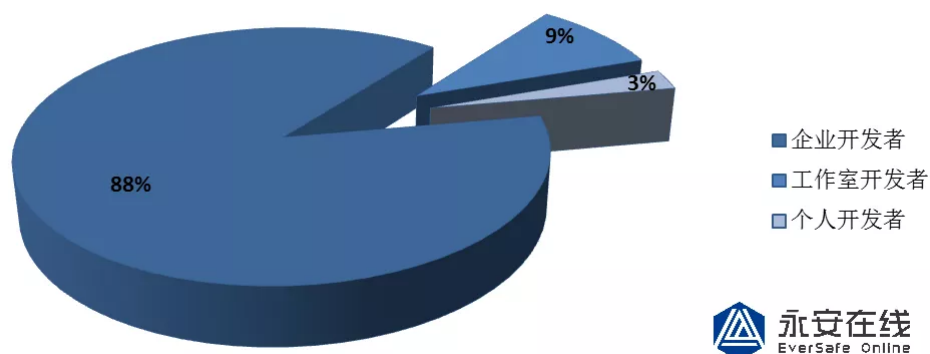


图为：2014年—2020年真人作弊APP开发者数量发展走势

(注：2020年上半年整监测到的真人作弊APP开发者数量是771个，基于真人作弊发展现状，我们合理推测：2020年全年真人作弊APP开发者数量可达到1,542个。)

在永安在线监控到的所有移动开发者中，企业开发者有1,407个，占比总数1,598的88%。

各类开发者数量占比

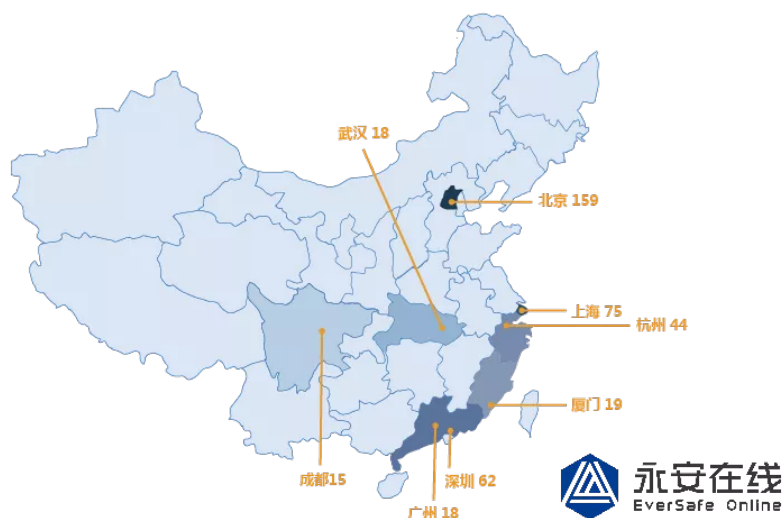


图为：各类型开发者数量占比

企业开发者占比近90%，提供真人作弊平台类服务的利润可见一斑。因小知大，这也从侧面反映出，整个真人作弊产业的利润何其丰厚。

开发者的地域分布也和中国互联网的地域发展特征基本吻合，前四个地区分布是：北京、上海、深圳、杭州：

真人作弊开发者城市分布



图为：真人作弊开发者城市分布

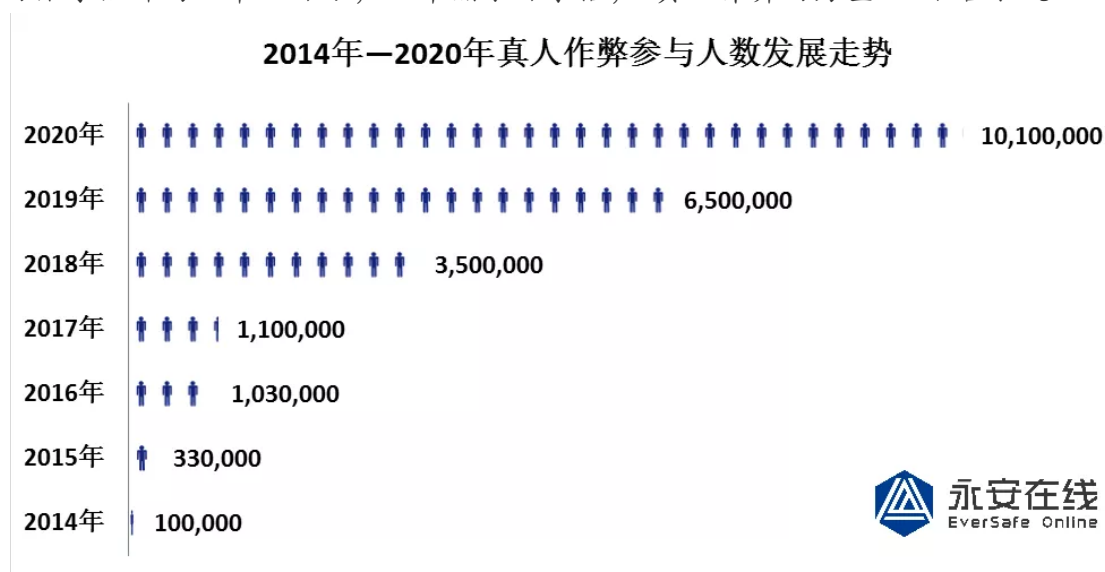
更有甚者，个别公司同时开发了很多款真人作弊平台了APP，比如位于蚌埠的某家公司，同时开发了23款真人作弊APP；青岛的某家公司，同时开发了10款真人作弊APP等等。所谓无利不起早，可见开发真人作弊APP，能够为这些公司带来的利润不会太少。

4.1.3 真人作弊参与人群画像

那么，参与真人作弊的用户都有什么特征呢？

1) 真人作弊产业人数

无论是真人作弊任务的多样性还是APP的蓬勃发展，其背后都是因为巨大的需求推动。实际上，永安在线监控到的参与真人作弊的用户的确呈现指数型增长，从2014年的十万余人，到今年的保守估计约一千一百万，七年翻了百余倍，"真人作弊的力量"已不容小觑：

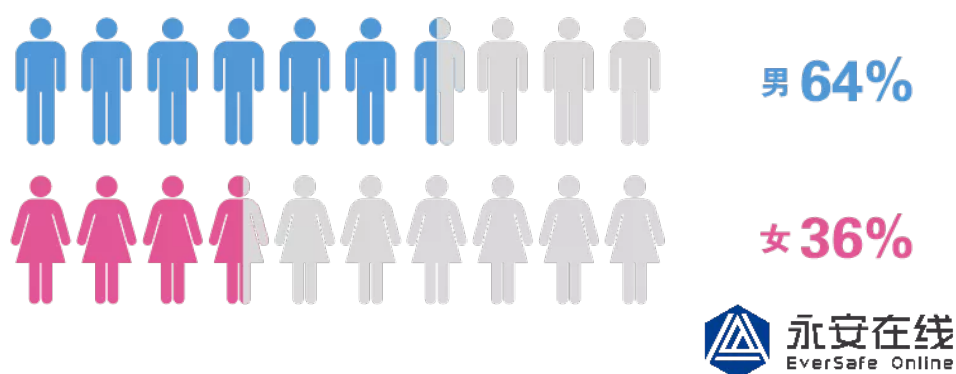


图为：真人作弊参与人数发展走势

2) 真人作弊男女比例

通过对参与真人作弊用户群体的随机抽样调查发现，真人作弊参与者以男性居多，占比为64%，女性为36%：

真人作弊参与者男女比例

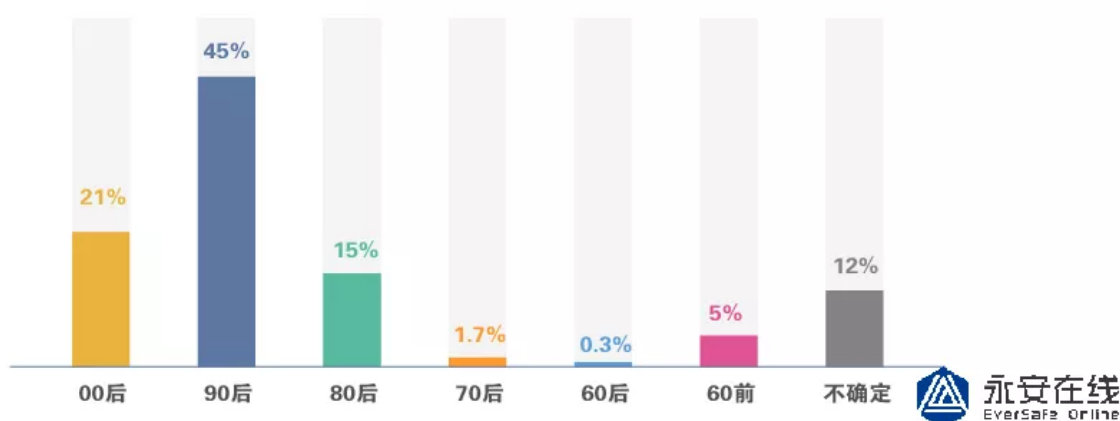


图为：真人作弊参与者男女比例

3) 真人作弊年龄分布

在年龄分布方面，90后是真人作弊的主力军，占比45%，接下来是00后及80后，分别占21%和15%，可见参与作弊的人普遍年轻，这也从侧面反映出来，真人作弊的产业还会继续发展下去。

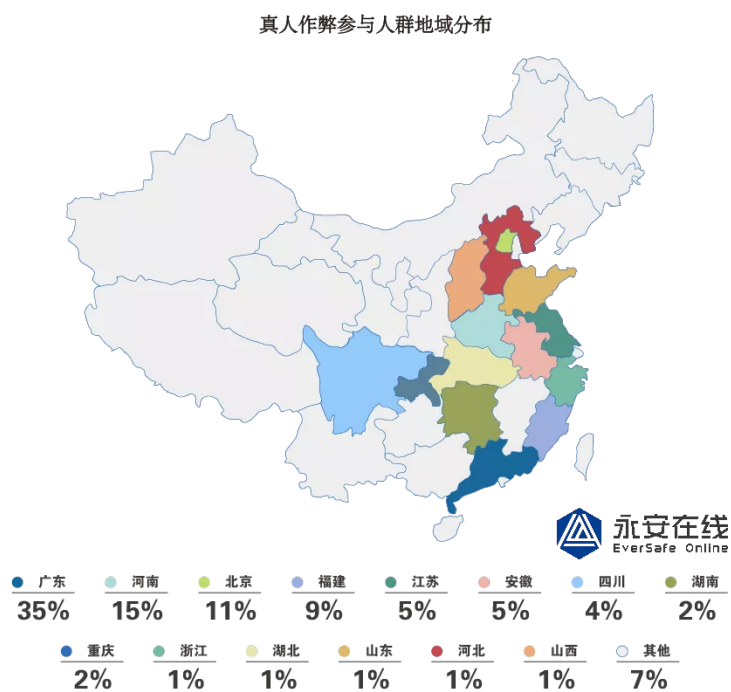
真人作弊参与者年龄分布



图为：真人作弊参与者年龄分布

4) 真人作弊参与人数地域分布

从地域上来看，真人作弊的参与者分布在华南、华东、华北、华中这几个区域，其中华南区域的广东省占比最多，达35%：



图为：真人作弊参与人群地域分布

4.1.4 真人作弊对行业造成的损失统计

那么真人作弊对各个行业造成的损失是多少呢？永安在线对近半年的真人作弊平台任务进行了全量统计，以悬赏数量、悬赏金额、完成数、悬赏时间、完成时间等因素进行计算，共得出以下结论：

真人作弊产业每年约产生20亿元的悬赏金额流水、10亿元完成金额流水，直接对目标平台造成数十亿甚至百亿的损失。

4.2 痛点与危害

4.2.1 真人作弊 vs 机器作弊

	真人作弊	机器作弊
作恶群体	黑产团伙+大量真实用户	黑产团伙
作恶设备	真机	群控、云手机、模拟器
作恶资源	真实手机号、真实IP	黑卡、黑IP
作恶流程	真人操作	协议破解/模拟操作

表为：真人作弊和机器作弊特点对比

4.2.2 真人作弊 vs 传统风控

传统风控是基于黑产资源和黑产团伙所表现出的“非正常人”的特征来做风险行为的检测和识别，当黑产藏匿于幕后，以现金奖励调动真实用户完成作弊任务，“人机识别”被“真人”挑战，传统风控便显得捉襟见肘。风控痛点具体表现在以下四个方面：

1) 防护手段失效

无论是规则层面的风险数据库、风险规则库、风险特征库等，还是模型层面的AI算法、决策引擎等，其知识的积累主要来自于长期对机器作弊的数据分析与沉淀。猫池黑卡、代理IP等传统风控数据黑名单完全不适用于真人作弊的场景，另外，真人作弊人群行为、画像、用户关系等特征往往比较离散，且变化多样，虽然不是完全的无迹可寻，但算法模型的输入强依赖于安全人员对风险数据和场景的洞察和分析能力，需要非常高的运营成本。

2) 处置边界模糊

相较于处置违规的黑产账号，处置违规真实用户账号的复杂度大幅提升。如何合理地对真实用户的违规行为分类分级，如何兼容风控指标和用户体验，如何向业务团队提供强可解释性的处置理由等等，这些对于风控团队而言，考验进一步升级。

3) 风险响应滞后

一旦真人作弊风险事件发生，在前期风控团队几乎是无力的，只能任风险事件的影响范围不断扩大。从风险事件的发生，到对抗方案的实施落地，时间差越大，损失越大。真人作弊场景下，这个时间差远大于机器作弊。

4) 溯源复盘困难

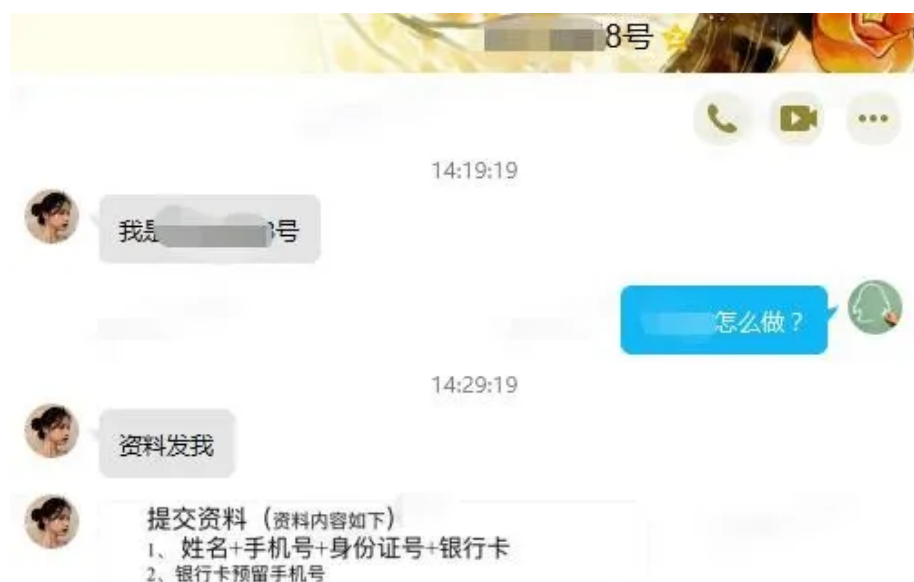
真实用户介于黑产与受害企业之间，为黑产筑起天然屏障，难以进行事后追踪与溯源。且从已掌握的作弊数据，只能关联扩散有限范围的作弊数据，真人作弊模式变化频繁，无法对今后的真人作弊行为形成有效的知识传递与经验复用。

4.2.3 真人作弊带来的额外风险

除了常见的机器作弊带来的常见危害（如营销作弊、渠道作弊、虚假用户、刷单假量等）之外，真人作弊还引入了个人信息被黑产滥用和泄露的风险。

黑产收购真人用户注册的账号，用于不法用途。黑产诱导真人用户协助完成好友辅助认证、实名、人脸认证等，真人用户不但违反平台用户条款，甚至还需承担潜在的法律风险。另外，永安在线安全团队在对真人作弊产业链进行调查的时候，曾经深入调查一个金融类的悬赏任务，这个任务是“认证绑卡”类型的任务：用户只需要绑卡成功就能得到30—50元的佣金奖赏。

首先，从收入产出比上看，黑产肯拿出这么高的佣金，说明黑产的收益很可能达到百元甚至更多，所以对于进行推广的金融平台来说，必然会承受不小的损失；其次，我们在与任务发布者进行聊天的时候，被要求在完成任务后提供：姓名+手机号+身份证+银行，如下图所示：



图为：与任务发布者聊天

注意，把这些资料交给任务发布者之后，还是不能拿到佣金，必须完成最后一步：把手机接到的短信验证码交给任务发布者后，才能收到佣金。姓名、手机号、身份证、银行卡以及短

信验证码，是非常敏感的个人信息，完全暴露在黑产的控制之下，个人信息甚至财产安全受到严重威胁。

4.3 对抗与解决

如此澎湃汹涌的真人作弊，有着相对于机器薅羊毛的种种优势，以及对传统风控直捣黄龙式的挑战，所带来的挑战愈发严峻。那么，到底该怎么防控呢？

永安在线认为，情报能力和数据能力为风控赋能，是对真人作弊新型欺诈模式的解决办法。

4.3.1 情报维度

举个例子，永安在线去年在对真人作弊平台进行全面监控的时候，发现了一些类似这样信息的任务：“注册下载XX软件，密码统一设置为a123456，做完之后与我联系结付。”

之后，我们顺藤摸瓜，在其余的几百个真人作弊平台中找到了同类相关任务达近十万个，其密码设置要求都是一样的，这明显说明是同一个团伙在对这个平台进行批量注册类攻击，为了便于记忆和统一管理，所以要求任务完成者设置统一的简单密码。

我们捕捉到这个威胁信息之后，进行了全网的情报搜集和关键信息整理，包括密码特征、任务发布者信息、任务最早开始时间等等，然后第一时间把这些关键信息交给了该社交平台。平台在接到我们的情报信息之后，也在第一时间进行了反向溯源和定位，结果的确揪出来了一个大型的灰产团伙，并成功打击，直接维护了平台的安全、和谐，并提前将伤害扼杀在摇篮之中。

4.3.2 数据维度

情报维度的信息，可以帮助我们直接抹去和黑产之间的信息差，并在最短的时间夺取主动权，然而，仅有情报信息，终究单薄，此时还需要数据信息对黑产进行定位以及后续挖掘工作的支持。真人作弊相关的风险数据包括：风险APP、风险设备、风险账号以及真人作弊中任务的二维码、链接、教程、任务流程等等。

举个例子，今年5月份开始，某家国内支付平台开始做拉新和绑卡送礼的活动，因为涉及到支付和银行卡，所以奖励金额很高，这自然会被黑灰产盯上。但毕竟这类活动要求实名、绑定银行卡等，机器作弊的成本和门槛较高，所以拥有特定渠道资源的黑灰产开始在众多真人

作弊平台发布任务（我们在长期跟踪研究之后发现，有些黑灰产团伙拥有大量的返现资源，这种资源被他们成为“口子”）。

永安在线在第一时间感知到威胁之后，对此类作弊方式进行了重点监控，一方面从情报维度进行广泛的情报收集与分析，一方面基于永安在线上亿级的设备画像能力，对真人作弊用户进行了风险设备的定位以及信息提取工作，另外也把这些风险设备、任务分享链接和结算链接等数据特征交付给了该支付平台。

平台在收到数据后进行了匹配验证，直接发现了数千个风险账号，之后又通过这些账号的共性行为和网络关系再次定位到了数百个上游师傅账号，以及数万个下游风险账号。永安在线进一步协助该平台研究这些师傅账号的行为，发现这些师傅账号长期隐匿在平台，每逢活动就组织薅取羊毛的恶意用户。

三、攻防技术的迭代

1. 黑产群控进化史

2018年下半年的时候，出现了一家号称“市面上最好用群控”的设备厂商，大肆地鼓吹和宣传自己的产品，据说光占地面积就要比传统群控节约95%。我们购买并动手拆了一台设备，拆解发现，这是一个需要连接网线和电源线的箱型设备，可以简称它为“箱控”。

1.1 群控&箱控

群控，是一种通过操作多台手机进行批量攻击的方式，可以说是黑产工作室的刚需，在市场需求催生下，群控类设备的供应商都非常擅长与利用各类技术对其进行升级优化。以下是某工作室的群控设备照片。



下图这次的主角——箱控的内部构造。将十二台安卓手机的屏幕拆掉，把主板通过电路集成方式集成至一块大主板，进行统一供电和管理。



至于设备数量问题，它通过切割内存的方式，将每个手机主板切割为十个分身。最终达到，操作一台箱控相当于操作一百二十个不同手机的观感。原本需要一个大厅存储的手机设备，现在只需要几个货架，大幅缩减了黑产的设备运营成本。

批量操作方式上，企业大部分业务接口的关键参数都设置有特定算法，在无法对其破解进行直接攻击的时候，黑产常常需要通过模拟点击的方式伪装正常用户操作，达到攻击目的。常见的模拟点击方案是通过识别颜色、文字、形状来定位到需要点击的坐标，这种方式经常需要进行容错判断，再一次通过识别颜色形状等，来判断自己是否点击进入了目标页面，每次识别要消耗时间，速度相对较慢。

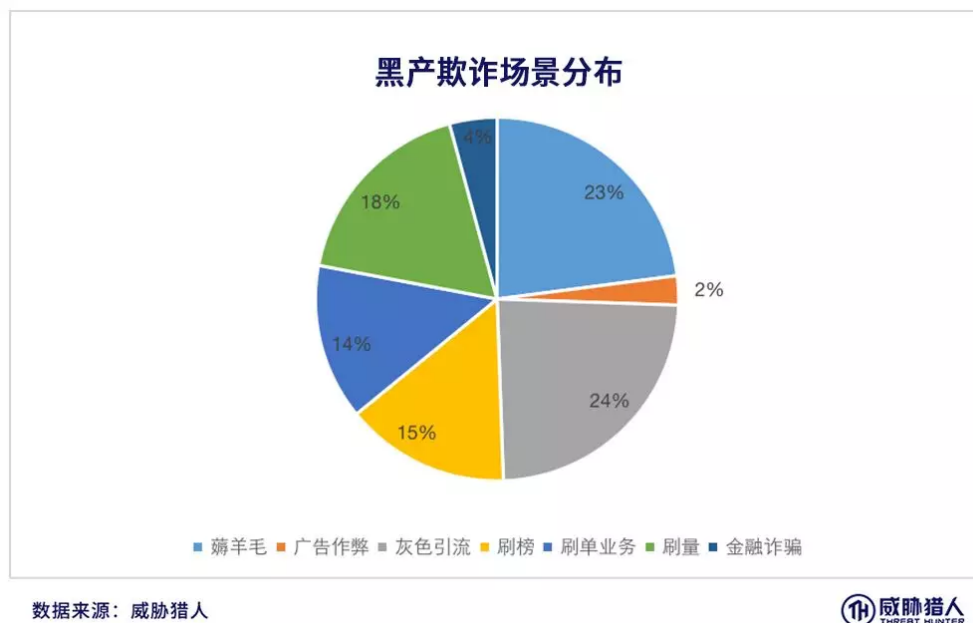
箱控使用了appium——基于Google UiAutomator2的安卓自动化测试工具，通过文字、控件id、控件名称等直接定位到APP的控件进行操作，也就是说和上述方式相比，不用每次点击后截图，也不用根据图片一个像素一个像素的判断该点击的位置，速度得到了提升，而很多企业自身产品的自动化测试就是采用appium完成的。

1.2 黑产进化，优化攻击效率和成本

回想“群控”一路的进化变种，再结合近来的种种事件，我们发现，当前互联网黑灰产攻击有两个特点：

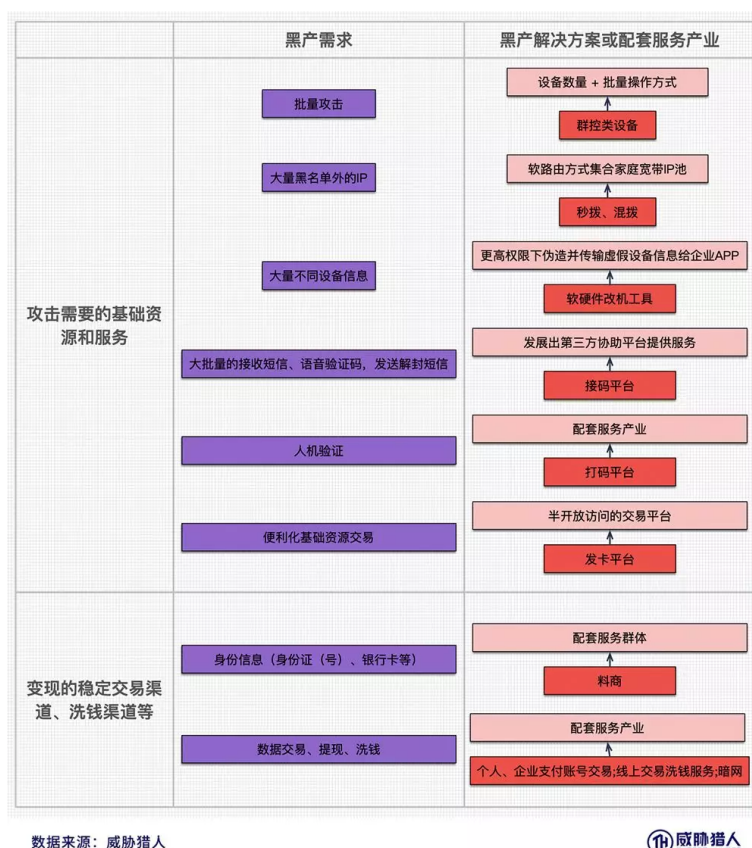
1.2.1 六成攻击场景以量取胜

随着互联网的发展，黑产形成了一些固定的攻击模式和套路，有大量的攻击场景依附于流量，通过伪装成正常业务，再通过不断重复获利。



1.2.2 重度依赖黑产基础资源

在黑产市场，像设备这样需求庞大而稳定的“资源”还有很多：IP、身份证、银行卡、支付账号、改机工具、自动化攻击软件、过滑动验证码、隐秘变现渠道等。也都逐渐形成了像接码平台一样的“服务型黑产协作平台”，这些平台越来越多，组合成了一张庞大的黑灰产基础资源网络。黑产攻击也严重依赖这些基础资源。



图为：黑产需求及对应的解决方案

由于攻防逻辑和上游服务资源均趋于固定，黑产目前已经从攻防逻辑迭代的时代逐渐过渡到攻击效率和成本的优化迭代上。依旧以攻击设备为例，我们来一探其变化过程。

1.3 黑产解决批量攻击的方式

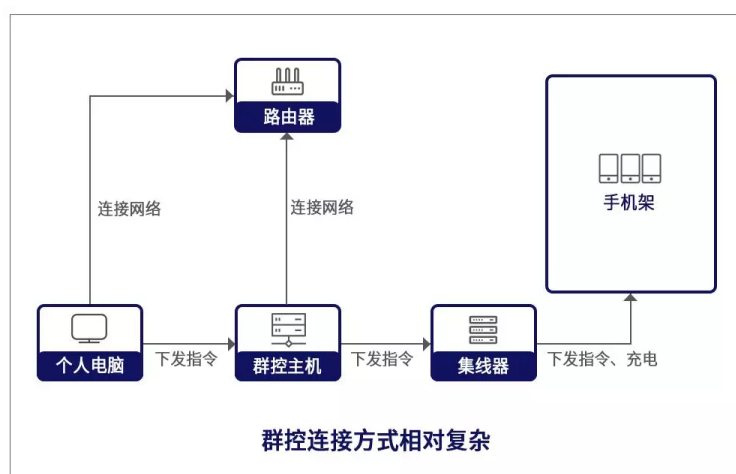
1.3.1 箱控

优化点：将通用类的攻击工具打包配套提供服务，降低了攻击的操作门槛

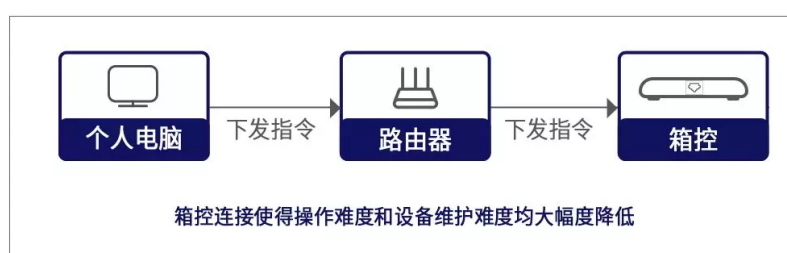
黑产在群控类的设备与服务商，均表现出将秒拨IP、改机工具等一些通用类型的功能进行打包集合的趋势。

将VPN功能和改机功能、虚拟定位功能内置，并且提供了云端备份能力，黑产可以将一套攻击环境连同环境上登录的账号一并上传备份，通过还原快照的方式切换环境，从而进行大量攻击。箱控也提供了内存管理等能力，更好的满足了群控类设备的目标——降低运营成本，即可以用更少的人力操作更多的设备，攻击的效率和频次均得到了有效提升。

除了运营成本和攻击效率以外，这种打包的方式，也有效降低了黑产的操作和技术门槛，小白只需要保证配置正确即可，意味着黑产可以在对“技术要点”了解更少的情况下发起攻击，防守方将面临更多更杂的攻击人员。



图：威胁猎人绘制



图：威胁猎人绘制



1.3.2 租赁模式-“云手机”

优化点：租赁模式，自由“扩容”，降低了维护设备成本，且方便备份传输设备信息

“云手机”是一种攻击设备租用模式，操作者可以通过客户端或浏览器直接对远端的手机（或虚拟手机）进行操作，发起攻击。

云手机与“群控”类设备的趋势相同，越来越多的云手机将“一键新机”、虚拟定位和代理IP进行打包销售，这样的打包服务价格4元/天。加上手机号接码成本和网络成本，几十元到百元就可以拿到游戏的入场券。其成本远远低于传统实体手机的攻击方式。企业面临攻击人员更复杂广阔的现实问题。

黑产熟手还可以在需要时，利用云手机对自己的攻击设备群进行即时“扩容”，模式实在灵活。

原本受到盈利低于攻击成本或是设备数量限制，而无法进行攻击的场景，由于攻击效率的提升和灵活的租用模式，现在均可进行攻击，真实环境中，大部分工作室基本都是固定攻击某个行业的某些厂商，同时关注营销活动，在合适的时机，利用设备的空闲剩余价值，“捎带”一些副业进行盈利。



图为：某云手机操作页面

1.3.3 中控

优化点：解决了传统群控因数据线传输屏幕数据和指令数据造成的设备数量限制问题。

手机设备中安装客户端，用户在PC端客户端上统一管理手机并向其下发命令，由网络传输后手机客户端执行模拟点击完成攻击。

1.3.4 云控

优化点：设备无需在同一地点，脚本命令存储在云端，团伙间交易脚本时无需发送源码，方便了脚本传播和管理大量手机

一个广域网版本的“中控”，操作者通过任意浏览器对手机进行管理和下达命令。

1.3.5 群控

优化点：早期的批量操作设备解决方案，在脚本开发上限制较多，为避免卡顿，设备数量限制在百台左右。

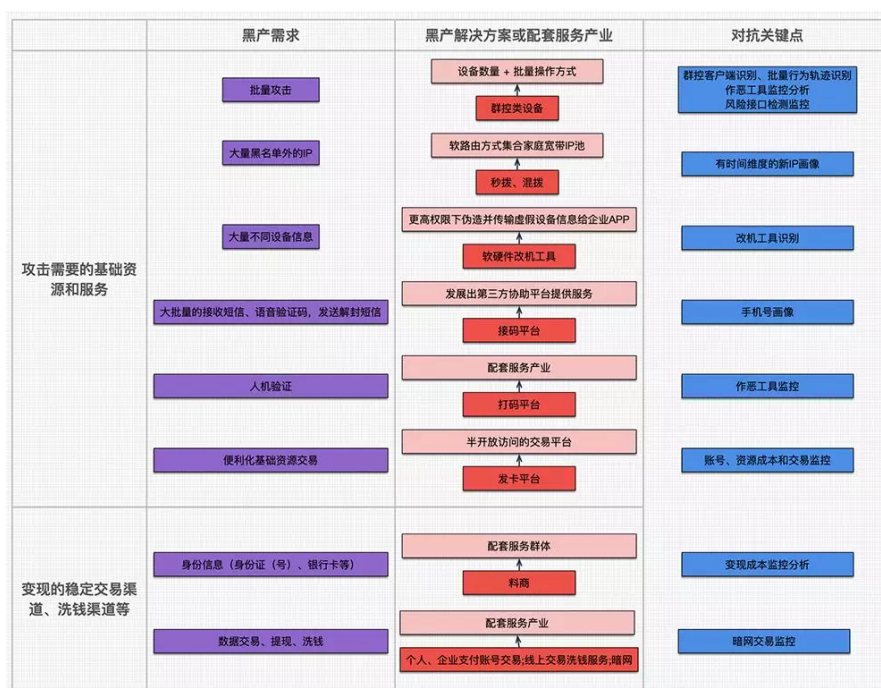
采用屏幕映射的方式将手机屏幕映射到电脑，通过集线器将手机与电脑通过数据线连接，从而传出屏幕内容和操作指令。

1.4 攻防建议

面对当今黑产这样产业化、专业化、团伙化和链条化的运作模式，攻防对抗将是企业与黑产双方不断厮杀成长的一场持久战。

企业可通过反欺诈情报（事前预防，事后根据攻击方法找到防护点）+欺诈数据标签（定位攻击流量）的综合对抗，填补认知盲区，打平信息差，了解对方的目标、攻击思路和策略。熟悉对方的作恶成本，了解对方发起攻击所需要的资源、时间、金钱成本、渠道门槛、对接的上下游以及通过攻击得到的营收等。在业务侧，综合审视自己的目标，对比双方资源、调整策略，定位到黑产的攻击账号、流量等，予以打击防护。

黑产以量取胜，但也因为如此，批量就一定有迹可循。黑产有庞大的上游基础资源供应，但同时也非常依赖这些资源，这些是产业链的关键结点，也同时是我们识别、打击和防护的有效结点。下图我们对黑产攻击方式给出了企业风控可以做的相应的对抗点的建议：



数据来源：威胁猎人



• 反欺诈情报——业务安全攻防中的隐性力量

从全产业链上下游视角出发的布控和收集的情报，可以作为风控策略的解释与支撑。同时欺诈情报如黑产舆情和趋势也能有效反馈企业风控策略的有效性，并帮助企业控制攻防成本。反欺诈情报一般包括：黑产准备攻击的接口、所涉及到的交易平台、攻击的目标接口、所利用的攻击工具、所涉及到的相关资源（手机号、IP）等。通过这些节点的布控，可以有效的在黑产资源准备时就及时发现风险，并了解黑产的攻击路径和逻辑，提前做好风控策略。

• 欺诈数据标签——高效落地的判别方案

不管黑产的技术上、设备上如何迭代，他们发起攻击时总绕不过一些基础的欺诈资源的储备，例如注册用的手机号和访问的IP。据我们统计，全网每日黑产发起的恶意注册攻击达到800W次，每日活跃欺诈手机号150W以上，平均每个手机号每日进行6次攻击。如果从黑产角度对其使用的基础资源进行监控，识别出企业业务场景下的黑产欺诈资源，则可以针对这些黑灰产做恶的虚假账号进行直接的拦截或降权。从黑产基础资源识别的风控方式，能够一定程度上降低风控的误判率并提高可解释性。

2. 黑产IP资源进化史

IP，作为互联网空间中最基础的身份标识，一直以来都是黑产与甲方争夺对抗最激烈的攻防点。

然而，在永安在线深耕业务安全领域数年的时间里，发现黑产技术迭代进化的速度令人咋舌，但是不少甲方却对黑产的研究和认知依旧停留在早些年的初级阶段。黑产发展迅速，而甲方对黑产的了解却停滞不前，必然造成在攻防过程中的信息不对称，防御难度加大，防守响应滞后，效率和效果大打折扣。

举个例子，对于黑产而言，“秒拨”早已不是一个新词，秒拨IP资源早已成为当下主流的黑产IP资源，可是，永安在线在与多个甲方客户沟通交流的过程中发现，很多在甲方做业务安全的学生对秒拨的概念一知半解，甚至完全不了解。

这个现象值得反思，秒拨在2014年前后已经是成熟的IP资源解决方案，到现在2019年，被广泛用于批量注册、投票、刷量等短时间内需要大量IP资源的风险场景，并且由于秒拨IP难以识别的特性，对当前互联网业务安全场景已造成巨大危害，但是很多安全行业的学生居然觉得这个东西很新鲜。

不论是在IP这个对抗点，还是在手机号、设备指纹、风险流量和行为等其他对抗点上，传统的【先被攻击】，然后【事后发现】，最后【补充规则】的被动式的对抗方式已经无法适应当前与黑产的攻防节奏，研究黑产、了解黑产、掌握黑产的最新技术和动向，才能把控更多主动权。

想打赢业务安全的战争，必须由“亡羊补牢”式的攻防形态向“未雨绸缪”式的攻防形态转型。

2.1 秒拨

自从甲方开始在IP层面根据一些简单的规则（如设定单位时间内IP的访问次数阈值、限制触发特定行为的IP等）做风控起，就正式向黑产在IP战场上宣战。

早期黑产主要是通过代理IP的方式绕过甲方的风控规则，售卖代理IP的网站便如雨后春笋般涌现。这些网站收集代理IP的方式主要利用高性能的服务器对全网进行扫描，扫描开放代理服务的服务器，或者是直接爬取其他代理网站的数据，收录有效代理IP和端口，以免免费或者付费的形式交付给用户。此方式最大的弊端是代理IP的有效性和数量无法把控，代理网站无法把控，用户更无法把控，这就非常影响黑产做自动化攻击的效率。也有黑产利用VPN绕过

甲方风控，VPN相对稳定，但是成本更高且有效IP数量有限，并不适用于黑产大规模批量化的攻击。

全网的代理IP数量相对有限，且早期代理服务一般都架设在数据中心的服务器上，不少甲方慢慢开始积累代理IP池，进一步打压了黑产使用代理IP的效果。

不少做业务安全的同学对黑产IP资源的认知就停留在了此处。然而不甘心的黑产开始做资源升级，研发出秒拨的技术。

通俗的讲，秒拨的底层思路就是利用国内家用宽带拨号上网（PPPoE）的原理，每一次断线重连就会获取一个新的IP。与时俱进的黑产掌握大量宽带线路资源，利用虚拟化和云计算的技术整体打包成了云服务，并利用ROS(软路由)对虚拟主机以及宽带资源做统一调配和管理。这种云服务交付给黑产用户其实就是云主机（俗称“秒拨机”），黑产用户可安装Windows或Linux系统，通过RDP、VNC或者SSH连接，部署自动断线重连切换IP以及攻击的工具后，便可发起攻击。

秒拨机web管理页面截图：

控制面板

云服务器信息/变更状态

转移服务器

预装操作系统

修改云服务器密码

返回用户区

欢迎您使用功能强大的控制面板

云服务器自助管理

产品类型:	拨号A型
在数据库中的状态:	正常
开通时间:	2019-
到期时间:	2019-
云服务器名:	
云服务器信息:	远程地址: 管理员:administrator密码: 拨号帐号: 密码1
在服务器上的状态:	正常运行中
更改状态:	[开机] [关机] [重启]
硬件情况:	实时CPU使用: 1% 内存上限: 512M 硬盘总大小: 15 G
已运行时间:	2876 分钟
唯一识别名GUID:	
实时截图:	

[返回用户区]

秒拨机桌面以及某拨号软件截图（黑产用户可在秒级切换IP）：

Administr... 系统重启.bat

计算机

内网高速下载中心

网络

Google Chrome

回收站

adsl重拨软件.exe

腾讯QQ

log_IP.txt

宽带连接

配置.ini

ADSL拨号软件 v1.3

拨号设置

网络连接: 宽带连接

宽带帐号:

宽带密码: *****

☐ 启用IP重复自动重拨号功能

清空IP

工作配置

断开时间(秒): 5

连接时间(秒): 5

停止

开始执行

拨号记录

2019-05-31 17:20:29	121.234
2019-05-31 17:20:42	113.222
2019-05-31 17:20:56	115.205
2019-05-31 17:21:8	117.95
2019-05-31 17:21:21	122.195
2019-05-31 17:21:33	36.62.1
2019-05-31 17:21:45	114.231
2019-05-31 17:22:4	122.245
2019-05-31 17:22:16	114.237
2019-05-31 17:22:28	27.31.
2019-05-31 17:22:41	61.145
2019-05-31 17:22:53	180.11
2019-05-31 17:23:6	106.11
2019-05-31 17:23:18	117.60
2019-05-31 17:23:30	117.95
2019-05-31 17:23:43	122.7
2019-05-31 17:23:56	117.95
2019-05-31 17:24:8	59.61.

断开时间请大于5秒! 10-23日更新 修复IP不显示的BUG, 请去"使用说明"或"内网下载中心"下载

友情提示: 距离下次拨号还有4

威胁猎人

下午 5:24

2019/5/31 星期五

- **IP池巨大**：假设某秒拨机上的宽带资源属于XX地区电信运营商，那么该秒拨机可拨到整个XX地区电信IP池中的IP，少则十万量级，多则百万量级；
- **秒拨IP难以识别**：因为秒拨IP和正常用户IP取自同一个IP池，秒拨IP的使用周期（通常在秒级或分钟级）结束后，大概率会流转 to 正常用户手中，所以区分秒拨IP和正常用户IP难度很大。

一台秒拨机上发现大量注册机以及其他黑产工具和资源:



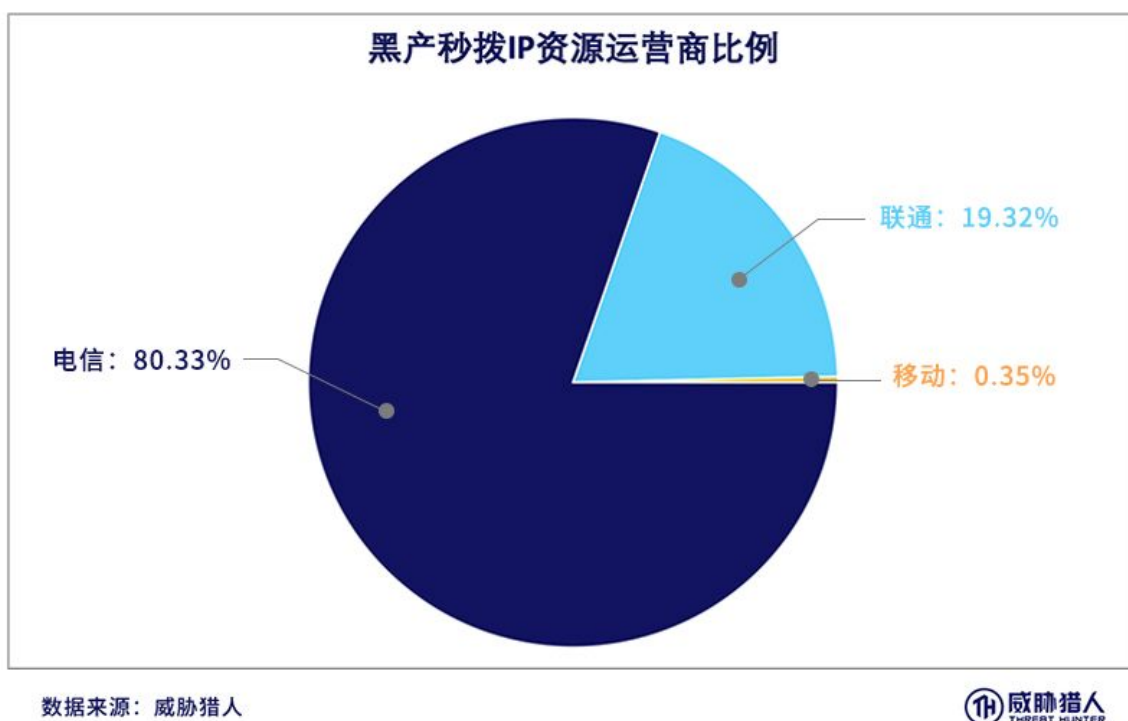
永安在线对市面上提供秒拨机的主流平台做了统计，其提供的秒拨IP可覆盖全国所有约300个城市。



黑产秒拨IP资源分布前十的省份为：

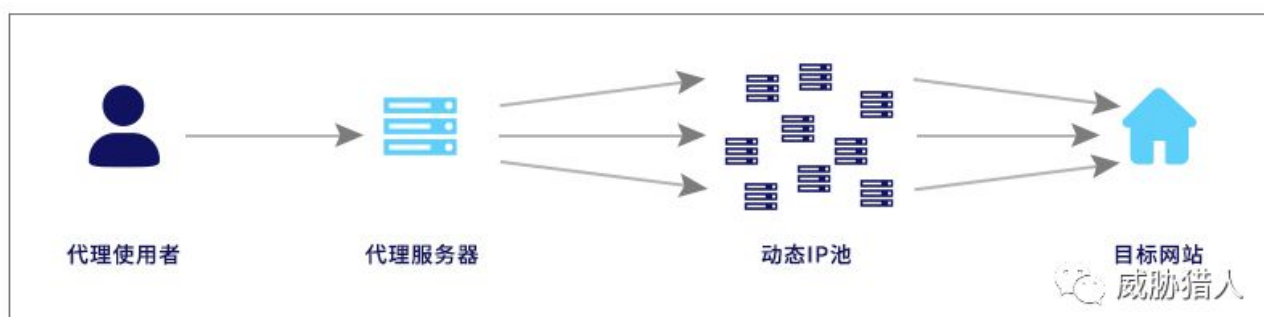


另外，黑产秒拨IP资源运营商比例分别为：

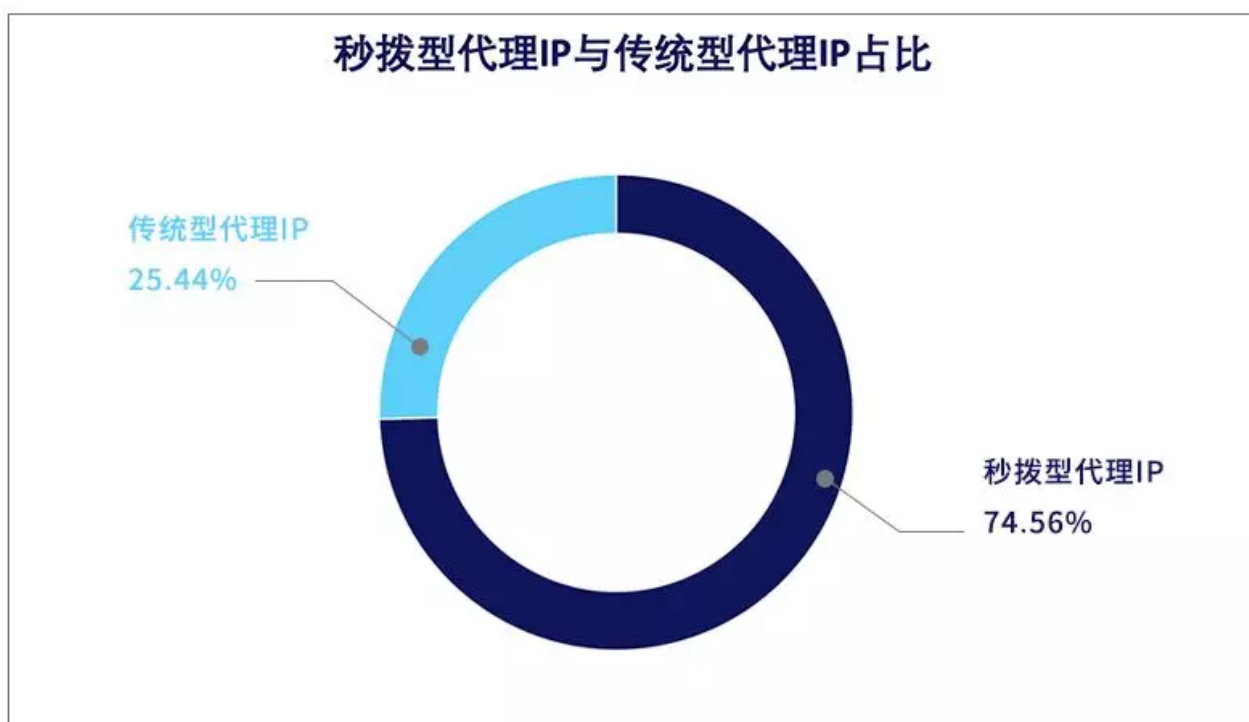


黑产还在不断扩大覆盖其秒拨IP资源的地域覆盖范围，甚至部分平台也可以提供美国、韩国。香港等非大陆IP资源。

另外，前文中提到过，早期黑产收集代理IP的方式是全网扫描，可用性无法保证。其实黑产早已把秒拨的技术应用于代理IP，黑产利用秒拨技术积蓄代理IP池，再提供给下游黑产用户，并且此类代理IP继承了秒拨IP的优势，一是IP池巨大，二是难以识别。秒拨型代理IP常见的实现方式是动态转发，如下图所示：



永安在线情报监测平台数据显示，当前黑产使用的代理IP资源中，秒拨型代理IP占74.56%，传统型代理IP仅占25.44%。甲方如果还想以积累IP池的传统方式与黑产对抗，必然会引入大量误报。



数据来源：威胁猎人



此外，使用代理平台提供的Windows/Android/iOS客户端，通过PPTP/LT2P等VPN协议，可把黑产终端直接变成“秒拨机”，大大提高了黑产作恶的便捷性。

2.2 攻防建议

总之，秒拨已然成为支撑黑产与甲方在IP层面攻防的核心技术，也是当下业务安全行业的痛点之一。文中提到秒拨的两个天然优势，对于黑产而言，是两道天然的屏障，但是给甲方在风险IP识别和判定上带来极大的难度。

当前形势下与黑产在IP层面上的对抗，依靠传统地积累IP威胁情报库的方式，根本无法直接应用和落地到业务侧，典型的使用效果是，对黑IP的检出率很高，对正常用户IP的误判率也很高。

所以，识别风险IP的核心依据应该是，**该IP是否当下被黑产持有，IP的黑产使用周期和时间有效性**这两个指标尤为重要，尤其是对于像家庭宽带IP、数据中心主机IP这种“非共享型”的IP。针对基站、专用出口等“共享型”的IP，由于单个IP背后会有大量用户，风控阈值应该相对更宽松，但是如果能够准确识别IP是否当下被黑产使用，也能提供很重要的参考价值。

永安在线长期致力于黑产IP资源的研究，旨在帮助甲方解决业务安全场景下风险IP的识别问题，并于近日实现突破，**通过对黑产ROS秒拨节点的布控，可实时监控和收集黑产当下使用的秒拨IP**。永安在线愿与各方共同交流与努力，一起攻克行业性技术难题。

3. 秒拨IP识别技术案例分析

IP是互联网最基础的身份标识，也是黑灰产业发展不可或缺的底层资源支撑。如果说IPv4是一颗星球，那IPv6就是一整个宇宙，它的地址空间接近无限。

目前我们所说的IP通常是指IPv4地址，这也是当前我们与黑产进行安全对抗的最激烈的攻防点之一。

IPv4由32个二进制位组成，空间里面有 2^{32} （约43亿）个地址，其中约有2.8亿的地址是为特殊用途所保留的。然而，随着地址不断被分配给终端用户，IPv4地址枯竭的问题也在随之产生。

这个情况刺激了作为当前唯一的长期解决方案的IPv6的推进。

和IPv4相比，IPv6由128个二进制位组成，拥有 2^{128} （约 3.4×10^{38} ）个地址，是IPv4的 7.9×10^{28} 倍，庞大的地址空间几乎接近无限，被十分形象的称为可以为全世界的每一粒沙子分配一个地址。

然福兮祸之所伏，IPv6的地址空间远超当前IPv4，也意味着黑灰产掌握的IP资源体量也将无限扩大，他们将有能力为每个恶意账号独立使用一个IP。以往在对抗过程中积累下的风控策略，具备的完备IPv4安全体系，在IPv6规模化普及后将面临新的挑战。

网络发展，安全先行。永安在线鬼谷实验室监测到的数据显示，目前已存在数据中心IPv6地址上发起的恶意机器流量，并且国外黑灰市场上早已出现IPv6代理资源，实验室推测，这在一定程度上与IPv6的普及度有关。当国内IPv6部署逐步展开，以此为基础的黑灰产攻击必顺势而来，值得注意的是，当前让业务方最头疼的黑产IP资源——秒拨，也悄然增加了对IPv6的支持。

3.1 黑灰产已经开始利用IPv6资源

由市场强大需求带动的IP资源发展，已经成为黑灰产业链上的重要环节，专门提供IP资源的黑灰产团伙也随之产生。

黑灰产的技术非常与时俱进，在与企业玩转“猫鼠游戏”的过程中攻击手段也有所升级。比如从早期的通过代理IP绕过风控规则的方式，到现在已经演化出“秒拨”“混拨”等，甲方的对抗策略也在IPv4的环境下也有相应的得到提升和积累。

然而，当IPv4开始向IPv6迁移，IP环境的变化不仅牵涉了网络设备、路由管理、IPv6协议栈的相应改变，IPv4下搭建的风控体系在迁移的过程也会面临改造和升级。

原本适用于IPv4的防护策略如果改造不及时，将会面临多大的风险？这是所有企业都需要考虑和面对的问题。比如：

- **海量地址扫描：**IPv6由128个二进制构成，这意味着，如果一个子网使用其中IPv6网络中的64位来分配IP，则子网的总容量，也就是可分配的IP数为2的64次方。假设遍历IPv4的全部地址需要一个小时。那么将这个子网下面的所有IP地址遍历一遍，将需要50万年...

- **黑名单库失效**：在IPv4环境下积累的大量黑IP数据，对黑产IP进行识别有显著的帮助。但是，当IPv6时代来临，接近无限的IP地址会对黑名单库造成强烈冲击，原本高效的识别机制，在IPv6环境下将接近“无效”。
- **未知下的误判**：IPv6部署的初级阶段，将面临IPv6地理位置、设备指纹等风险数据缺失的问题，从而导致无法准确判定IP性质，产生误判。
-

目前全球IPv6普及率达到23.97%，发达国家的IPv6普及率为25%，而全亚洲IPv6普及率达到27.13%，其中，中国的IPv6普及率达到了14.46%。以下是各大洲和发达国家以及中国的IPv6普及率统计结果：



随后，我们查看了永安在线监控平台捕获到的恶意机器流量，通过对资源进行分析，我们发现目前黑灰产掌握的主要IP资源中都存在IPv6的踪迹。

1) 代理

据调查，国外的代理平台早已存在出售IPv6代理的情况。由于当前IPv6普及率还较低，IPv6代理商并不是直接提供IPv6地址和端口，提供的依旧是IPv4和端口，通过类似6in4加IPsec的隧道协议，将IPv6数据包封装在IPv4数据包中。



我们对这些IPv6代理进行收集，分析其特征特点，发现其主要来自国外IDC机房。

	Proxy IP:PORT	168.2...094
IPv6	Login	61...V
	Password	vp...
	Type	HTTPS
	IPv6	2604:0180:...078d

而相比国外，国内并没有发现专门批量出售IPv6代理的平台，但是我们也捕获到一些国内IPv6代理样本，而且很有意思的是，国内的IPv6代理大部分源于国内教育网的IDC机房。

由于其教育网的性质，如果简单地将各个教育网IDC对应的IPv6段进行拦截，最直接的结果就是误伤很大部分的正常学生用户。

2) 秒拨

秒拨IP是黑灰产掌握的另一主要IP资源，并且，现在已有部分秒拨厂商开始支持并提供IPv6的服务。

我们对从秒拨机器上获取的IPv6地址进行分析，发现它的性质属于**国内家庭宽带**，利用拨号上网（PPPoE）的原理，每一次断线重连都会获取一个新的IP。和IPv4的秒拨性质类似，但比IPv4更具优势的地方在于，它的**IP池庞大到接近无限，并且IP地址更难以识别**的问题。

- **无限IP池**

假设某秒拨机器上的宽带资源属于XX地区电信运营商，那么该秒拨机可拨到整个XX地区电信IP池中的IP，在IPv4环境下具有少则十万多则百万的量级。而IPv6环境下，量级巨大，难以估计。我们对某一批IPv6地址进行重复性统计，**监测到的10万数据中几乎不存在重复的IPv6地址，而实际的IPv6秒拨池中，远不止这个数。这意味着，传统的利用IP黑名单库给IP打风险标签的方式将不再适用。**

- **秒拨IP难以识别**

另外，由于秒拨IP和正常用户IP存在于同一个IP池，每次断开连接，原本属于被黑产使用的秒拨IP，都有可能在下一次拨号的时候流入到正常用户手中，这会给秒拨IP和正常IP的区分带来非常大的难度。

3.2 攻防建议

发展基于IPv6的下一代互联网，看似取之不尽的IP资源的确为当前逐渐枯竭的IPv4带来了救赎，但不容忽视的也恰是“取之不尽”背后潜藏的安全隐患。从上述数据我们可以推测，黑灰产对IPv6的利用情况很大程度上和普及度相关。

由于大多数发达国家IPv6的普及度及采用度都处于高位，相应的也诞生了专门售卖IPv6代理的平台。目前，在我国大部分主流网站都尚未支持IPv6访问的情况下，黑灰产已经开始研习IPv6技术，利用IPv6资源。当我国IPv6部署规模紧随政策一步步落实和推进，IPv4不得不向IPv6转移的档口，如果企业的风控设施的改造和升级没有跟上部署的脚步，将会面临一段时间的安全防护的“空窗期”，黑灰产可以毫不费力的进入平台，兴风作浪，歌舞升平。

因此，未雨绸缪是企业应对风险的最佳手段。我们有理由相信，当越来越多的国内网站支持IPv6，并且功能性和稳定性趋于完善后，基于IPv4的攻防战场势必会向IPv6转移，对于所有

的技术和安全人员，在保障技术稳定升级的同时，安全性问题的考量同等重要。永安在线作为业务安全行业的先行者，已投入大量人力和资源在IPv6黑产资源的研究上，并开始积累实时IPv6风险数据，期望能帮助向IPv6迁移的厂商解决预想不到的安全问题。

4. 新工具“IP魔盒”案例分析

众所周知，IP资源是黑产进行规模化攻击的核心资源，在永安在线的过往报告中大量讨论了黑产为了绕过IP检测，使用代理IP、秒拨IP等技术进行攻击。

根据永安在线长期的研究，得知这类IP本质上还是家庭宽带、数据中心等IP，通过一定的技术手段，在一定时间内都可以将IP和设备进行关联标记。

但随着攻防对抗的升级，黑产将视线转移到更为隐蔽的基站IP上。近日，永安在线发现一款能让PC设备使用基站IP的工具，黑产称它为“IP魔盒”。

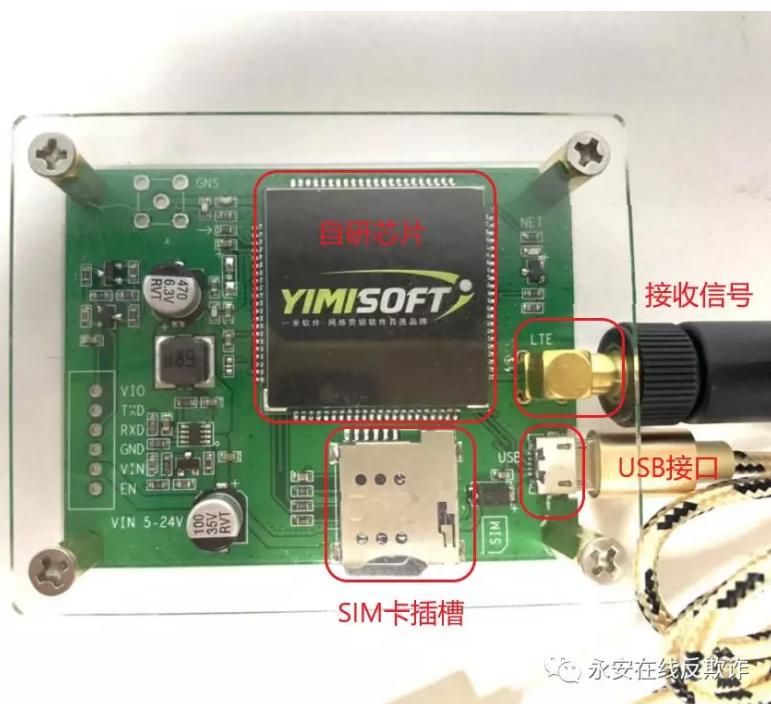
4.1 IP魔盒

IP魔盒一款比手掌还小的硬件盒子，USB接入后，可以使普通PC拥有基站IP。

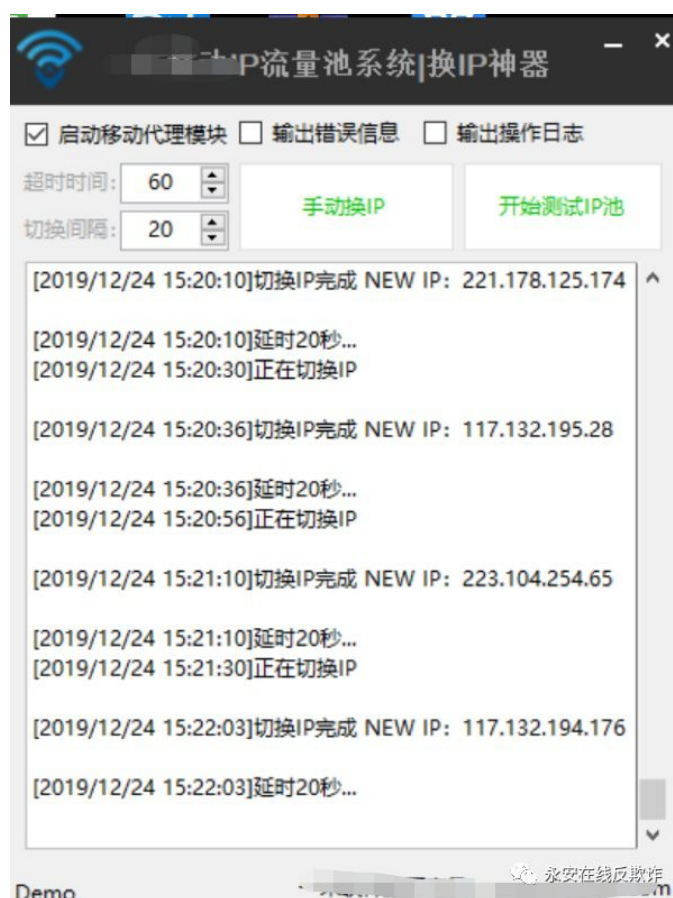
它主板设计简单，使用方便，不仅只兼容国内电信，移动，联通三网通的sim卡，也支持海外sim卡。它通过自研芯片模块组的USB接口与个人主机连接，让PC可以实现4G上网。接着下载模拟开关飞行模式的脚本和安装相应驱动后，即可进行切换IP。



图为：IP魔盒设备



图为：IP魔盒芯片



图为：PC上的IP魔盒控制端

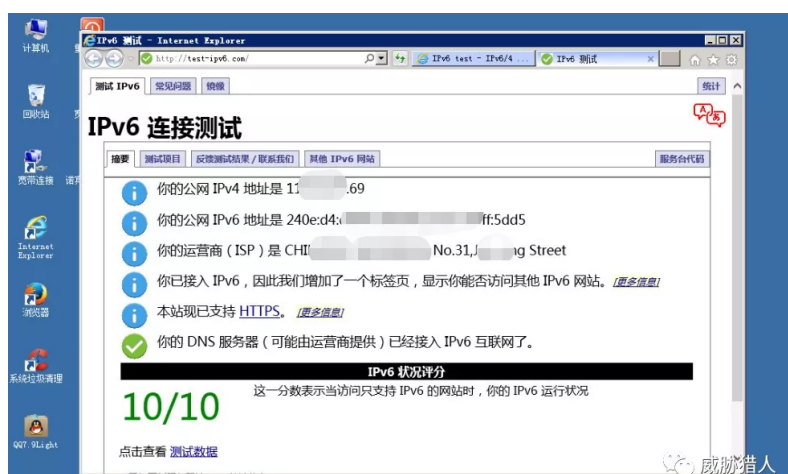
而IP魔盒配套使用的物联网卡，更是价格便宜，使用方便。

我们总结了IP魔盒拥有以下特征：

- 1) 关联用户多：一个基站IP背后会关联着大量的用户群体，如果对IP进行拦截，极易误杀正常用户，影响用户体验，导致用户流失。
- 2) 切换IP简单：仅需要通过打开关闭飞行模式，即可实现IP切换。
- 3) 成本较低：据我们统计一般全国物联网卡，开卡价格为4-6元，10G流量价格仅需要15元。
- 4) 海量IP池：经测试一张全国物联网卡可以获取至少17个段的IP，且分布在不同的地区。

因为IP魔盒获取IP的特殊方式，它在IP量、攻击效率、价格成本、检测方式、部署成本各个方面都大大优于秒拨IP和代理IP，下表为对比结果：

	IP 魔盒	秒拨 IP	代理 IP
IP 量	利用的是真实运营商移动 IP，短时间内可以随意切换任意 IP。	拥有海量家庭宽带 IP，短时间内可切换 IP 取决于 ROS 的 IP 池数量。	IP 量有限，通常一家供应商的 IP 池在 1~2 万。
攻击效率	使用 4G 网络，网络稳定，带宽高。	采用 VPS 的方式使用。随着使用者增多，带宽和机器会不稳定波动。	极不稳定，大部分代理 IP 提供商采用的 IP 扫描和爬取的方式获得。IP 有效期在 5 分钟。
价格成本	硬件盒子：900 元 物联网卡：4-6 元/张 流量价格：10G/8~15/月。	2M 带宽：50~200 元/月	10000IP：100 元/月
检测方式	真实运营商基站 IP，背后关联大量真实用户，只可对风险 IP 进行标记。	可对短时间内的风险 IP 进行标记拦截。	IP 量少，通过聚类方式容易检测。
部署成本	安装脚本和驱动即可使用。飞行模式切换获取新 IP。	登录到 VPS 进行操作，受限于 VPS 性能。	通过 API 编写代码对接。 永安在线反欺诈



图为：利用秒拨测试IPv6支持情况

实验室通过IPv6对国内的各类主流网站进行测试，发现大部分的厂商并没有开始支持IPv6访问。少部分支持IPv6的厂商，也仅是支持主网可以通过IPv6进行访问，但网页加载的速率，以及访问链接的稳定程度就显得有点差强人意。一旦需要涉及到用户登陆或者其他用户操作的时候，就会经常出现访问失败或者登陆超时的情况。而国外支持IPv6访问的网站不论在稳定性和响应速率，还是支持用户相关的操作上，都比国内情况好很多。

5. 定制ROM改机案例分析

改机是黑产团伙大规模作恶所依赖的重要技术手段。通过改机，黑产可以批量伪造新设备，进而绕过甲方的业务风控。因此围绕改机展开的攻与防，是我们跟黑灰产对抗的重点研究工作之一。过去几年，黑产改机的手段主要有安卓模拟器、改机工具、应用多开/分身。

通过Karma业务情报监测平台，我们发现黑产团伙从去年开始使用一种新的手段，即定制ROM的方式来实现改机，这种改机技术更加底层，更加难以检测，目前技术也愈发成熟。经过一段时间的深入研究，我们在前段时间升级了设备风险SDK，全面支持检测定制ROM改机。

5.1定制ROM改机的技术原理

简单来说就是通过修改Android系统源代码，在底层直接修改并返回设备参数。这种修改是全局的，即可以对所有的应用进程和shell进程都生效。

5.1.1 修改机型信息

我们以修改机型信息为例，获取机型信息大多会调用_system_property_get这个函数，位于/system/lib/libc.so这个系统库中。在定制rom该机的设备上，该函数代码如下：

```
1 int fastcall system_property_get(int a1, BYTE *a2)
2 {
3     _BYTE *buffer1; // r4
4     const char *key; // r5
5     int result; // r0
6     _DWORD *v5; // r0
7
8     buffer1 = a2;
9     key = (const char *)a1;
10    if ( !shouldGjInLibc() )
11        goto LABEL_15;
12    if ( !_j_strcmp((int)"init.svc.mtpd", (int)key) )
13    {
14        LABEL_11:
15        result = 0; rom作者新增的代码，原本android官方没有这些
16        *buffer1 = 0;
17        return result;
18    }
19    if ( !_j_strcmp((int)"sys.usb.config", (int)key) || !_j_strcmp((int)"sys.usb.state", (int)key) )
20    {
21        buffer1[2] = 112;
22        *(_DWORD *)buffer1 = 29805;
23        buffer1[3] = 0;
24        return 3;
25    }
26    if ( !_j_strcmp((int)"persist.sys.usb.config", (int)key) )
27    {
28        LABEL_15:
29        if ( !isWgProp((int)key) )
30            return wgzs_property_get(key, buffer1); 判断是否是自定义的属性，如果是调用自定的属性获取函数，
31        v5 = ( _DWORD *)_j__system_property_find(key); 获取属性值。这段代码也是作者新增的
32        if ( v5 )
33            return _j__system_property_read(v5, 0, (int)buffer1);
34        goto LABEL_11; 非自定义属性获取
35    }
36    *(_DWORD *)buffer1 = 0x656E666E;
37    buffer1[4] = 0;
38    return 4;
39 }
```

可以看到定制rom的开发者对函数做了修改，添加了自己的代码逻辑。如果在改机工具中自定义了某个属性，则该属性值的获取不走系统默认的读取函数，转而执行工具定制的读取函数。同时，我们发现开发者对init进程做了深度定制，最终是在init中修改了机型信息。

5.1.2 修改IMEI

获取IMEI信息通常会调用getDeviceId函数。这是一个phone服务的IPC调用，响应代码位于：packages/services/Telephony/src/com/android/phone/PhoneInterfaceManager.java中，如下所示：



可以看到返回IMEI值，调用的是phone.getDeviceId函数，进一步跟进其代码，如下所示：

```
public String getDeviceId() {
    String mImei2 = this.mImei;
    if (WgzsUtil.shouldG3InService(Binder.getCallingUid())) {
        Log.d("PhoneHook", "call getDeviceId and should g3");
        return getHookValue("IMEI");
    } else if (isPhoneTypeGsm() || ((CarrierConfigManager) this.mContext.getSystemService("carrier_config")).getConfigForSubId(getSubId()).getBoolean("force_imei_bool")) {
        return mImei2;
    } else {
        String id = getMeid();
        if (id != null && !id.matches("^@*$")) {
            return id;
        }
        loge("getDeviceId(): MEID is not initialized use ESN");
        return getEsn();
    }
}
```

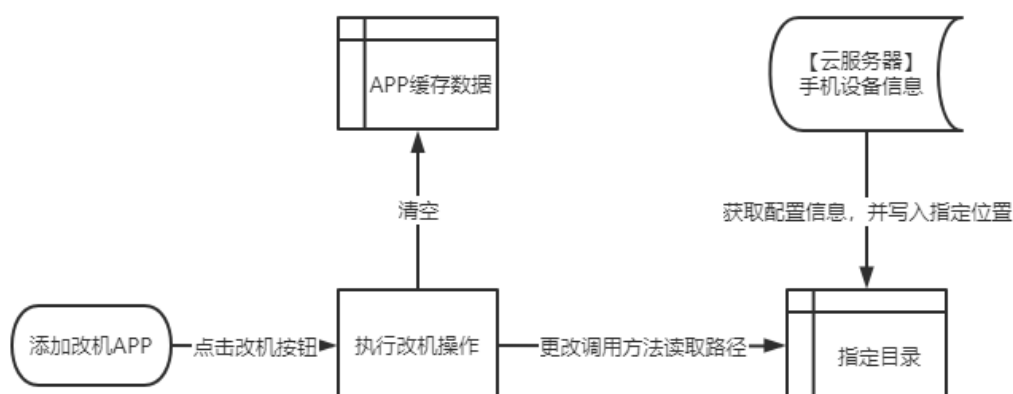
可以看到，根据IPC调用发起方的UID(可以看作一个用的唯一标识)，来判断是否需要修改IMEI。如果是，则调用getHookValue返回伪造的IMEI。为了方便使用，作者提供了设置接口，可以在使用前设置哪些应用需要修改IMEI。

5.2 定制ROM改机的使用

由于定制ROM改机直接修改Andorid源代码，改机的对象是真实设备，对应用本身没有任何侵入行为，所以难以被检测，而且改机效果非常稳定。此外，定制ROM改机的使用也非常方便：

- 1) 可镜像备份机型数据环境至云服务器，方便账号对应的设备环境管理；
- 2) 打通系统调试接口，方便自动化脚本编写、降低开发成本；
- 3) 傻瓜式一键式操作，完成设备信息修改、设备数据恢复。

定制ROM改机运行流程如下图所示：



基于Karma业务情报监测平台的情报数据，引流是当前定制ROM主要的使用场景之一。黑产从业人员通过定制ROM改机，轻松实现了设备的重复利用，再结合定制脚本进行批量化自动化的引流操作。



5.3 定制ROM改机的检测

检测其他改机技术的攻防平面，很难应用到定制ROM改机。因此需要在深入分析定制ROM改机工具的基础上，结合工具的实际运行原理和运行过程，寻找到新的攻防平面。目前我们对于几款活跃的定制ROM改机工具，都找到了工具难以反制的攻防平面，并在之上定义了针对每款工具的检测逻辑。我们的设备风险SDK，也第一时间进行了升级。

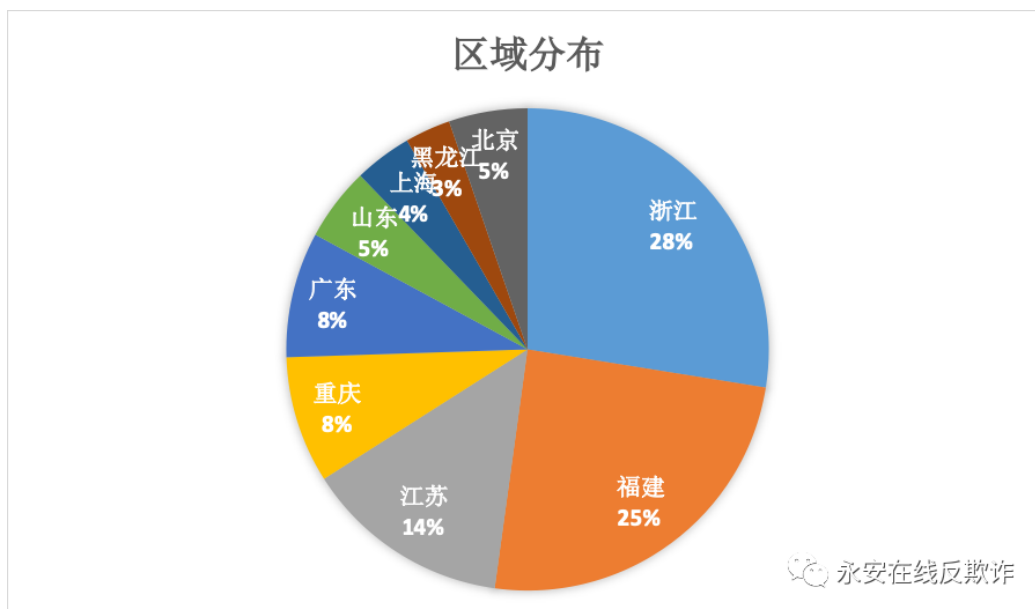
当然，与黑产的攻防，始终是一个持续对抗的过程。如果仅仅依赖一成不变的防御机制，最终也会有被破解的一天。尤其在大多时刻，防守方相比于攻击方会更加被动，因此需要建立发现问题到快速解决问题的闭环，从而尽量降低业务遭受的损失。

6. 黑产攻击流程自动化体系

对于黑产而言，他们会想尽一切办法，来不断降低攻击成本，提高攻击效率，自动化攻击便是其中的关键方法之一。

当前的黑灰产业链条中，从提供黑产资源的上游，到利用黑产资源发起攻击的下游，已经形成了一套低耦合，高自动化的完整生态。基于永安在线业务情报监测平台近期捕获到的网络黑灰产情报，我们对符合自动化攻击特征的黑产数据、行为以及技术原理做了分析，并尽量展示其全貌。

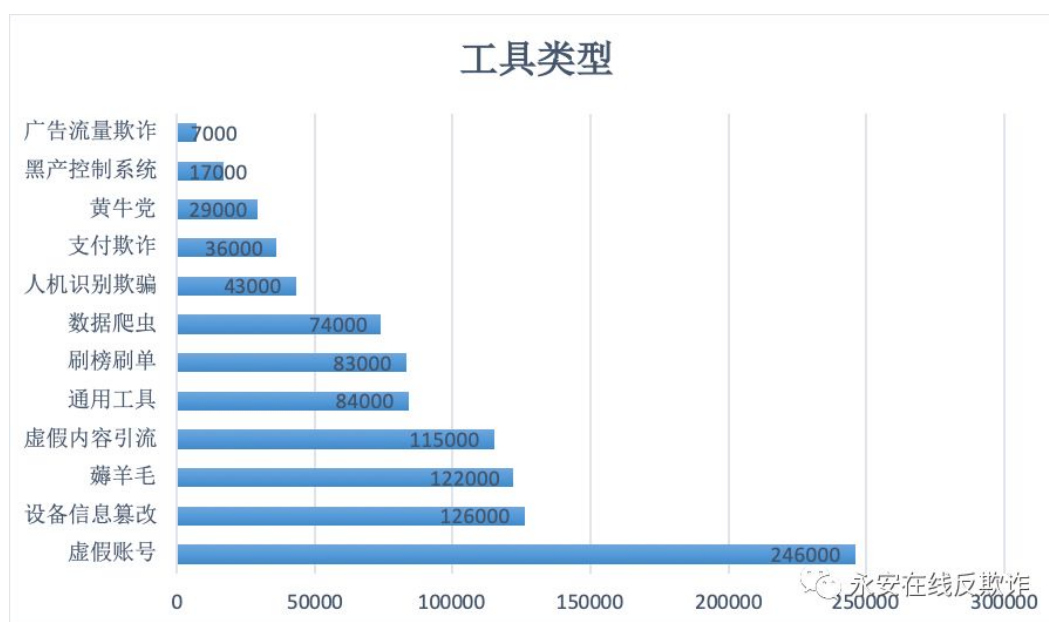
从攻击者地域分布来看，经济发达的沿海地区，如浙江、福建、江苏、广东等，自动化攻击的比例也更高：



从被攻击的行业分布来看，黑产可以规模化获益的O2O、电商、短视频等行业是黑产自动化攻击的重灾区：



从攻击行为来看，批量注册，批量薅羊毛，刷量，刷单，引流等，往往需要操控大量的账号，因此对自动化攻击的依赖性更强：



6.1 黑产资源高度集成自动化攻击流程

我们在以前的报告中，有详细讲述过网络黑灰产对厂商业务发起攻击需要的各种资源以及提供资源的平台，包括提供手机号资源的接码平台，提供账号资源的发卡平台，提供IP资源的代理IP网站和秒拨平台，提供设备资源和设备管理的群控/云控/箱控等。为了便于使用，这些资源平台提供了多种方式，黑产下游在进行自动化攻击的过程中可以无缝集成和使用。

6.1.1 API接口

黑产资源平台为了方便，最典型的方式的是提供API接口，这样便可以在自动化脚本或程序中直接调用。以接码平台为例，提供的API接口主要有两个，取手机号和取验证码。其中取手机号的接口一般定义如下：

`http://api.xxxxxx.com/api/do.php?action=getPhone`

参数action=getPhone表示获取手机号，此外还需要通过参数sid来指定项目，即手机号要注册的产品或业务。有些产品对于新用户注册管控比较严格，可以通过参数exclude来排除虚拟运营商的号段；有些活动只针对部分区域，比如某个产品在成都举行的拉新活动，可以通过参数location来指定获取归属地在成都的手机号。

获取验证码的接口一般定义如下：

`http://api.xxxxxx.com/api/do.php?action=getMessage`

参数action=getPhone表示获取验证码，此外也需要通过参数sid来指定项目。返回的数据格式一般为：1|短信内容，1表示成功，短信内容里面包含了验证码，通过简单的字符串匹配或正则表达式即可提取出验证码，然后进行注册。

【小技巧】 由于各个接码平台API接口除了域名外，参数格式都大同小异，所以可以通过定义一些正则表达式，从流量中（比如我们的蜜罐流量）捕获接码平台的API接口访问流量，从而可以大致掌握全网的接码平台数量和规模。

再以代理IP网站为例，基本上也都提供API接口，相比接码平台的API接口，使用起来更加简单，如下图所示，是一个代理IP网站提供的API接口说明：

返回示例

```
{
  "ERRORCODE":"0",
  "RESULT":[
    {"port":"43617","ip":"222.85.5.118"},
    {"port":"43569","ip":"180.122.20.108"},
    {"port":"20443","ip":"221.230.254.73"}
  ]
}
```

使用说明

- * 生成API链接，调用HTTP GET请求即可返回所需的IP结果
- * 可以直接按照以下格式组装所需的API链接:<http://api.greatrecharge.com/greatip?spiderId=xx&orderno=xx&returnType=2&count=xx>
- * 动态白名单添加接口:http://www.ipagent.com/newWhiteList/update3-Order?orderno=**&ip=**&spiderId=**

只需要调用一个API接口，返回的数据是json格式，可以直接解析出IP地址和端口。

很多厂商为了对抗自动化攻击，往往会在业务流程中接入验证码，从而进行人机识别。相应的，网络黑灰产把验证码的自动识别也集成到了自动化攻击中。提供验证码自动识别功能的平台我们一般称为打码平台或过码平台，无论是图片验证码、滑动验证码还是一些复杂验证码，这些平台都提供了用于绕过这些验证码的API接口。如下图是其中一个过码平台，绕过某验证码的API使用说明：

```
POST /api/gateway.html HTTP/1.1
Host: api.ddocr.com
User-Agent: Mozilla/5.0 Chrome/77.0.3865.120 Safari/537.36
Accept: text/html;
Content-Type: application/x-www-form-urlencoded;

wtype=geetest&secretkey=用户密钥&gt=xxxxxxx&referer=http://www.baidu.com&challenge=xxxxxxx&supporttype=3

请求成功返回
{
  "status": 0,
  "msg": "识别成功",
  "data": {
    "challenge": "de8a5eac0ffae9d764a72e736cf3ece6k"
    "validate": "aaf189b2c9abd93fd8606d7b7fc63893"
  }
}

失败返回
{
  "status": -1,
  "msg": "识别失败",
  "reasonCode": 101
}
```

永安在线反欺诈

子程序名	返回值类型	公开	易包	备注	
极验识别	文本型				
参数名	类型	参考	可空	数组	备注
gt	文本型				所在网站极验的gt值
referer	文本型				所在的页面来源地址
challenge	文本型		✓		通过请求目标站配置项获取，每次获取到的challenge仅能使用一次。如网站为极验感知此参数可不填，比如拉钩

变量名	类型	静态	数组	备注
url	文本型			
secretkey	文本型			后台的接口访问密钥
body	文本型			
supporttype	文本型			
response	文本型			
http	WinHttp			
ip	文本型			

```
url = "http://api.ddocr.com/api/gateway.jsonp"
' 这里替换为你的密钥，这个为必填
secretkey = "XXXXXXXXXXXXXXXXXXXX"
supporttype = " " ' 如果遇到特殊图像传supporttype=3 注意特殊图像比较贵 识别成功则扣30点
ip = " " ' 如果网站ip，需要使用自己的ip的话传此参数，一般情况下不需要
body = "wtype=geetest&secretkey=" + secretkey + "&gt=" + gt + "&referer=" + referer + "&challenge=" + challenge + "&supporttype=" + supporttype + "&ip=" + ip
http.Auto (真)
' 设置60秒超时
http.SetTimeouts (3000, 3000, 3000, 60000)
http.Open ("POST", url)
http.Send (body)
response = http.GetResponseTextVB6ToAnsi ()
' 调试输出 (response)
返回 (response)
```

永安在线反欺诈

```
public class GeetestRecognition {
    private static final String api = "http://api.ddocr.com/api/gateway.jsonp";
    //这里为您的后台的首页的，开发者信息的接口密钥
    private static final String secretkey = "";

    /**
     * @param gt 所在网站极验的gt值
     * @param referer 来源页面地址
     * @param challenge 通过请求目标站配置项获取，每次获取到的challenge仅能使用一次。如网站为极验感知此参数可不填，比如拉钩
     * @return
     */
    public static String recognition(String gt,String referer,String challenge){
        StringBuffer body = new StringBuffer();
        body.append("wtype=geetest&secretkey=").append(secretkey);
        body.append("&gt=").append(gt).append("&referer=").append(referer);
        body.append("&challenge=").append(challenge==null?"":challenge);
        //如果想使用自己的代理ip传进来即可
        body.append("&ip=");
        body.append("&proxyuser=");
        body.append("&proxypwd=");
        body.append("&supporttype="); //如果遇到特殊图片，请传3，其他则不用
        String resp = HttpUtils.getInstance().post(api, body.toString());
        return resp;
    }
}
```

永安在线反欺诈

```
<?php
require_once 'curl.func.php';

$appkey = 'your_appkey_here';//你的appkey
$pic = base64_encode(file_get_contents('11.jpg')); //验证码图片
$type = 'n4'; //图片类型
$url = "https://api.jisuapi.com/captcha/recognize?appkey=$appkey";

$post = array(
    'pic'=>$pic,
    'type'=>$type
);
$result = curlOpen($url, array('post'=>$post));
$jsonarr = json_decode($result, true);

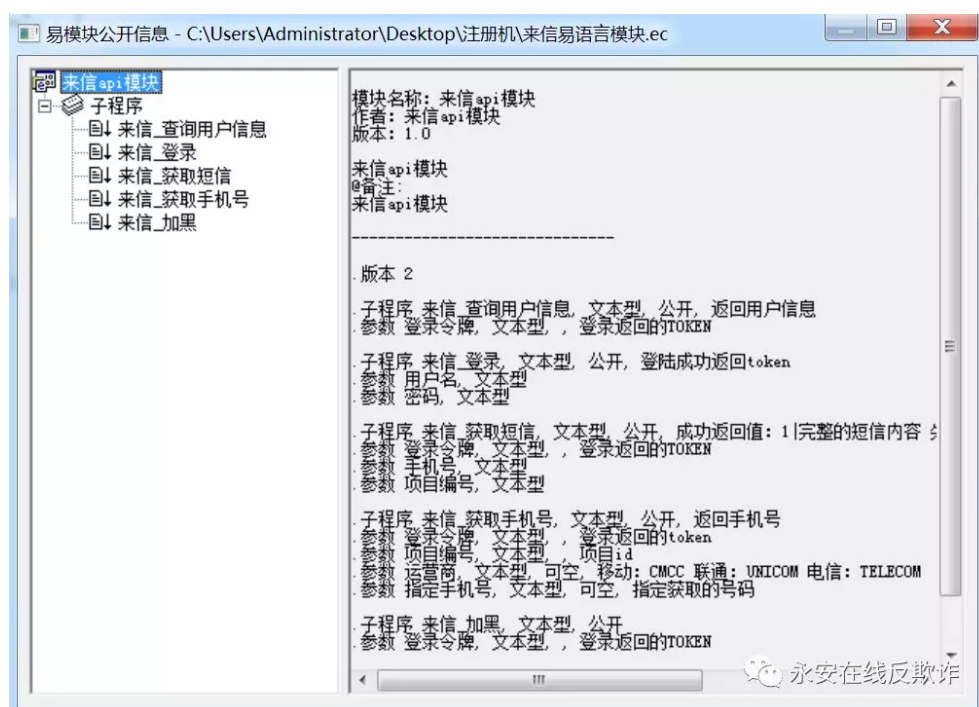
if($jsonarr['status'] != 0)
{
    echo $jsonarr['msg'];
    exit();
}

$result = $jsonarr['result'];
echo $result['type'].' ' . $result['code'];
```

永安在线反欺诈

6.1.2 功能模块

对于黑灰产实现自动化攻击来说，API接口已经足够方便了，但黑灰产也追求“精益求精”，于是有了另外一种更为方便的方式，直接提供封装好了的功能模块。由于黑灰产工具软件绝大多数都采用易语言编写，因此大多提供的是易语言封装的模块。我们还是以接码平台为例，下图是一个接码平台的易语言模块(.ec)导出信息，可以看到需要的功能都已经封装好了：



我们以一款近期发现的用易语言编写的自动化薅羊毛工具为例，其跟接码相关的代码只需要寥寥数行代码：

1) 登录接码平台，获取手机号：

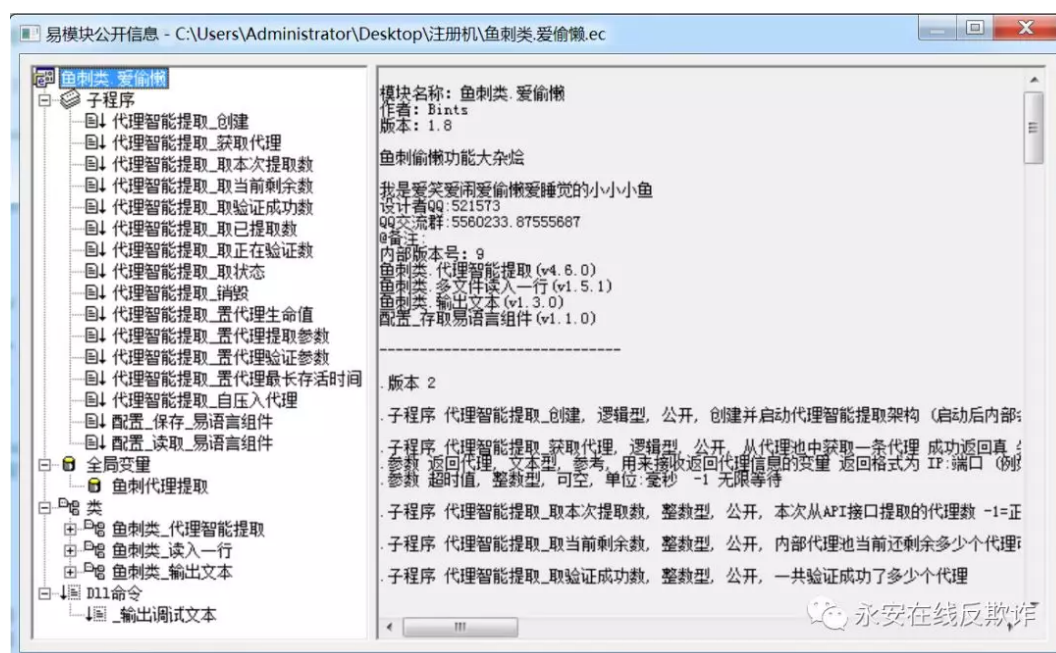
```
token = 登录( )
日志_输出(正在登录接码平台)
如果真 (token = "")
    日志_输出("登录失败", )
    返回 0
判断循环首 (真)
    延时 (2000)
    日志_输出("正在获取手机号", )
    手机号 = 获取手机号(token, "1309", , )
    如果真 (手机号 = "")
        日志_输出("获取手机号失败", )
        返回 0
    日志_输出("手机号:" + 手机号, )
```

2) 获取验证码：

```
日志_输出 ("发送验证码", )
计次循环首 (0)
短信内容 = 取短信 (token, 手机号, "1309")
如果真 (文本_取中间文本 (短信内容, "1|", , 假) > 0)
跳出循环 0
延时 (3000)
计次循环尾 0
验证码 = 文本_取出中间文本 (短信内容, "验证码是 ", ", 10分钟内", , )
如果真 (验证码 = "")
日志_输出 ("获取不了短信验证码, 重新注册", )
到循环尾 0
```

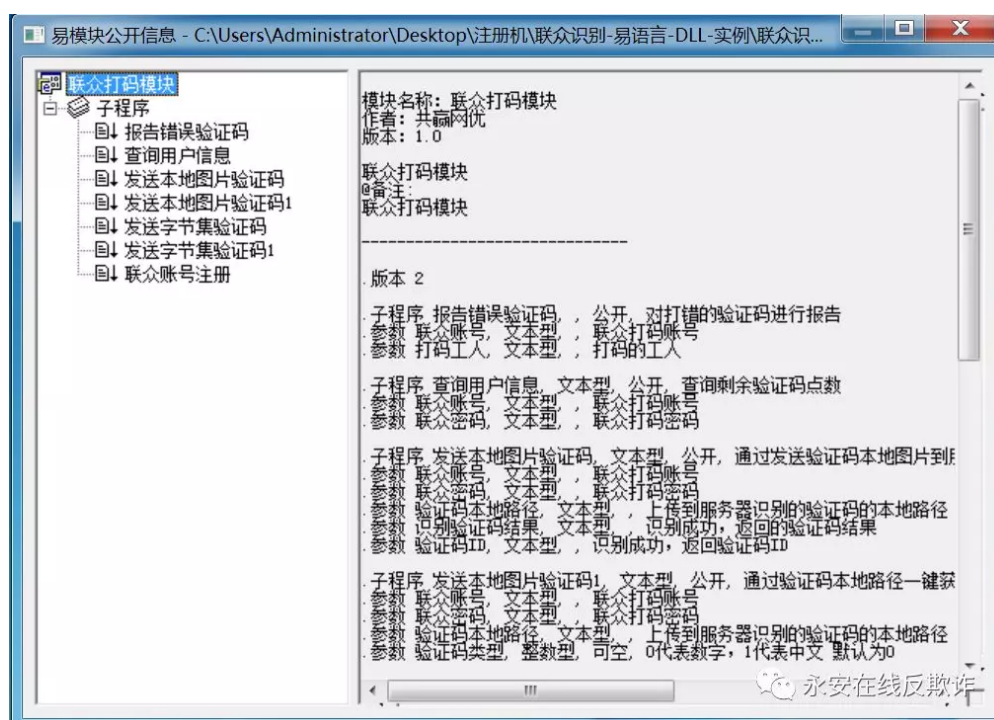
永安在线反欺诈

对于代理IP的使用，也有封装好了的功能模块可以使用，如下图所示：

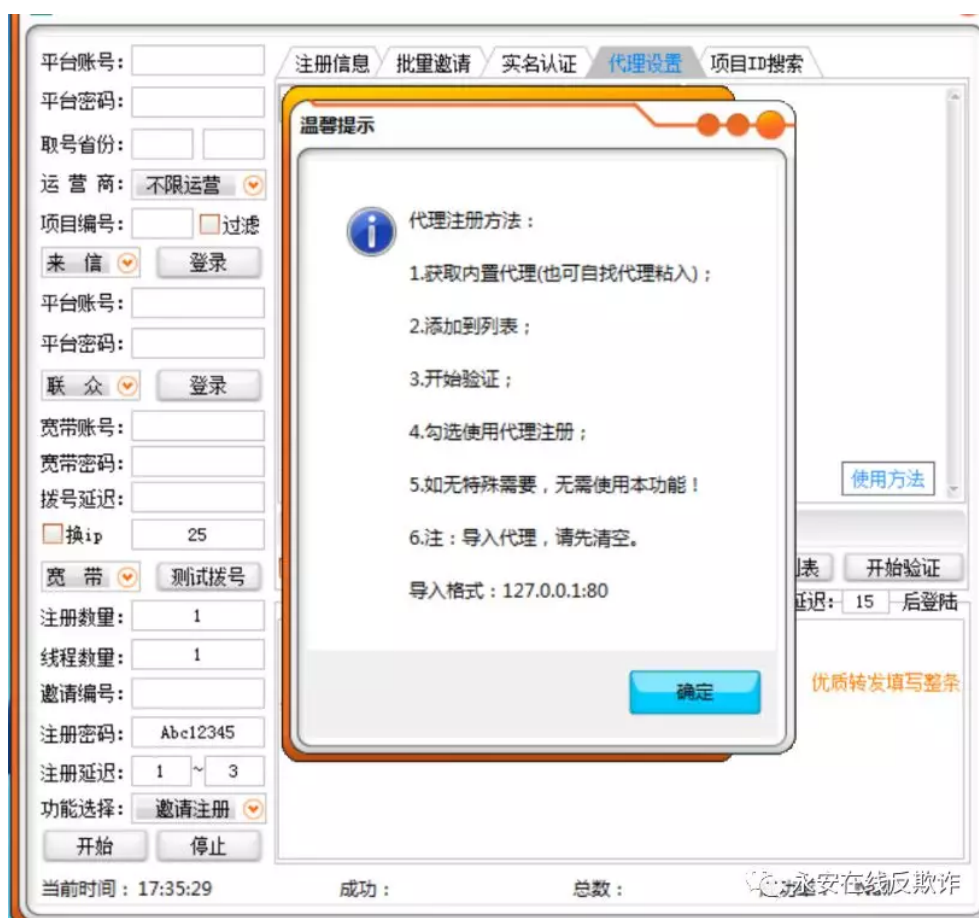


除了提取代理IP之外，还提供了验证代理IP有效性的功能，使用者无需再用其他工具或自行编写代码去验证代理IP的有效性，不可不谓“贴心”。

部分打码平台也提供了易语言的功能模块，如下图所示：



下图这个用易语言编写的自动化注册机工具，可以说是一个典型的“集大成者”，包括接码平台，打码平台，宽带拨号，代理IP等黑产资源的功能模块，都集成到了工具中。只需要在界面上填入各个黑产资源平台的账号密码，并进行一些简单的配置，即可一键进行所有的自动化攻击流程。



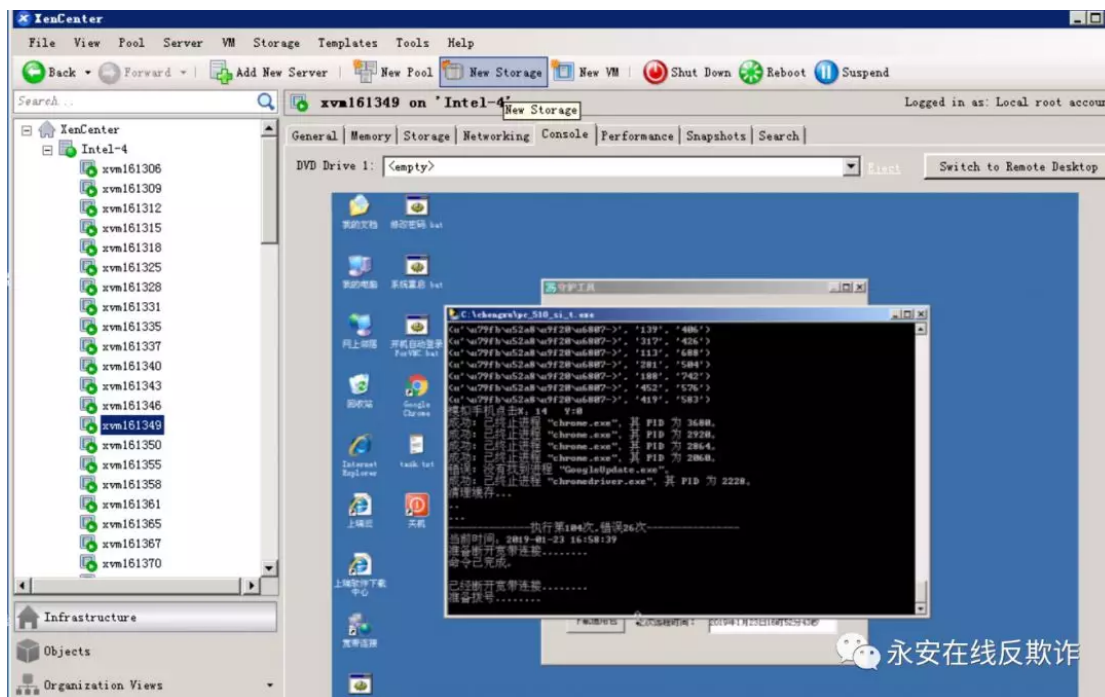
6.1.3 提供环境

对于提供IP资源的平台来说，秒拨相比于代理IP，除了价格更低，可用的IP资源更多之外，对于自动化攻击来说，使用更方便：不需要在脚本或程序嵌入API接口或功能模块，直接将自动化攻击运行在秒拨提供的环境下即可。有两种方式：

1) 启动秒拨的客户端程序，开启自动拨号，然后执行自动化攻击：

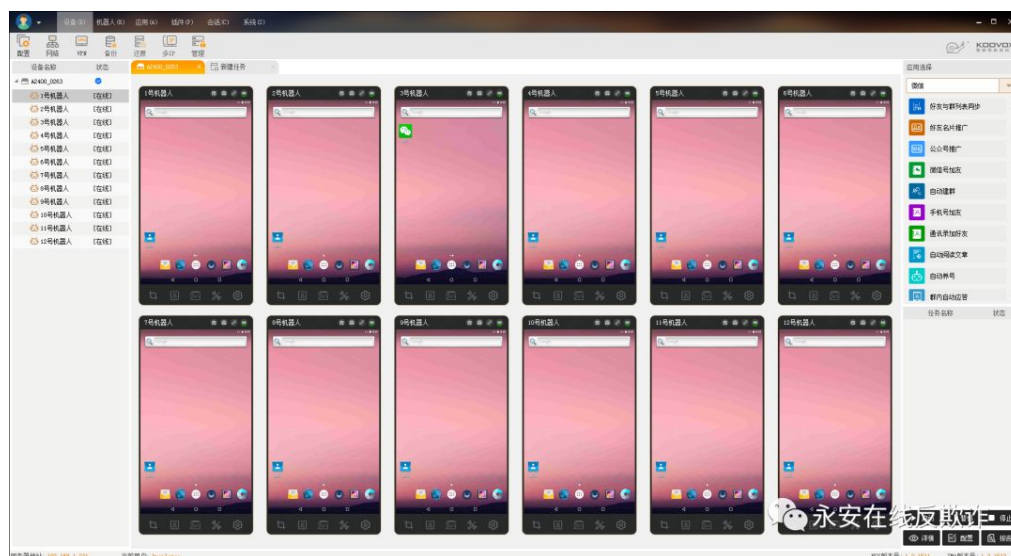


2) 将自动化攻击的脚本或程序运行在秒拨VPS中，秒拨VPS提供自动拨号的功能：



6.1.4 集成系统

黑产设备资源的提供者，我们可以理解为黑灰产行业的硬件厂商。近年来手机硬件厂商在不断提升硬件能力之外，也在不断发力软件市场。比如在手机系统中直接集成了自己的应用商店，浏览器，手机管理软件等，用户不需要再去额外安装。类似的，用于黑产设备提供者来说，他们也不再是单纯的提供硬件设备，而是将黑灰产完成自动化攻击所需要的各种资源，都集成到了里面。而在对外包装上，往往会打着“一站式营销”，“私域流量营销”等宣传语。

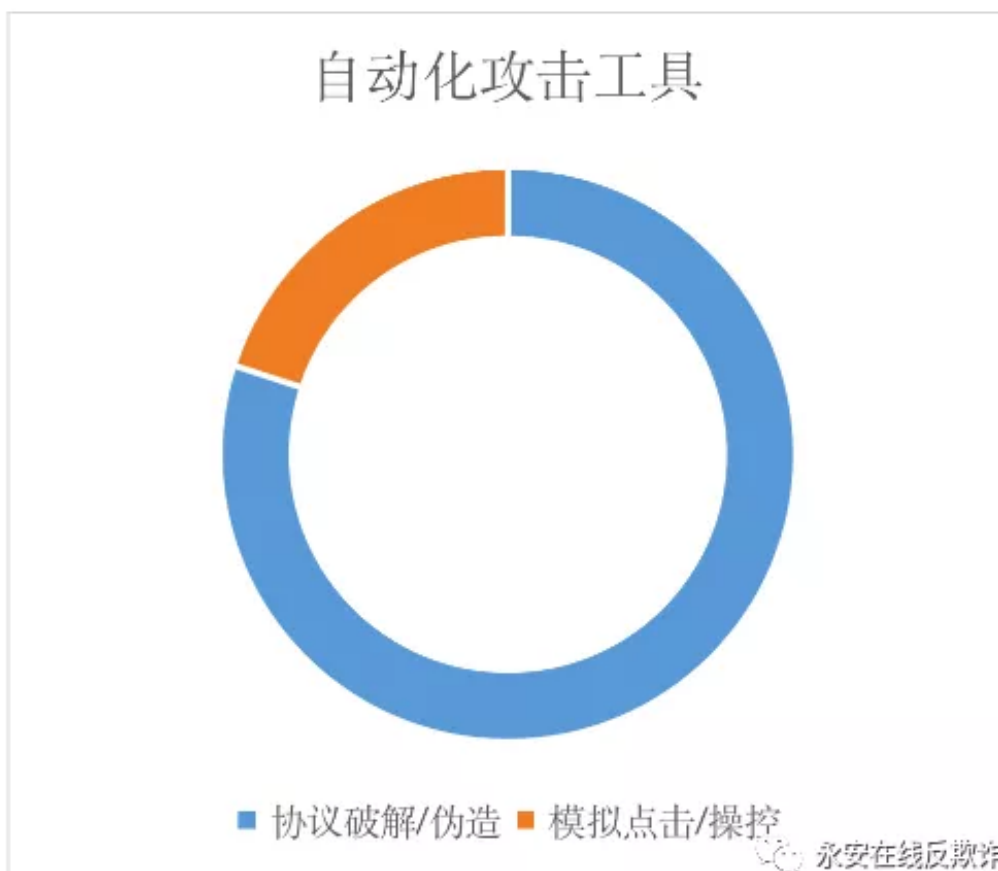


我们以某款箱式群控为例，从下图可以直接看到，这款箱控工具已经内置了以下一些功能：

- 1) VPN拨号功能，可以方便的切换IP；
- 2) 虚拟定位功能，可以方便的修改定位，从而实现虚假出行订单或站街招嫖；
- 3) 改机功能，可以方便的修改IMEI，IMSI等硬件参数，从而伪造更多设备；
- 4) 主流的移动端App自动化操控脚本，比如微信自动加好友，自动加群，自动发朋友圈，抖音自动关注，自动点赞，自动发表评论等；
- 5) 云端备份功能，可以将整套攻击环境连同环境上登录的账号一并上传备份，通过还原快照的方式切换环境，从而进行大量攻击。

6.2 自动化攻击的技术手段和攻防对抗

黑产实现自动化攻击，主要通过2种技术手段：协议破解/伪造，以及模拟点击/操控。前者需要先破解应用的接口协议，存在一定的技术门槛，难度相对较大；而后者开发简单，可读性强，上手门槛较低，对于黑产来说，受众也更广。我们近期捕获到的自动化攻击工具里面，模拟点击/操控类工具的占比也更高：



接下来我们对这两类自动化攻击技术做更详细的介绍。

6.2.1 协议破解/伪造

协议破解/伪造指的是通过抓包+逆向分析等方式，获取到客户端跟服务端通信的请求接口以及参数，直接伪造接口协议和参数来完成自动化操作。

我们先以一款旅游类应用的自动发帖机为例。通过分析，我们可以看到这个发帖机会自动访问该应用的很多后端接口：

.rdata:004DF0EC	0000001C	C	https://[redacted]at/s
.rdata:004DF887	0000002E	C	https://[redacted]/rest/app/user/login/
.rdata:004DECFC	00000030	C	https://[redacted]/rest/app/note/content/
.rdata:004E0142	0000002D	C	https://[redacted]/rest/app/note/base/
.rdata:004DFC65	00000038	C	https://[redacted]/note/detail/get_note_detail/v1
.rdata:004DE4D8	00000028	C	https://[redacted]/notify/reg.php
.rdata:004E0477	0000002C	C	http://[redacted]/note/up/uploadPhotos
.rdata:004DE8E6	00000033	C	http://[redacted]/note/create.php/modify/?id=
.rdata:004DF2D5	0000002C	C	http://[redacted]/note/ajax_exinfo/set
.rdata:004DF1A1	00000032	C	http://[redacted]/note/ajax/post/saveHeadImg
.rdata:004DF161	0000002F	C	http://[redacted]/note/ajax/edit/setCover
.rdata:004DEA64	00000032	C	http://[redacted]/note/ajax/edit/insertNodes
.rdata:004E0580	0000002E	C	http://[redacted]/note/[redacted]
.rdata:00EAA377	00000025	C	http://[redacted]/msg/sms/index

由于破解了接口协议和参数，所以在访问接口之前，所有的参数都已经构造好了：

```

push    offset aScreenHeight12 ; "&screen_height=1280"
push    [ebp+var_timestamp]
push    offset aAppVer813AppCo ; "&app_ver=8.1.3&app_code=com.mfw.roadboo"...
push    [ebp+var_deviceid]
push    offset aOpenUdid ; "&open_udid="
push    [ebp+var_token] ; 固定值:0_0969044fd4edf59957f4a39bce9200c6
push    offset aChannelIdMfwXA ; "&channel_id=MFW&x_auth_mode=client_auth"...
push    [ebp+sys_ver] ; 固定值:"4.4.3"
push    offset aSysVer ; "&sys_ver="
push    [ebp+var_deviceid]
push    offset aMfwSdkVer20140 ; "&mfw_sdk_ver=20140507&getui_errorcode=0&"...
push    [ebp+var_hardwaremodel]
push    offset aGetuiCid403b1a ; "&getui_cid=403b1a478bb5418536996a16e8fb"...
push    [ebp+var_oauth_nonce]
push    offset aOLat31247221Ap ; "o_lat=31.247221&app_version_code=506&oa"...
mov     ecx, 0Fh
call    strcat_4010B8

```

其中有一些参数的伪造成本并不高，甚至直接硬编码在代码里面。

有一些参数会根据一定的规则动态生成，以满足合法性校验。以os_api和os_version这两个参数为例，在代码里面内置了一个os_version的数组：

```
array_os_version_31B08F3 dd 1 ; DATA XREF: gen_os_  
dd 9  
dd offset a8_0_0 ; "8.0.0"  
dd offset a5_1_0 ; "5.1.0"  
dd offset a5_0_1 ; "5.0.1"  
dd offset a5_1_1 ; "5.1.1"  
dd offset a6_0_1 ; "6.0.1"  
dd offset a5_0_0 ; "5.0.0"  
dd offset a4_4_4 ; "4.4.4"  
dd offset a810_0 ; "8.0.0"  
dd offset a4_4_1 ; "4.4.1"
```

永安在线反欺诈

构造参数时，会根据这个数组随机选择os_version的值，同时会根据os_version的值来适配os_api的值：

```
v22 = sub_405FCE(v37, "6.0") == 0;  
if ( v37 )  
    j__krnl_MFree(v37);  
if ( v22 )  
    return "23";  
v8 = *a2;  
if ( !*a2 )  
    v8 = &unk_64E2AC;  
v38 = (_BYTE *)j__krnl_MCallKrnLibCmd(2, (char)v8);  
v23 = sub_405FCE(v38, "5.1") == 0;  
if ( v38 )  
    j__krnl_MFree(v38);  
if ( v23 )  
    return "22";
```

永安在线反欺诈

再比如device_type和device_brand这两个参数，在代码里面内置了一个很大的设备类型的数组：

```
brand_array_31B0587 dd 1 ; DATA XREF: gen_brand_50E1AA+2;
dd 0CDh
dd offset aSamsungB7330 ; "SAMSUNG B7330"
dd offset aSamsungB7300 ; "SAMSUNG B7300"
dd offset aSamsungI350 ; "SAMSUNG i350"
dd offset aSamsungI637 ; "SAMSUNG i637"
dd offset aSamsungSghI688 ; "SAMSUNG SGH-i688"
dd offset aSamsungSghI728 ; "SAMSUNG SGH-i728"
dd offset aSamsungSchM490 ; "SAMSUNG SCH-M490"
dd offset aSamsung931sc ; "SAMSUNG 931SC"
dd offset aSamsungC6625 ; "SAMSUNG C6625"
dd offset aSamsungB7610 ; "SAMSUNG B7610"
dd offset aSamsungSphP900 ; "SAMSUNG SPH-p9000"
dd offset aSamsungSphP920 ; "SAMSUNG SPH-P9200"
dd offset aSamsungB7620 ; "SAMSUNG B7620"
dd offset aSamsungI8000 ; "SAMSUNG i8000"
dd offset aSamsungI8180c ; "SAMSUNG i8180C"
dd offset aSamsungI8305 ; "SAMSUNG i8305"
dd offset aSamsungI8320 ; "SAMSUNG i8320"
dd offset aSamsungI920 ; "SAMSUNG i920"
dd offset aSamsungB7350 ; "SAMSUNG B7350"
dd offset aSamsungI770 ; "SAMSUNG i770"
dd offset aSamsungSghI780 ; "SAMSUNG SGH-i780"
dd offset aSamsungSghI788 ; "SAMSUNG SGH-i788"
dd offset aSamsungSghI600 ; "SAMSUNG SGH-i600"
```

构造参数时，也是进行随机选择。如果选择了数组的第1个元素，那么生成的参数就是device_type=B7330并且device_brand=SAMSUNG。

以上举例的这些参数，伪造起来都比较简单，但是还有一些参数的伪造，难度要大很多。特别是一些做了协议保护的应用，会存在专门用于校验接口请求合法性的参数，而且多个参数之间相互校验，只要其中一个参数构造得有问题便无法通过校验。

理论上来说，黑产似乎因为对抗成本的提高而望而却步，但实际情况却并非如此。

首先，在开源或免费渠道上，GitHub，CSDN等网站上面有大量的协议算法的原理讲解，甚至破解代码。虽然作者的出发点可能是单纯的技术探讨，但却被别有用心的黑产直接利用：



其次, 存在一些破解网站, 其背后有专门的技术人员, 也提供收费的算法破解服务:

算法 ID	12
标题名称	算法
价格	1 点/次
JS 引擎类型	V8 引擎
调用说明	函数名: Encrypt 参数: [WiFi;mi max;Android;22;720*1280;yyb;z N:863114004408832] 功能: 计算 其中 参数内的 设备信息 自己修改

另外, 虽然随着移动端应用加固技术的发展 (包括成熟的商业化产品和方案), 核心算法的破解难度也越来越大, 但由于攻防的不对等, 黑产可以绕过这道防线, 选择从防御的薄弱点下手。而Web端应用就成为了这样的一个突破口。虽然Web前端的代码可以做混淆做加密, 但破解的难度相对要小很多。甚至可以不用破解, 直接把算法的关键代码扣出来, 通过脚本引擎进行调用和执行, 从而完成加密参数的构造:


```

var CryptoJS = CryptoJS || function (u, p) {
  var d = {}, l = d.lib = {}, s = function () {
  }, t = l.Base = {extend: function (a) {
    s.prototype = this;
    var c = new s;
    a && c.mixIn(a);
    c.hasOwnProperty("init") || (c.init = function () {
      c.$super.init.apply(this, arguments)
    });
    c.init.prototype = c;
    c.$super = this;
    return c
  }, create: function () {
    var a = this.extend();
    a.init.apply(a, arguments);
    return a
  }, init: function () {
  }, mixIn: function (a) {
    for (var c in a) a.hasOwnProperty(c) && (this[c] = a[c]);
    a.hasOwnProperty("toString") && (this.toString = a.toString)
  }, clone: function () {
    return this.init.prototype.extend(this)
  }
},

```

对于厂商而言，由于协议破解/伪造脱离了环境和设备的限制，黑灰产可以用很低的成本完成批量化规模化作案，因此危害也更加严重。如何更加有效的防止或检测这类自动化攻击，除了加强核心算法的复杂度之外，也可以尝试从情报入手。前面提到伪造的接口协议中，其中有一些参数是硬编码的，基于这些硬编码的参数，可以做特征聚类和分析，并针对性的提取识别规则。此外，黑产在构造自动化攻击的代码时，也不是天衣无缝，往往会在一些地方留下破绽。其中一种比较典型的情况是访问不同接口时，存在构造的参数不一致的情况。比如登录请求传入的设备类型的是iPhone：

```

'http://[redacted]/2/auth/login/v2/?platform=[redacted]'
; DATA XREF: sub_4AAF55+111↑o
'[redacted]&iid=&device_id=&ac=&channel=yingyonghui&aid=1128&ap'
'p_name=aweme&version_code=144&version_name=1.6.8&device_'
'platform=iPhone&device_type=&device_brand=&os_api=22&os_'
'version=5.1.1&vid=&openudid=&manifest_version_code=16807'
'&resolution=720*1280&dpi=192&update_version_code=16807',0

```

但紧接着进行设备注册时，注册的信息却变成了操作系统是Android，设备厂商是华为：


```
'http://[redacted]/service/2/device_register/',0
; DATA XREF: sub_4A03DA+143↑o
'727e09',0 ; DATA XREF: sub_4A03DA+20B↑o
'{"magic_tag":"ss_app_log","header":{"appkey":"5161a27ec07'
; DATA XREF: sub_4A03DA+356↑o
'[redacted]","udid":"{ieml}","openudid":"{mac}","sdk_
'
'version':1,"package":"[redacted]","channel'
'":"[redacted]","display_name":"[redacted]","app_version":"2.9.0"
',"version_code":290,"timezone":8,"access":"wifi","os":"A'
'ndroid'" "os_version":"5.1.1","os_api":22,"device_model":
'"{device_model}","device_brand":"{device_brand}","device'
'_manufacturer'" "HUAWEI","language":"zh","resolution":"17'
'76x1080","display_density":"mdpi","mc":"{mc}","carrier":
'"中国联通","mcc_mnc":"46001","clientudid":"{clientudid}","in'
'stall_id":"{iid}","device_id":"{device_id}","sig_hash":'
```

通过这些情报信息，可以不断补充和完善对于协议破解/伪造类自动化攻击的识别。

6.2.2 模拟点击/操控

模拟点击/操控是指通过触发鼠标/键盘/触控等事件，或者通过代码注入等方式，完成界面控件的输入、点击、移动等操作。如果说协议破解/伪造的对抗是技术的硬碰硬，模拟点击/操控则可以可以说是以巧致胜，而且由于上手门槛低，也成为了当前黑灰产最为喜欢的自动化攻击方式。接下来我们分别讲解几种比较常见的模拟点击/操控类攻击方式。

1) 按键精灵

按键精灵是一款大家非常熟悉的老牌自动化脚本工具，也是目前黑产使用最为普遍的通过模拟点击实现自动化攻击的工具。黑灰产从业人员通过编写相关的逻辑脚本，便可通过模拟用户操作去实现他们想要的功能，比如手机触摸、按键等操作；也可以先手动“录制”一遍想要操作的功能，这样按键精灵会自动记录操作行为序列和坐标轨迹，十分方便。

我们以某短视频平台的一款引流工具为例，该工具是基于按键精灵（安卓版）脚本打包生成的一个apk文件，其主要功能是自动给平台上的短视频点赞、评论，以及给用户发私信，从而达到引流的效果，如下所示：



使用该工具时，只要打开短视频平台某网红主页的粉丝列表界面，便可自动按顺序打开每个粉丝的主页，给视频点赞、评论以及给粉丝发私信，并且该工具也支持自定义配置，比如是否关注粉丝、自定义引流话术等。

2) Auto.js

如果说按键精灵是老牌精英，Auto.js则可以说是后起之秀。根据情报显示，大约从18年底开始，越来越多的黑灰产从业者使用Auto.js来开发自动化攻击脚本。Auto.js是一个基于JavaScript的安卓平台自动化脚本框架，相比与按键精灵，Auto.js有以下一些优势：

- 1) 设备无需Root，使用成本更低，而且可以躲避基于Root的风险设备环境检测；
- 2) 按键精灵基于识别图片、颜色、坐标等实现模拟操作，存在分辨率的兼容问题，而Auto.js可以直接操作控件，自动适配各种安卓机型，稳定性更高；
- 3) 使用Auto.js开发打包生成的apk文件体积更小。

我们以某社交平台的添加群成员好友的自动化脚本为例，首先判断是否处于群聊天窗口：

```
launchApp( );
sleep(500);
if(currentActivity() != "com. .activity.TroopMemberListActivity"){
    toast("请打开要加的群的聊天窗口");
    openGroupMemberList();
}
```

永安在线反欺诈

在获取到群成员QQ号后，自动完成点击“加好友”、填写验证信息、发送请求：

```
function addAsFriend(){
    var qq = getQQ();
    toast(qq);
    if(added[qq]){
        while(!click("返回"));
        return;
    }
    added[qq] = true;
    if(click("加好友")){
        sleep(800);
        setText(0, "好友验证信息");
        while(!click("发送"));
        sleep(800);
        if(click("取消")){
            sleep(400);
        }
        while(!back());
    }else{
        while(!back());
    }
}
```

永安在线反欺诈

Auto.js脚本开发者可以使用Visual Studio Code + Auto.js插件开发脚本，电脑连接手机终端，可直接控制装有Auto.js客户端的手机执行脚本，也可将脚本保存至手机终端，编译为APK，运行APK执行操作。

3) 浏览器内核

对于Web端应用来说，黑灰产往往通过浏览器做自动化攻击的载体。其中一种方式就是在工具中嵌入浏览器内核。以Chromium为例，Google为了方便给第三方应用提供可嵌入的浏览器支持，做了一个开源项目：CEF，全称Chromium Embedded Framework。

CEF隔离底层Chromium和Blink的复杂代码，并提供一套产品级稳定的API，发布跟踪具体Chromium版本的分支，以及二进制包。CEF的大部分特性都提供了丰富的默认实现，让使用者做尽量少的定制即可满足需求。CEF的应用场景之一就是用于自动化Web测试，这也给黑灰产打开了便利之门，将之用于自动化攻击。

我们以某智能爬虫采集器为例，该软件内置了 Chromium浏览器，通过直接操控页面控件来完成自动化操作。该爬虫采集器使用方式非常简单，只需在软件界面输入目标网站，就可以根据需求爬取目标网站的数据，界面如下：



利用该工具，爬取某旅游网站数据如下：

导出状态	序号	标题	标题链接	缩略图	detail1	detail2	location	view
	1	第一次去泰国，一...	http://www...	http://b1-q...	Q 如何办理泰国签...	Q 去泰国需要买航...	泰国	446669
	2	干货！普吉岛居民...	http://www...	http://n1-q...	NO.1选西不选东，...	西海岸南部最方便	普吉岛	60533
	3	值得收藏！保姆式...	http://www...	http://p1-q...	一、护照	二、签证	泰国	184376
	4	落地签免签证费~...	http://www...	http://n1-q...	支付宝可办理泰国...	落地签证是什么？	泰国	369
	5	超详细易懂的泰国...	http://www...	http://b1-q...	图片目录（看图片...	前期准备	泰国	37172
	6	泰国猛男餐厅升级p...	http://www...	http://n1-q...	猛男酒店：华富里P...	监狱酒店：曼谷So...	泰国	145
	7	曼谷必游经典、网...	http://www...	http://n1-c...	★经典必去景点	大皇宫	曼谷	129683
	8	第一次去泰国怎么...	http://www...	http://b1-q...	第一次出境游为何...	泰国旅游地那么多...	泰国	710732
	9	曼谷+甲米6天自由...	http://www...	http://p1-q...	行程规划：上海+...	1、先说说航空公司	泰国	92390
	10	三天时间，教你怎...	http://www...	http://b1-c...	初识清迈	1.清迈在哪里	清迈	245015
	11	手把手教你填写泰...	http://www...	http://p1-c...	一、办理落地签需...	二、快速办理落地...	泰国	20974
	12	泰国购物 泰国这些...	http://www...	http://n1-q...	外用篇	草药足贴	泰国	242192
	13	吐血整理！实测23...	http://www...	http://b1-q...	01、小老板海苔	02、泰好吃榴莲干	泰国	65864
	14	泰国落地签免签证...	http://www...	http://b1-q...	准备资料	填写说明	泰国	6329
	15	泰国王权免税店全...	http://www...	http://n1-q...	在王权免税店购物...	买什么划算？	泰国	355251
	16	泰国旅游实用帖 物...	http://www...	http://p1-q...	蜈蚣丸	老虎贴	泰国	72984
	17	7天时间，告诉你怎...	http://www...	http://p1-q...	初识“曼谷”	为什么7天时间最合...	曼谷	52390
	18	绕脑的泰国落地签...	http://www...	http://n1-q...	所需的材料	机场办理	泰国	57026
	19	泰国购物买什么？3...	http://www...	http://p1-q...	一、必买泰国本地...	1、Soffel驱蚊液	泰国	276145
	20	如何兑换泰铢	http://www...	http://n1-q...	国内兑换	当地兑换	泰国	642201

4) 自动化Web测试

为了方便自动化Web测试，主流的浏览器自身也展现出了足够的开放性，比如大家都比较熟悉的自动化测试工具Selenium/WebDriver，就是基于浏览器的一些开放特性，完成了对Web页面的自动化操控，而黑灰产利用Selenium/WebDriver来完成自动化攻击也非常常见。对于厂商而言，也往往会在Web端代码里面嵌入一段JavaScript脚本，来检测这类自动化测试工具：


```

"value": function ()
{
    var a = common_func.map(
    [
        common_func.some(["phantom", "_phantom", "callPhantom", "webdriver", "_Selenium_IDE_Recorder", "_selenium",
        {
            return r in window
        }]),
        common_func.some(["__driver_evaluate", "__webdriver_evaluate", "__selenium_evaluate", "__fxdriver_evaluate"
        {
            return r in document
        }]),
        common_func.some(["selenium", "webdriver", "driver"], function (r)
        {
            return document.documentElement.getAttribute(r)
        }]),
        new RegExp("PhantomJS", "i").test(navigator.userAgent),
        !!navigator.webdriver
    ],

```

 永安在线反欺诈

除了以上这些，还有一种自动化Web测试的手段：Chrome远程调试，也被黑灰产用于自动化攻击。我们以某社区软件的账号注册机为例，该工具会通过远程调式的方式打开Chrome浏览器：

```

asc_4EB4A3      db '浏览器已创建, 当前配置全部无效',0 ; DATA XREF: sub_419222+2B1fo
aCProgramFilesX_0 db '兄弟, (C:\Program Files (x86)\Google\Chrome\Application\chrome.exe)默'
; DATA XREF: sub_419222+90fo
db '认路径没浏览器呀',0
aRemoteDebuggin db '--remote-debugging-port=#引号',0
; DATA XREF: sub_419222+E2fo
asc_4EB538      db ' ',0 ; DATA XREF: sub_419222+171fo
; sub_419222+27Cfo ...
aUserDataDir    db '--user-data-dir=#引号',0 ; DATA XREF: sub_419222+1EDfo
aIncognito       db '--incognito',0 ; DATA XREF: sub_419222+2B6fo
aStartMaximized db '--start-maximized',0 ; DATA XREF: sub_419222+35Cfo
aProxyServer     db '--proxy-server=#引号',0 ; DATA XREF: sub_419222+41Bfo
aUserAgent_1     db '--user-agent=#引号',0 ; DATA XREF: sub_419222+4EDfo
aNoFirstRun      db '--no-first-run',0 ; DATA XREF: sub_419222:loc_4197BEfo
asc_4EB5A5       db ' ',0 ; DATA XREF: sub_419222+6B2fo
; sub_419222+805fo ...
aWindowPosition db '--window-position=#引号',0 ; DATA XREF: sub_419222+6BAfo
aWindowSize      db '--window-size=#引号',0 ; DATA XREF: sub_419222+80Dfo

```

 永安在线反欺诈

然后通过WebSocket通信对浏览器进行控制。包括：

- 执行
document.querySelector('[name=username]').select()获得手机号输入框的焦点；
- 发送
Input.dispatchEventKeyEvent消息，自动填写从接码平台获取到的手机号；
- 执行
document.querySelector('button.Button.CountingDownButton.SignFlow-smsInputButton.Button--plain').click()点击“获取短信验证码”按钮；

- 执行

```
document.querySelector('[name=digits]).select()获得验证码输入框的焦点，自动填写验证码，并执行  
document.querySelector('button.Button.SignFlow-submitButton.Button--primary.Button--blue').click()点击“注册/登陆”按钮。
```

移动端的模拟点击/操控类攻击，需要在设备上运行被攻击的移动端应用。

而且如果要实现批量化规模化攻击，需要有大量的设备资源（群控、云控、箱控，或者通过模拟器/改机工具伪造设备资源），因此对于厂商来说，可以从设备环境层面进行风险检测。无论是使用按键精灵、Auto.js、改机工具、GPS伪造等工具，还是模拟器、群控等设备环境，可从设备指纹数据中找到蛛丝马迹，设备指纹除了用作唯一性标识之外，还应该对基本的应用多开、改机环境/环境伪造、Hook行为、Root/越狱、代理/VPN等风险场景有识别能力。如果具备较强的情报能力，可以尽可能多的收集自动化攻击脚本程序，并在应用启动的时候检测安装列表（Applist）中是否存在这类程序。

另一方面，模拟点击/操控类攻击虽然会模仿正常用户的操作行为，但与用户实际的行为特征还是会存在差异，可以从行为层面做检测。

比如针对某电商平台刷店铺访问量的工具，每一次刷量行为一定会包含“打开首页”、“搜索目标店铺的商品关键词”、“先进入两家同类商品的店铺浏览商品”（模仿正常用户货比三家的习惯）、“在进入目标店铺浏览商品完成刷量”，并且在每个页面的停留时间也在固定的。

从业务数据中提取用户关键行为做特征进行聚类分析，可以有效识别程序化的模拟操作。

再比如上述的某智能爬虫采集器，虽然会产生看似正常的页面浏览行为，但是没有正常的鼠标点击、键盘输入或屏幕触控等操作，也属于高度可疑的行为。

当然，设备层面和行为层面的数据往往是互补的。为保证高准确性和识别率，风险行为的判定要结合多个维度综合判断。

6.3 攻防建议

从技术上实现攻击流程的高度自动化，是黑灰产提高运营效率，降低运营成本的必然道路。

稳定的、成熟的自动化测试工具和技术被黑产滥用，又极大的提高了黑产的开发和攻击效率。这对于厂商的业务安全防护策略来讲，无疑将不断面临更大的挑战。庆幸的是人机识别的对抗是一个持续升级和演进的过程，不管是对于业务方来讲，还是对于黑灰产来讲，都没有绝对的银弹。

业务方除了在风控规则模型上下功夫外，还可以在设备上进行检测：

- 1) 对业务运行的设备环境进行检测。黑灰产无论是在设备信息欺骗上，运行自动化脚本工具，都需要使用一些特殊的运行环境。这些环境通过分析一般都能找到一些通用的检测点。比如改机工具，可以对Hook框架进行检测，模拟点击可以检测系统参数。这些都可以作为可疑设备特征进行加权打分。
- 2) 对业务上的用户行为识别。黑产自动化通常会用到的协议模拟技术和模拟按键技术，这都跟自然人的操作路径会有巨大的差距。比如当用户登录时，账号密码的输入不会是瞬间完成的，又或者每次按钮的点击，也不会在相同位置。这些都可以作为检测特征，当我们对用户操作行为进行识别，这大大增加了黑灰产的对抗成本。

在未来的人机对抗中，企业将会面临越来越多的自动化攻击。

企业在业务安全的纵深防御上，除了基础风控的建设之外，还需要在设备上进行检测，从而提高黑灰产的攻击成本，提升防护效果。

四、黑产工具情报分析

对于企业方面来说，黑产工具情报可以有效的提高业务安全的攻防效率。通过分析工具利用的业务接口，不仅可以将黑产作恶行为进行有效的追踪，对其进行有效的处理，还能强化业务层面对安全的认知，知晓业务接口中的安全薄弱点，并进行持续性的安全加固。

1. 工具样本的快速分析和有效性验证

由于环境依赖、组件依赖、资源依赖等原因，可以手动运行并执行相应功能的工具样本占比并不高。绝大多数工具样本可以通过另外的一些方法进行快速分析和有效性验证，剩下少量的未知样本或高价值样本再尝试通过手动运行的方式进行复现。

不容易手动执行并复现功能的原因主要有以下一些:

1) 缺少工具运行的环境, 比如.net 编写的工具需要.net的运行时环境, XPosed 程序需要XPosed 框架等;

2)缺少工具运行所依赖的一些组件, 主要出现在部分 PC 端工具样本, 在运行时需要一些其他的动态库(DLL)支持;

3)工具运行时会检测虚拟机环境, 导致在虚拟机中运行不起来, 主要出现在 部分 PC 端工具样本;

注:工具样本中存在病毒伪装工具, 以及带毒打包工具等情况, 因此运行工具请务必放在虚拟机环境中, 以防感染实体机环境;

4)工具需要激活或注册才能够使用, 对于这种情况, 可以尝试联系作者进行购买, 或者通过破解等手段绕过激活或注册, 直接进入工具主界面;

5)工具执行相应功能时, 缺少需要的资源文件, 比如部分工具在执行批量回复、点赞、关注等操作时, 需要读取本地的账号资源文件;

6)工具执行相应工功能时, 需要购买黑产平台的资源, 比如注册机类工具, 往往需要先在接码平台注册账号并充值, 然后在工具运行时填入接码平台的账号密 码;

7)工具执行的流量比较复杂, 有的需要按照一定的步骤一步步执行, 有的需要先执行一些前置操作。对于这类工具往往得先找到教程并按照教程来执行等。

1.1 PC 端工具的分析

1.2.1 搜索“http:”和“https:”

PC 端的工具样本绝大多数都是协议类工具(直接伪造前端和服务器的通信协议, 完成批量自动化操作), 我们可以在工具内置字符串中搜索“http:”以及 “https:”开头的字符串, 如果搜索到的字符串中包含对应业务的接口URL, 如下所示:

▼ 工具内置字符串	命中 facebook 相关信息4条 命中
44	.location.replace
45	https://m.facebook.com/messages/read/?fbid=
46	errorSummary
47	Adodb.Stream
48	WriteText
49	https://m.facebook.com/friends/center/friends/?ppk=
50	https://m.facebook.com/messages/
51	&jazoest=&__dyn=&__csr=&__req=a&__ajax__=&__a=

则基本可以断定该工具就是一款协议类工具。

1.2.2 硬编码参数

明确了协议类工具之后，接下来验证工具的有效性。大部分协议工具都会存在一些硬编码的请求参数，在工具内置字符串中，接口URL 附近往往可以找到这些 硬编码的参数，如下所示：

▼ 工具内置字符串	命中 相关信息3条
143	http://
144	G955F&ssmix=a&iid=58510009238&os_api=19&device_id=621077666838&resolution
145	&count=49&comment_style=2&digged_cid=&insert_cids=&ts=
146	&cursor=
147	https://api
148	comments
149	
150	comments.[

以这些硬编码参数为过滤条件，对接口流量进行筛选，如果有命中的流量，则说明该工具(或同类工具)对接口 URL 进行了协议请求。同时可以进一步观察这些请求是否可以被识别为恶意请求，如果没有被识别出来，则说明当前该工具是有效的。

1.2 移动端工具的分析

1.2.1 工具的包名

移动端的工具以模拟操控为主，因此工具运行之前，需要先安装目标 App，并将其运行起来。如果目标 App 有采集终端设备上包含包名信息的 App List，则可以通过工具的包名将其

识别出来。将下载下来的工具拖动到 JDE等分析工具中，可以获取到包名信息(后续我们也会在情报平台上展示工具的包名):



```
e:cxsgdbb.com
e:com.android.launcher3
e:com.android.provision
e:com.example.script1580808591565
e:com.android.providers.settings
e:com.android.sharedstoragebackup
e:com.example.script1583655012709
e:com.android.webview
e:com.android.inputdevices
e:com.example.script1585045685614
e:com.mobile.myappfdy
e:com.sbdsoft.clgl.wz
```

```
<?xml version="1.0" encoding="UTF-8"
<manifest android:compileSdkVersion="28"
android:versionCode="1" android:versionName="1.0"
platformBuildVersionName="9" xmlns:android="http://schemas.android.com/apk/res/android"
<uses-sdk android:minSdkVersion="28"
<uses-permission android:name="android.permission.INTERNET"
<uses-permission android:name="android.permission.ACCESS_NETWORK_STATE"
<uses-permission android:name="android.permission.ACCESS_WIFI_STATE"
"com.android.launcher.permission.LAUNCH_SETTINGS_APP"
```

如果终端设备上有这个工具，则可以认为该设备属于高风险的设备，对其发起的业务请求采取必要的限制。

1.2.2 工具的源代码

大多数移动端工具都可以在情报平台上下载通过一定技术手段还原出来的源代码。直接阅读源代码可以清晰的了解工具的运行原理，依赖的资源，执行的步骤等。以 3 种不同类型的工具来说明:

1) 按键精灵

按键精灵还原出来的源代码是 Lua 脚本，代码量比较大，往往有上百K。分析时可以先从 main 函数开始阅读(一般在源码最后)，可以快速了解其核心功能逻辑。如下是某短视频应用红包工具的 main 函数代码片段:

```
;(function()
local L0_1965
L0_1965 = nil
id494e5458, id494e5459, L0_1965 = LuaAuxLib.FindPicture(0, 0, 0, 0, "Attachment:滑块.png", "000000", 0, 0.9)
return L0_1965
end)()
if id494e5458 > -1 then
LuaAuxLib.TracePrint("_28:", "找到验证码")
ide6bb91e58aa8()
LuaAuxLib.Sleep(10000)
LuaAuxLib.Swipe(519, 1565, 519, 465, 1000)
LuaAuxLib.Sleep(3000)
;(function()
local L0_1966
L0_1966 = nil
id494e5458, id494e5459, L0_1966 = LuaAuxLib.FindPicture(0, 0, 0, 0, "Attachment:滑块.png", "000000", 0, 0.9)
return L0_1966
end)()
if id494e5458 > -1 then
break
end
else
LuaAuxLib.TracePrint("_38:", "没找到")
end
;(function()
local L0_1967
L0_1967 = nil
id494e5458, id494e5459, L0_1967 = LuaAuxLib.FindPicture(0, 0, 0, 0, "Attachment:领取.png", "000000", 0, 0.9)
return L0_1967
end)
```

按键精灵主要通过 FindPicture 找到界面上需要输入或点击的位置，然后自动化完成操作。

2) autojs 脚本

autojs 还原出的源代码有点类似于 Javascript，代码分为两部分，第 1 部分是页面布局，描述了工具运行后的主界面：

```
"ui";
ui.layout(
  <vertical>
    <text textColor="#B22222" textSize="20sp" gravity="center" text="
    <horizontal>
      <text text=" 1: 私信话术" textColor="#9400D3" />
      <input hint="点击此处填写" id="we" text="" />
    </horizontal>
    <horizontal>
      <text text=" 2: 私信话术" textColor="#9400D3" />
      <input hint="点击此处填写" id="wr" text="" />
    </horizontal>
    <horizontal>
      <text text=" 3: 私信话术" textColor="#9400D3" />
      <input hint="点击此处填写" id="wt" text="" />
    </horizontal>
    <horizontal>
      <text text=" 4: 私信话术" textColor="#9400D3" />
      <input hint="点击此处填写" id="wn" text="" />
    </horizontal>
    <horizontal>
      <text text=" 5: 私信话术" textColor="#9400D3" />
      <input hint="点击此处填写" id="wm" text="" />
    </horizontal>
    <horizontal>
      <text text=" 6: 喜欢用户配对" textColor="#00008B" margin="2"/>
    </horizontal>
  </vertical>
)
```

第 2 部分是功能函数，即点击某个功能后所执行的操作：


```

var a=className("android.widget.TextView").depth(11).text("聊天").findOne()
click(a.bounds().centerX(),a.bounds().centerY())
sleep(2500)
var b=className("android.widget.FrameLayout").depth(16).drawingOrder(1).find()
var c=b.length-1
swipe(b[4].bounds().centerX(),b[4].bounds().centerY(),b[2].bounds().centerX(),b[2].bounds().centerY(),2000)
sleep(2500)
var n=ui.wv.getText()
for(var i=0;i<8;i++){
var tv=b[0]
if(tv){
var o=i+1
sleep(2000)
toast("回复第"+o+"个用户")
sleep(3000)
var r=className("android.widget.LinearLayout").depth(15).findOne()
click(r.bounds().centerX(),r.bounds().centerY())
sleep(2500)
var A=ui.wv.getText()
var B=ui.wr.getText()
var C=ui.wt.getText()
var D=ui.wn.getText()
var E=ui.wm.getText()
sleep(random(2000, 3500))
var data = []

```

相比于按键精灵，autojs是通过 className 定位控件的方式来找到操作对象。

无论是按键精灵还是autojs，都是按照脚本代码一步步的执行，其操作流程是非常固定的(可以看到每执行一步操作后的sleep时间也都是固定的)，而正常人显然不会有这样的操作，因此可以基于此提取针对该工具的人机识别特征。

3) Xposed 程序

Xposed 程序还原出的源代码是 Hook 类的 Java 代码，代码片段如下所示：

```

public final class M implements IXposedHookLoadPackage {
    public M() {
        super();
    }

    public final void handleLoadPackage(XC_LoadPackage$LoadPackageParam arg10) {
        if(arg10.packageName.startsWith("com.")) {
            d v0 = new d();
            ClassLoader v1 = arg10.classLoader;
            int v4 = 2;
            Object[] v5 = new Object[v4];
            v5[0] = Integer.TYPE;
            v5[1] = new com.DyMjsUopenpb.XTS.a.d$10(v0);
            XposedHelpers.findAndHookMethod("android.app.ApplicationPackageManager", v1, "getInstalledApplications", v5);
            v5 = new Object[v4];
            v5[0] = Integer.TYPE;
            v5[1] = new com.DyMjsUopenpb.XTS.a.d$11(v0);
            XposedHelpers.findAndHookMethod("android.app.ApplicationPackageManager", v1, "getInstalledPackages", v5);
            v5 = new Object[v4];
            v5[0] = Integer.TYPE;
            v5[1] = new com.DyMjsUopenpb.XTS.a.d$12(v0);
            XposedHelpers.findAndHookMethod("android.app.ActivityManager", v1, "getRunningServices", v5);
            v5 = new Object[v4];
            v5[0] = Integer.TYPE;
            v5[1] = new com.DyMjsUopenpb.XTS.a.d$2(v0);
            XposedHelpers.findAndHookMethod("android.app.ActivityManager", v1, "getRunningTasks", v5);

```

Xposed 程序先通过包名定位到目标 App，然后调用 findAndHookMethod来完成对目标 App 某些关键函数的 Hook，从而截取信息或植入行为。

如果在源码中搜索到自身应用的包名，则基本可以确定该工具的目标就是自身业务。接下来再搜索“findAndHookMethod”或“hookAllMethods”，查看哪些函数被工具 Hook 了以及 Hook 后执行的操作。

1.3 关于工具样本的常见疑问与解答

1.3.1 为什么会有一些看起来一样的样本？

部分工具样本的更新会非常频繁，甚至 1 天几个版本，这些不同的版本看起来基本一样，不过不用每一个都分析，分析发现时间最近的样本(最新版本)即可。

短视频平台自动维护工具.exe

协议类工具

分析完成: 2020/04/10 08:39:55

发现: 2020/04/04 11:18:36

1.3.2 为什么有的工具样本发现时间和分析完成时间间隔得比较久？

发现指的是我们从情报中感知到有这款工具的存在，之后需要挖掘下载渠道并下载工具样本，然后调度自动化分析平台对工具样本进行识别和分析，这中间可能会耗时比较久，目前整个流程仍然在优化，耗时会持续缩短。

2. 工具分析及案例

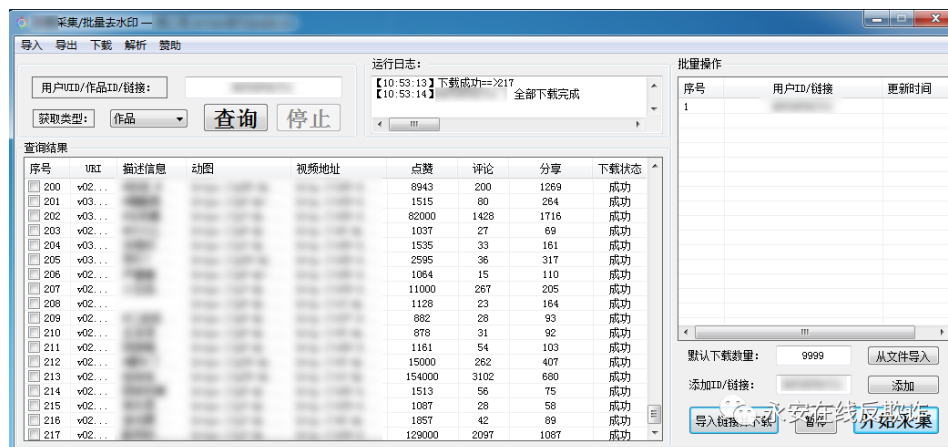
接下来我们以恶意爬虫、抢券工具和注册机三种工具来谈一下黑产工具情报的分析方式，并给出对应的案例分析：

2.1 恶意爬虫工具

2.1.1 分析方法

爬虫工具：xx采集/批量去水印.exe

工具用户：需要批量下载某短视频平台内容的普通用户，以及需要将视频在其他平台投稿的视频转载搬运人员。



xx视频采集/批量去水印工具截图

工具攻击方法：在输入框内输入该平台作者的ID或作品链接后，爬取该作者发布和喜欢的作品并下载到本地。除批量下载外，也可采集指定作品ID或分享链接的视频。



工具分析：这是一款运行在PC端的协议工具，发现时间为2020年5月2日。这个工具的作恶方式是通过访问作品分享链接，获取到视频平台用户唯一识别ID，再通过拼接参数，伪装成该视频应用的移动客户端进行获取视频列表、视频ID的操作，并利用某个暴露在外的接口，构造无水印视频下载链接，实现视频“去水印”功能。

```
['item_list'][0].desc  
['item_list'][0].video['dynamic_cover']['url_list'][0]  
['item_list'][0].video.vid  
['item_list'][0].statistics['digg_count']  
['item_list'][0].statistics['comment_count']  
userlist  
['aweme_list']  
['aweme_list']
```

永安在线反欺诈

通过拼接参数获取到的视频ID

 永安在线反欺诈

[永安在线反欺诈](#)

发现时间：2020年5月

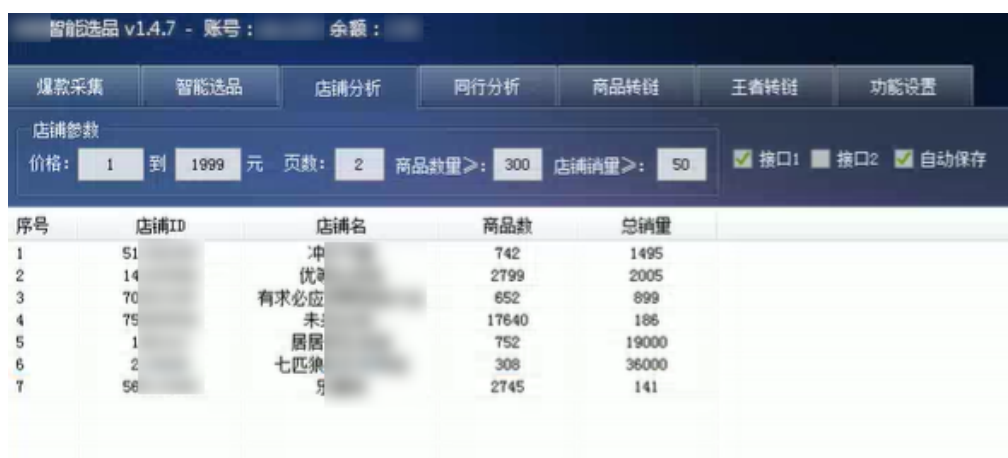
本次分析的工具是给“无货源商家”做电商选品与盗转商品信息用的工具。

这个工具一个功能较多的综合化电商选品工具，其中包括爬虫工具、转链工具和上货工具，其中对电商平台影响最大的还是爬虫工具。我们检测到了该工具会爬取包括○宝、拼○○等多家电商平台的商品信息，并涉及到了对应平台返利联盟的返利比例爬取。

根据对该工具的视频教程进行分析，我们可以了解到，该工具爬取的数据包括商品ID、店铺ID、商品标题、商品价格、销量、佣金比例，以及店铺商品数量、销量等信息。

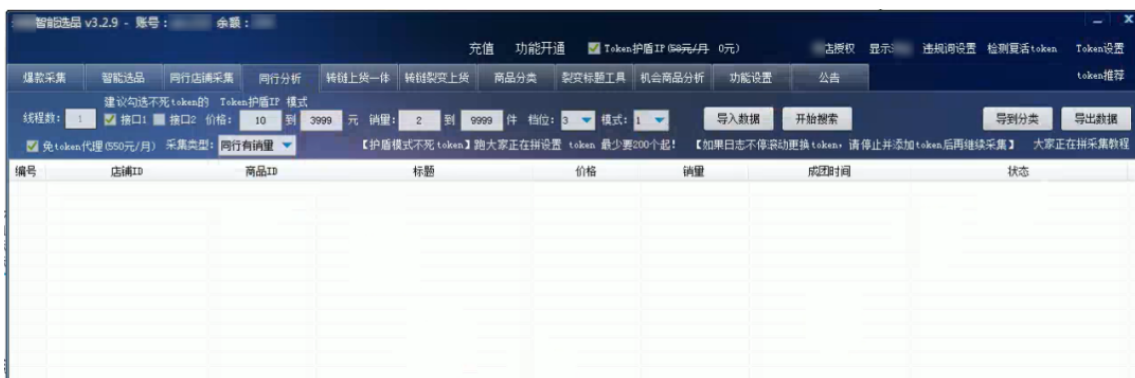


根据关键词库爬取商品信息



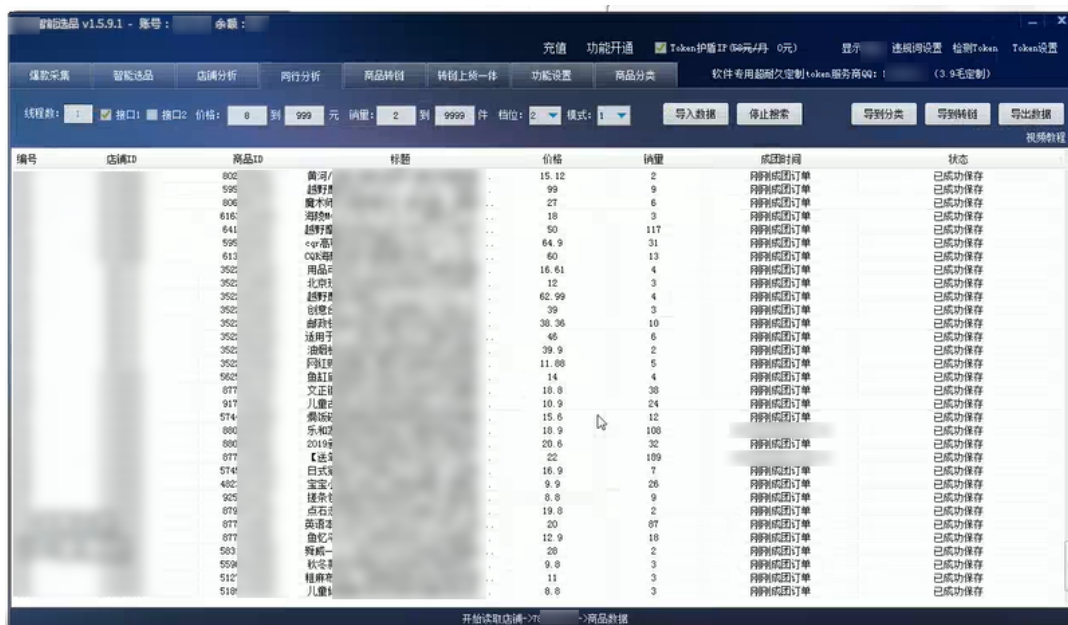
利用该工具爬取店铺信息

而伴随着爬取工具的升级，该工具逐渐在版本更新中添加了大量的辅助类工具，如裂变标题生成、同行分析、转链上货一体化操作等，这些新增功能均是基于爬取商品信息后再进行的分析，进一步加大了电商平台的爬虫压力。



同行分析相关功能

众所周知，各大电商平台对价格爬取是有一定的反制措施的，包括但不限于限制单IP、单账号的搜索请求频率。在这个工具中，我们从主界面就可以看到，为了爬取到商品信息，该工具采取了“人海战术”，即利用大量的账号资源与代理IP资源去进行数据“分布式爬取”，将所需的店铺ID、商品ID、标题、价格等数据进行爬取，再整合到一个列表中，从而实现将大量的商品信息爬取到本地。该工具主要爬取的电商平台为○宝与拼○○。



图为爬取拼○○商品信息

该工具爬取时会利用软件集成代理IP与事先导入的电商平台账号进行爬取，由于电商平台会对异常行为账号进行行为校验或屏蔽，该工具为了提高爬取的效率，还会对账号登录信息Token的可用性进行检测。

检测Token有效性					
编号	uid	Token	登录状态	详情状态	正在拼状态
1	AYXG2		正常	可用	可用
2	STEPQ		正常	可用	可用
3	APAON		正常	可用	可用
4	NN470		正常	可用	可用
5	OP4MX		正常		

2) 工具分析

基本信息：

文件名	**智能选品.exe
文件 MD5	07cd03571*****b480576e
文件大小	30.64M
发现时间	2020 年 5 月
编写语言	E 语言
是否加壳	VMP
运行平台	Windows

详细分析：

该工具首次发现于2020年5月26日，是一款采用E语言编写，并且使用VMP加壳的工具软件。对该工具进行静态分析，我们可以确认该工具是一款协议工具，通过破解各大电商平台app的业务接口通信协议，向电商的后台服务器发送精心伪造的数据包，从而达到自动爬取商品信息的目的。

相比于模拟按键脚本（触控精灵/按键精灵等），协议工具脱离了设备的限制，黑灰产利用协议工具可以更低成本完成批量化规模化作案，因此危害也更加严重。

以该工具对拼○○上的商品信息爬取为例，工具首先会调用以下接口进行登陆：

hxxps://mms.pin***.com/latitude/auth/login

```
v48 = (int *) "https://mms.pin***.com/latitude/auth/login";
if ( v72 )
    sub_A7015F(v72);
v72 = v48;
v64 = (char *) sub_86CC04();
v63 = 0;
v48 = 0;
v62 = "crawlerInfo";
(*(void (__stdcall **)(int **, char **, char **, _DWORD, _DWORD)))(*v71 + 20))(&v71, &v62, &v64, 0, 0);
if ( v62 )
    sub_A7015F(v62);
if ( v64 )
    sub_A7015F(v64);
v64 = 0;
v48 = 0;
v63 = "oppo a33";
v62 = "deviceName";
(*(void (__stdcall **)(int **, char **, const char **, _DWORD, _DWORD)))(*v71 + 20))(&v71, &v62, &v63, 0, 0);
if ( v62 )
    sub_A7015F(v62);
```

爬取商品信息时所使用到的一些接口:

hxxps://mms.pin***.com/venus/api/goods/list

hxxps://pifa.pin***.com/pifa/goods/queryGoodsDetail

hxxps://pifa.pin***.com/pifa/goods/queryGoodsPropertyInfo

hxxps://youhui.pin***.com/network/api/goods/queryByGoodsId

hxxps://mms.pin***.com/vodka/v2/mms/query/display/mall/goodsList

hxxps://mms.pin***.com/sydney/api/mallScore/queryMallScoreInfo

```
v76 = "accept: */*\r\n"
      "accept-encoding: gzip, deflate, br\r\n"
      "accept-language: zh-CN,zh;q=0.9\r\n"
      "anti-content: 0aoAfxnqUhhYq9E2h48L-4pc60UC4eIJO4fGD8p16B2k0KCEl9n1skKCoOxEIhy30wKR-VIpmoLhVEiL9XChWSNFIAw8Hg"
      "9EQ97V1ChQ9iOKNaJZOJ5mRZ9vSKDO-8vh9h0x-CwvBE0limhtsoeGKxpp_VvtJonpaeBpctgffax-MB9srCvL0qmCZLWi998DvQYqTAabJ"
      "U2xPzmmYfw65Q4PfewrjYpPwoVL9Bwkd90BZFgJxgA0m1Uf1teMzVdJ5sqGnnpa0-jtoNug66rRwJod2Q0_SvAHIDya0IwmC4CUuqRLnLkQ4"
      "8BkEUPlRaRQhrpTLakvvenvWbFzf0s-u2M1GwyA7HbhSPzLn_iGXlvcJTMyqzIFwWACX_aB1_2fwoW4cY1X8p0PLTOVMuvAwc5H-hfSo8OKf"
      "cL7JReIi3d0NRckqLMRMyKN-Qap_kiMD7RPNL2NdKhsd6r21fLFvNn-dfw7cjh_0d8hGLeKYjKJhfb2rpL6hJ\r\n"
      "cache-control: max-age=0\r\n"
      "content-length: 22\r\n"
      "content-type: application/ison\r\n"
      "cookie: api_uid= ; _pati=TFeKtKlF80Stf1APDi2Q0ygReSaH3qmB; _nano_fp=XpEoX5dJl09qlpdon"
      "o_x7ZumfjIHrzYbLDTpgQ2Q; VISITOR_PASS_ID=G0qKdjIMqg7g; RmKZAL28ZWyP6eF2DcRxqmRp1EL08jQBfhY"
      "HTv7WGFwm815mA-ZNPwkE0862XZV_irhUejRKhuo_f41c0dbdeb\r\n"
      "origin: https://pifa.pin***.com\r\n"
      "referer: https://pifa.pin***.com/goods/detail/?gid=3404818178\r\n"
      "sec-fetch-mode: cors\r\n"
      "sec-fetch-site: same-origin\r\n"
      "user-agent: Mozilla/5.0 (Windows NT 10.0; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/78.0.3904.108 Safa"
v75 = 0;
v74 = 0;
v73 = (int *) sub_41F983(
    &v111,
    1,
    1,
    &v109,
    1,
    &v74,
    0,
    &v75,
    0,
    &v76,
```

部分接口请求代码，其中请求头已内置

另外，此工具还用到了打码平台、代理平台来绕过电商平台的反爬虫策略。

该工具使用到的代理平台：

hxxp://www.**daili.cn/

该工具使用到的打码平台：

hxxp://www.**dama.com/

3) 攻防建议

爬虫对电商平台的威胁由来已久，针对这种爬取商品价格信息的工具也是层出不穷。虽然各电商已经有相对完善的手段去检测并拦截一些异常的自动化请求，但是来自黑灰产的需求源源不断，自然会出现绕过对应规则的工具，这属于长期的攻防对抗。

面对这种需要长期进行对抗的情况，电商平台的应对方式可以采取灵活多样的识别与拦截手段，从而提升黑灰产自动化工具的作恶成本，从而抑制其对数据的爬取。识别异常爬取行为可以利用IP风险识别、账号异常多地频繁登录、账号登录设备异常、账号搜索行为频率过高等检测手段进行发现与判断，并利用包括但不限于字符验证码、语音验证码等多种验证方式提高黑灰产的绕过成本，在不影响真人用户访问的情况下，对黑产的访问进行拦截。

2.2 抢券工具

2.2.1 分析方法

抢券工具：xxxx20200615.exe

工具用户：该工具主要是针对某平台特定活动的专用工具，其主要用户为利用平台大额优惠券进行牟利的黑产。

工具攻击手法：该工具主要的攻击方法是利用平台无设备校验的接口进行自动化抢券，并利用大量账号套取大量的优惠券进行牟利。

工具分析：该工具出现在2020年6月15日，采用QT语言编写。通过静态逆向分析该工具代码，发现其主要功能：

```
if ( *(_DWORD *)v304 < 0xFFFFFFFF && *(_DWORD *)v304 != 0 )
    _InterlockedAdd((volatile signed __int32 *)v304, 1u);
((void (__fastcall *)(int *, int))ZN7QString6appendERKS_)(v306, v153);
sub_43F8B0((int)&v307, (int)&v306, "优惠券领取");
v154 = v307;
v308 = v307;

{
    sub_43DAB0(&v216);
}
v366 = (volatile signed __int32 *)((int (__stdcall *)(const char *, signed
    "优惠券已领过",
    18);
v88 = ZN7QString7indexOferKS_in2Qt15CaseSensitivityE(&v273);
sub_43DFB0(&v366);
v286 = ((int (__stdcall *)(const char *, signed int, volatile signed __int32 **))Z
    "优惠券已抢完",
    18,
    v191);
if ( ZN7QString7indexOferKS_in2Qt15CaseSensitivityE(&v273) == -1 )
{
    v287 = ((int (__stdcall *)(const char *, signed int, int))ZN7QString16fromAscii_
    "优惠券已领完",
    18,
    v192);
if ( ZN7QString7indexOferKS_in2Qt15CaseSensitivityE(&v273) == -1 )
{
    sub_43DF70("当前优惠不在活动期间");
```

永安在线反欺诈

领券相关代码

在工具的代码中我们可以看到其针对的优惠券有酒店券、门票券、机票券这几种：

```
1) )
    sub_43DFF0("酒店券");
}
else
{
    sub_43DFF0("门票券");
}
}
else
{
    sub_43DFF0("机票券");
}
```

永安在线反欺诈

为了绕过平台对IP地址的风控限制，该工具在抢券前还会在部分代理IP平台上获取IP资源并设置代理，在代码中我们看到了其硬编码绑定的代理IP账号与密码。


```
a5SProxyM db 's5.proxy.163.com',0 ; DATA XREF: sub_404730+62fo
; sub_40B210+356fo
db '1952019',0 ; DATA XREF: sub_404730+81fo
db 'cb79ea163 Fe6cf746fb72e4b',0 ; DATA XREF: sub_404730+81fo

aHttpClas db 'http-cla.163.com',0 ; DATA XREF: sub_405390+22fo
; sub_405FC0+55fo ...
aH85 db '9e3fr2',0 ; DATA XREF: sub_405390+39fo
a37C db '781b36',0 ; DATA XREF: sub_405390+50fo
aUser db '/user',0 ; DATA XREF: sub_405390+39Afo
aPassword db '/password',0 ; DATA XREF: sub_405390+47Cfo
aBl db 'x',0 ; DATA XREF: sub_405FC0+1Ffo
a2019 db ' ',0 ; DATA XREF: sub_405FC0+3Efo
aHttp21 db '15716',0 ; DATA XREF: sub_405FC0+6Cfo
; 7809/vps/service/ip/get?type=1&airline=',0
align 10h
aHttp2187 db '15716_0',0 ; DATA XREF: sub_405FC0+8Efo
; 7810/bcp/api/bcp-vps-adsl-dispatch/vps/serv'
db 'ice/ip/get?type=1&airline=KN',0 ; DATA XREF: sub_405FC0+10Cfo
aUrl db 'url:',0 ; DATA XREF: sub_407690+97fo ...
```

代理IP平台账号密码与接口

攻防建议：

面对这种利用代理IP进行自动化批量抢券的黑产工具，除了从业务层面提高用券成本，降低黑产的潜在利益外，还可以从代理IP的角度去进行防御，利用永安在线的风险IP画像功能，将通过代理IP的请求进行拦截或进行二次安全验证。同时，在工具中也暴露了某些接口存在未校验请求来源的问题，在后续领券活动接口开发中要进行相关的业务安全加固。

2.2.2 案例：营销活动场景黑产拉锯战

关键字：营销活动 黑产攻击 恶意工具

发现时间：2020年8月

1) 针对某营销活动的作恶工具

超级星期五是国内某家网络运营商自2020年6月起在“**营业厅”APP中举办的每周固定的营销活动。该活动初期是运营商联合外卖平台进行的“来吃霸王餐”活动，支付方式包括在线支付与手机积分兑换，可实现免费获取相关优惠券。伴随着活动影响力的逐渐变大，活动更名为“超级星期五”，抢购范围也逐渐增加了针对音视频网站会员、出行，还有线下饮品店的大额折扣券。



最初的活动仅与外卖平台一家的合作



周五品牌日



近期新增的各类优惠券

伴随着该活动每周的升温，黑产也在蠢蠢欲动，尤其是最热门的10元购“满30减30”外卖红包，激发起了黑产对该活动的兴趣，对应的抢购工具也“应运而生”。不过真正检测到黑产大规模作恶动向的“实锤”是因为9月底的一次活动中，因众多黑产工具对活动接口的访问过多

无法正常响应，导致大量黑产下单后无法再进行付款操作，造成支付超时，抢购订单被释放。羊毛党在交流社群内围绕着该活动存在的各种问题进行大规模的吐槽，也印证了该活动已经被大量人群关注并进行攻击。



不过话说回来，因为抢购工具导致无法下单这事挺常见，因抢购工具导致系统瘫痪无法支付，黑产方面还要卖惨反手找客服投诉这事咱是头一回听说。至于为啥这个抢购工具能够连带着把支付业务的响应速度打慢，我们不如直接利用Karma业务情报搜索引擎的专家工具分析功能将作恶方式分析一下。

2) 工具分析

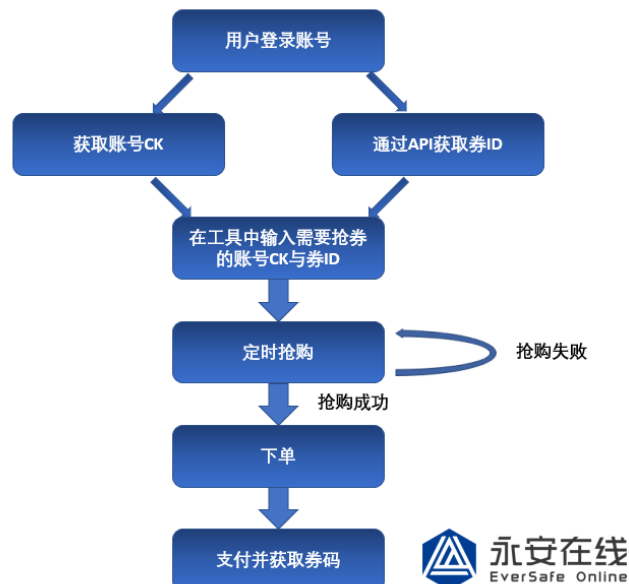
基本信息：

文件名	***_**星期五***-30 卷 v1.52.exe
文件 MD5	7a87c9efcd0e*****e3155e418c
文件大小	744,448 字节
发现时间	2020/08/29 23:01:38
编写语言	E 语言
是否加壳	UPX
运行平台	Windows

程序运行后界面：



程序的运作流程图如下:



详细分析:

该工具首次发现于2020年8月29日, 是一款采用E语言编写, 并且使用upx加壳的工具软件。脱壳后对该工具进行静态分析, 我们可以确认该工具是一款协议工具, 通过破解“**营业

厅”app的业务接口通信协议，向该应用的后台服务器发送精心伪造的数据包，从而达到自动化批量抢购优惠券的目的。

相比于模拟按键脚本（触控精灵/按键精灵等），协议工具脱离了设备的限制，黑灰产利用协议工具可以更低成本完成批量化规模化作案，因此危害也更加严重。

工具首先会调用接口：

https://m.client.100**.com/mobileService/sendRadomNum.htm

https://m.client.100**.com/mobileService/radomLogin.htm

发送获取验证码的请求，填入验证码后发送登陆请求获取手机号对应cookie，之后就使用这个cookie对应的手机号进行抢券，此软件支持使用3个号码的cookie进行抢券，其部分代码片段如下所示：

```
v5 = "D&version=android%405.91&keyVersion=";
v18 = (LPVOID)sub_4010DB((unsigned int)"mobile=");
if ( lpMem )
    sub_414DC4(lpMem);
v17 = 0;
v16 = 0;
v15 = 0;
v14 = 0;
v13 = 0;
v12 = 0;
v11 = 0;
v10 = 0;
v9 = 0;
v8 = "https://m.client. /mobileService/sendRadomNum.htm";
v7 = (LPVOID)sub_4089B0(
    &v8,

    v26 = (LPVOID)sub_4010DB((unsigned int)"isRemberPwd=false&loginStyle=0&deviceId=");
    if ( lpMem )
        sub_414DC4(lpMem);
    if ( v28 )
        sub_414DC4(v28);
    if ( v27 )
        sub_414DC4(v27);
    v25 = 0;
    v7 = 0;
    v24 = 0;
    v23 = 0;
    v5 = (_DWORD *)sub_414DBE(8u);
    v22 = v5;
    *v5 = 0;
    v5[1] = 0;
    v21 = 0;
    v20 = 0;
    v19 = 0;
    v18 = 0;
    v17 = 0;
    v16 = 0;
    v15 = 0;
    v14 = 0;
    v13 = 0;
    v12 = "Content-Type: application/x-www-form-urlencoded\r\nHost: m.client. \r\nUser-Agent: okhttp/3.9.1";
    v11 = 0;
    v10 = "https://m.client. /mobileService/radomLogin.htm";
    v9 = (LPVOID)sub_4034E0(
        &v10,
```


接下来软件使用以下接口获取优惠券的信息：

https://m.client.100**.com/welfare-mall-front-activity/mobile/activity/get619Activity/v1?
whetherFriday=YES&from=955000006

其部分代码片段如下所示：

```
v35 = "User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_0_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Mo"
      "bile/15E148 [redacted] version:iphone_c@7.0500}{systemVersion:dis}{yw_code:}";
v34 = 0;
v33 = 0;
v32 = 0;
lpMem = "https://m.client.[redacted]/welfare-mall-front-activity/mobile/activity/get619Activity/v1?whetherFriday=YES&from=955000006";
v30 = (LPVOID)sub_40B7A5(
      (int)&lpMem,

      v42 = "goodsName\\":\\"";
      sub_4115E9(&v53, &v42, &v43, &dword_5434F0, 1, 0, 0, 0, 0, &v46, 0, &v47, 0, 0, 0, 0, 0, 0, 0);
v42 = "goodsId\\":\\"";
sub_4115E9(&v53, &v42, &v43, &dword_5434F4, 1, 0, 0, 0, 0, &v46, 0, &v47, 0, 0, 0, 0, 0, 0, 0);
v42 = "price\\":\\"";
sub_4115E9(&v53, &v42, &v43, &dword_5434F8, 1, 0, 0, 0, 0, &v46, 0, &v47, 0, 0, 0, 0, 0, 0, 0);
v42 = "&Nowtime=";
sub_4115E9(&v53, &v42, &v43, &dword_5434FC, 1, 0, 0, 0, 0, &v46, 0, &v47, 0, 0, 0, 0, 0, 0, 0);
```

获取到优惠券信息后，用户即可开始使用工具抢购优惠券，使用的接口为：

https://m.client.100**.com/welfare-mall-front/mobile/api/bj2402/v1

其部分代码片段如下所示：

```
.text:0040F70D      mov     [ebp+var_C], eax
.text:0040F710      push   offset asc_4D5BF2 ; ":开始自动线程抢卷!(活动是每周五开始)"
.text:0040F715      push   [ebp+var_C]
.text:0040F718      push   offset asc_4D4E32 ; ":"
.text:0040F71D      push   [ebp+var_8]
.text:0040F720      push   offset asc_4D4E32 ; ":"
.text:0040F725      push   [ebp+lpMem]
.text:0040F728      push   offset asc_4D5C17 ; "已启动定时抢卷,将在"
.text:0040F72D      mov     ecx, 7
.text:0040F732      call   sub_4010DB
.text:0040F737      add     esp, 1Ch
-.-
```

循环抢券相关代码

```
while ( 1 )
{
    v20 = (LPVOID)sub_414DB8(4);
    if ( v20 != (LPVOID)-1 )
        break;
    lpMem = (LPVOID)sub_4010DB((unsigned int)"reqdata=%7B%22goodsId%22%3A%22");
    v20 = (LPVOID)sub_414DDC(1375797249, (LPCSTR)0x16012D10, 8, -1);
    v19 = 0;
    v18 = 0;
    v17 = 0;
    v16 = 0;
    v15 = 0;
    v14 = 0;
    v13 = 0;
    v12 = 0;
    v11 = 0;
    v10 = 0;
    v9 = 0;
    v8 = 0;
    v7 = 0;
    v6 = 0;
    v5 = "User-Agent: Mozilla/5.0 (iPhone; CPU iPhone OS 14_0_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) M"
        "obile/15E148 {version:iphone_c@7.0500}{systemVersion:dis}{yw_code:}";
    v4 = 0;
    v3 = "https://m.client. /welfare-mall-front/mobile/api/bj2402/v1";
    v2 = (LPVOID)sub_40B7A5(
        (int)&v3,
```

抢到之后自行去APP-我的订单-积分订单支付即可。

基于以上分析，该工具软件属于典型的“黄牛”抢购软件，抢占了普通用户的资源，导致运营商为普通用户提供的商品优惠，被少数黄牛党非法获取，破坏了诚信、公平交易的市场秩序。

版本更迭差异：

该作恶工具首次发现时间为8月29日，在Karma业务情报搜索引擎中我们发现该工具进行了多次的版本迭代，每次迭代都在降低黑产利用该工具的门槛，扩大该工具的影响力，继而影响后续越来越多的黑产开始利用该工具进行作恶。

版本	发现时间	功能状态
V1.0	8月29日	不支持发送验证码、不支持登录获取Cookies，需要用户自己手动利用抓包工具提取cookie、不支持定时、不支持库存捡漏
V1.1	9月3日	支持发送验证码、支持登陆并获取cookie
V1.3	9月4日	支持定时抢购、库存捡漏功能。
V1.4	9月18日	从V1.3版本起，该工具已经实现了登录账号即可抢购的功能，后续升级无前台新功能上线
V1.5	10月1日	
V1.51	10月2日	
V1.52	10月6日	

该工具各版本间对比

3) 黑灰产成本与获利

黑产在抢购成功后需支付对应的积分或金额，成本为10元。而在券码转售方面，转售价格一般为券码标价的8折，即30元的券码可销售价格为24元左右，去除掉成本后利润为14元左右。

成本：抢购成功后支付10元。

获利：出售券码价格24元，利润14元左右。

4) 攻防建议

该工具会定时循环访问厂商的https://m.client.100**.com/welfare-mall-front/mobile/api/bj2402/v1这个接口，且部分请求头的值写死在代码中，因此厂商可以以“是否定时循环访问该接口、多个账号请求头值相同”特征来区分出是自动化工具还是正常用户发起的请求。

从业务可用性的角度来说，由于该活动接口调用的是m.client.100**.com这个应用统一的接口来源，导致当该域名访问请求数量过多将造成整个连锁反应，严重影响其他用户的体验，可以通过拆分请求接口至活动专用接口，从而避免连锁反应，影响应用内其他业务的运转。

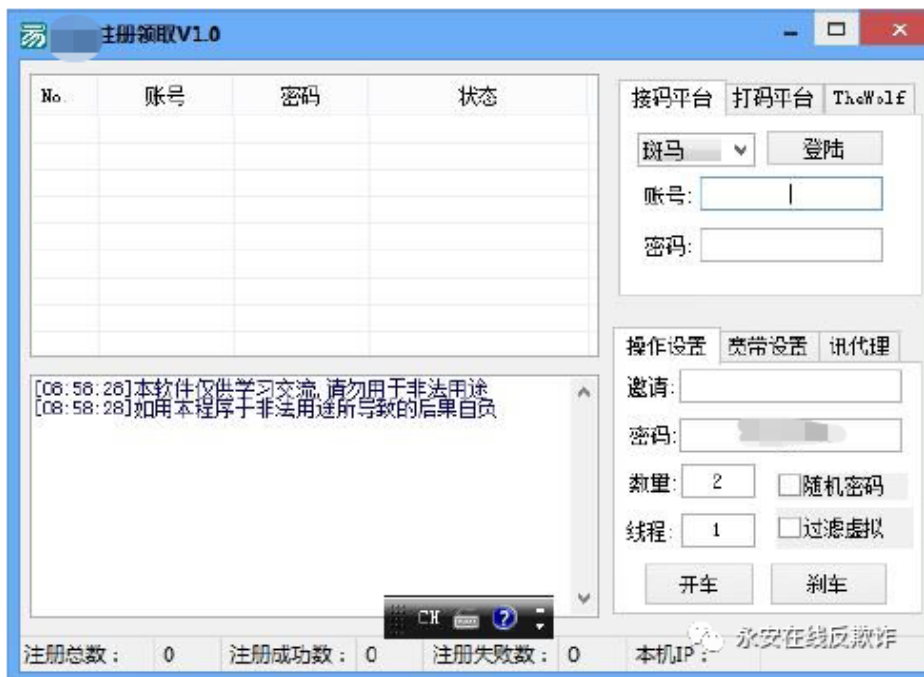
2.3 注册机工具

2.3.1 分析方法

注册机工具：xx注册领取V1.0.exe

工具用户：使用该工具的用户主要是专注于恶意注册领券的黑产。

工具攻击手法：这是一款运行在PC 电脑上的黑灰产专用工具，通过直接破解和伪造该app端与服务器的通信协议，自动化登录、注册等操作。相比于模拟按键脚本，协议工具脱离了设备的限制，黑产可以更低成本完成批量化规模化作案，因此危害也更加严重。



xx注册领取工具截图

工具分析：

工具登录过程中构造并访问了两个接口，这两个接口走的 https协议，请求方式为 POST，黑产通过抓包分析该电商app，可以轻易获取到相关信息，进而伪造接口协议和参数。通过逆向分析，我们发现工具通过接码平台获取手机号，然后得到验证码直接登录。

platform	android	hardcode
appId		hardcode
channel		hardcode
v	4.37.6	hardcode
loginToken	“ ”	hardcode
deviceTrait	RMX1931	hardcode
timestamp		动态获取
iid	“ ”	空值
oaid	“ ”	空值

某接口的参数列表

攻防建议：

从该工具的汇编代码中提取出的接口参数，大多数参数为硬编码hardcode的，因此平台可以基于这些hardcode的参数作为特征来识别工具发起的注册请求。

同时在这个工具中，我们看到了黑产在高净值恶意注册攻击上采用的技术：注册机不再是仅有单一的注册功能，现在还会集成自动化接码平台与内建网络模块，利用宽带秒拨和代理IP去多线程绕过平台的业务安全风控体系。黑产采用复合的攻击手段，使得现有的注册风控环节存在可被绕过的风险，此时平台可以结合风险IP画像和风险手机号画像，拦截黑产批量注册虚假账户的过程，或在登录环节上对相关账户进行业务层面的限制，以避免造成损失。

2.3.2 案例：利用集鞋卡活动进行牟利的“追鞋人”

关键字：电商抢购 薅羊毛 恶意注册

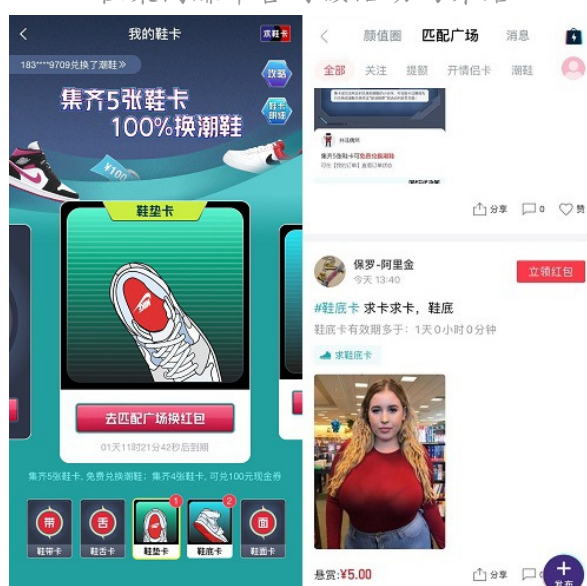
发现时间：2020年9月

1) 自动化兑换工具

某金融应用为拉动用户增长，推出了“集鞋卡换潮鞋”活动，用户通过参加活动，完成活动任务获得“鞋卡”。用户集齐鞋卡之后，可选择自己喜好的潮鞋进行兑换。但是由于活动方在不同时间放出的潮鞋种类及数量有限，并且部分价值相对较高的潮鞋需求量大，所以需要以“抢购”的方式去兑换潮鞋。在活动上线不久后，永安在线业务风险感知平台发现了针对该活动的工具，该工具可自动化完成兑换潮鞋的过程。



在某网赚平台对该活动的介绍

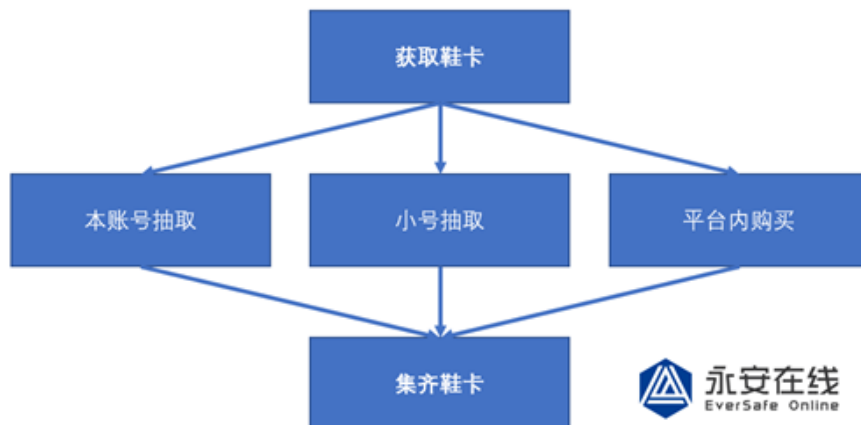


应用内截图

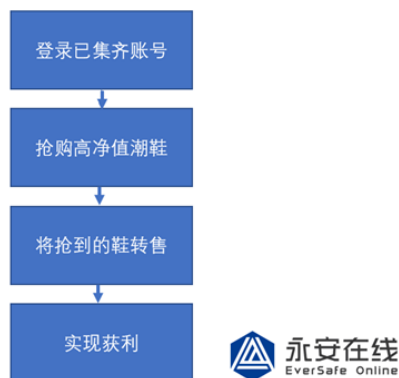
2) 薅羊毛逻辑

利用大量账号领取鞋卡，并在匹配广场进行一定的卡片交易，从而集齐鞋卡。在集齐鞋卡后通过抢购工具将价值相对较高的鞋抢购到手后再到其他平台销售。

集齐鞋卡流程



抢购流程



3) 工具分析

软件运行截图如下：



潮鞋兑换信息配置

场次 选择鞋码 输入 token 更多设置 提前打码参数

token:

交易密码:

IP地址/可留空/在更多设置里面可以载入:

帐号配置

场次 选择鞋码 输入 token 更多设置 提前打码参数

延迟/毫秒 1秒=1000毫秒:

订单号:

打码秘钥:

秘钥:

打码次数:

开始提前打码

熊猫代理 载入

黑灰产相关资源配置

攻击的目标接口:

https://api.***.com/v2/card/exchange/checkShare

https://api.***.com/v2/card/exchange/confirm

https://api.***.com/v2/card/exchange/skuInfo

https://api.***.com/v2/order/address/all.json

https://api.***.com/v2/shoes/card/sessionList

这是一款PC端的协议工具，需事先准备已集齐鞋卡的帐号token及交易密码，鞋卡可通过“悬赏红包”的方式获得。

2、用户发布【求鞋卡】动态可指定其所期望获得的鞋卡以及鞋卡剩余有效期，并设置悬赏红包，第一个赠与【求鞋卡】动态作者所期望获得的鞋卡的用户可得到悬赏红包；悬赏红包被领取前，可以撤销或重新设置；悬赏红包被领取后，不可撤销。

3、【求鞋卡】动态附加悬赏红包大小，属于用户自发行为，与平台无关。悬赏红包仅可用于活跃氛围，平台严禁鞋卡炒作、投机等行为，一经发现，平台有权禁止违规用户继续参与后续鞋卡发售活动；收集或赠与鞋卡时请注意鞋卡的有效期限，避免因鞋卡过期带来不必要的损失，过期的鞋卡不可兑换现金券或者潮鞋等奖品、不可赠与他人，不可折现。

也可以利用接码平台来完成邀请新用户获取鞋卡，但邀请新用户获取鞋卡的数量有上限，通过该方式集齐鞋卡的难度较大。

03 邀请好友规则

1、每成功邀请一位新用户（以下或称“好友”）首次下载并使用本APP，用户（以下或称为“邀请者”）有机会获得鞋卡奖励。邀请者可将活动页面通过微信、QQ或者微博、链接、短信等方式分享给好友且好友首次下载新浪分期APP（需注册新浪分期账号并登录APP），则视为邀请者邀请好友成功。

2、通过邀请好友所得鞋卡存在上限，达到该上限后，邀请者通过邀请好友暂无法获得鞋卡奖励，每个新用户只能被邀请一次，同一个登录账号、同一个手机号、同一个设备或同一提现账户，都视为同一个用户。

该工具内置了2个代理平台，用于绕过平台针对IP的风控策略。

hxxp://www.***daili.cn/

hxxp://www.*****daili.com/

还内置了1个打码平台，用于绕过验证码。

https://captcha.*****studio.cn/

4) 黑灰产成本与获利

黑灰产在抢到价值较高的潮鞋之后，再将潮鞋出售，从中获利。

成本：集齐鞋卡成本200~400元

获利：出售潮鞋500~5000元

5) 攻防建议

针对这种采取多个账号，并利用代理IP、验证码打码等方式绕过平台风控的工具，我们从业务层面可以利用风险IP画像中对相关IP的代理标签进行重视。同时，我们还可以通过相关账号的登录IP区域跨越来判断该账号用户行为是否异常，以判断该账号是否为黑产持有。

除了业务风控上的处理方案，由于奖品为实体商品，可以在物流和发奖流程上对其进行更为严苛的处理，针对相近地区的集中大量兑奖活动采取人工派奖、延后派奖、真人信息核验等方式，避免造成损失。

说明

1. 数据来源说明：

本报告数据来源于永安在线旗下Karma业务情报搜索引擎，基于Karma上监测到的数据进行取样分析，所得的数据分析结果与实际情况之间可能存在一定的偏差，敬请谅解。

2. 业务情报监测平台说明：

业务情报监测平台Karma，以攻击者的视角，依托强大的黑灰产布控能力及深层次的情报处理能力，帮助企业在业务环节精准筛选出恶意流量，还原风险场景，并量化对业务的影响，且持续对黑产进行实时监测，驱动风控决策引擎迭代，从而提升企业整体攻防效率。

版权申明

本报告版权属于深圳永安在线科技有限公司，并受法律保护。未经允许不得擅自转载、摘编或利用其它方式使用本报告文字或者观点，如需转载请联系永安在线。违反上述声明者，将追究其相关法律责任。



永安在线介绍

永安在线（EverSafe Online）成立于2017年，致力于成为企业客户的线上业务欺诈监控、预警、响应的专家。公司开创了以业务安全情报为核心的业务安全解决方案，通过强大的线上业务风险监控体系、风险情报数据能力、以及丰富的黑产攻防经验，帮助企业客户解决账号安全、营销反欺诈、流量欺诈、接口安全等线上业务欺诈问题，目前覆盖了90%的头部互联网客户累计合作客户超300+，每年帮助客户减少数十亿的资金损失。目前已合作的客户有：阿里巴巴、字节跳动、百度、京东、滴滴、贝壳找房、拼多多、爱奇艺、快手等。

联系方式

- ☎ 永安在线官方服务热线：400-809-3699
- ✉ 永安在线官方合作邮箱：marketing@yazx.com
- 🌐 永安在线官网地址：<https://www.yazx.com>



欢迎关注“永安在线”