编号：TH-HL-RJ-201809

互联网黑灰产工具软件

2018 半年报告

2018/09 期

报告编制：威胁猎人鬼谷实验室

发布日期：2018-09-15

版权申明

目 录

前言

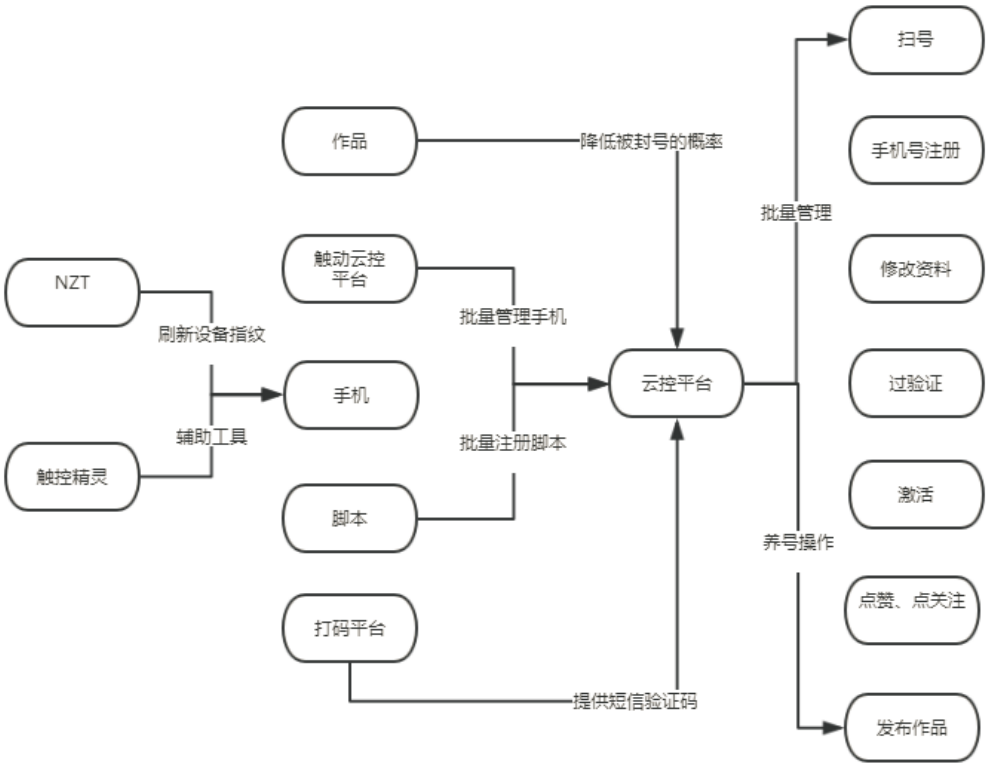
2017 年 5 月爆发的 Wannacry 勒索病毒造成了严重的影响，使得 NSA 武器库进入了大众的视野；在网络安全这片看不见硝烟的战场上，在战场的另外一个角落——互联网业务安全领域，黑灰产从业者手里也掌握着威力强大的武器库：各式各样的工具软件，而且不为人们熟知。如果说手机号、帐号、IP、设备等，是黑产从业者的弹药，那么工具软件就是将这些弹药威力发挥到最大的武器。而对于工具软件的分析和研究，是黑产研究的重要组成部分。

一、黑灰产工具软件特征分析

我们对过去半年捕获到的黑灰产工具软件进行了系统性的梳理和分析，发现现阶段黑灰产工具软件有如下一些明显的特征，深入理解这些特征，有助于我们对黑灰产业的发展有更加准确的掌控和判断。

1.1 与产业链深度整合

伴随着网络黑灰产的发展和成熟，如今的工具软件已经深度整合到了整个产业链当中，成为其中不可取代的一部分。以账号注册场景为例，黑灰产业除了掌握接码平台、打码平台和动态 IP 等资源外，还通过整合改机工具，模拟点击工具，批量扫号工具，代理软件工具等各类工具软件，实现了高度自动化和高度协同的作业流程，如下图：



1.2 极强的版本快速迭代能力

相较于正常的软件，黑灰产工具软件具有更快的版本更新迭代速度。以一款针对

京东的注册机工具软件为例，从 18 年 1 月到 18 年 4 月，我们共监控到该软件的 20 次版本更新，频繁时 1 天更新 2 个版本，如下图：

发现时间	软件版本号
2018 年 1 月 5 日	[注册客户端]京东注册 v18.0105.rar
2018 年 1 月 9 日	[注册客户端]京东注册 v18.0109.rar
2018 年 1 月 18 日	[注册客户端]京东注册 v18.0118.rar
2018 年 1 月 19 日	[注册客户端]京东注册 v18.0119.rar
2018 年 1 月 21 日	[注册客户端]京东注册 v18.0121.rar
2018 年 1 月 30 日	[注册客户端]京东注册 v18.0130.rar
2018 年 2 月 26 日	[注册客户端]京东注册 v18.0226.rar
2018 年 3 月 19 日	[注册客户端]京东注册 v18.0319.2.rar
2018 年 3 月 21 日	[注册客户端]京东注册 v18.0321.rar
2018 年 3 月 22 日	[注册客户端]京东注册 v18.0322.rar
2018 年 4 月 7 日	[注册客户端]京东注册 v18.0407.rar
2018 年 4 月 11 日	[注册客户端]京东注册 v18.04011.rar
2018 年 4 月 11 日	[注册客户端]京东注册 v18.04011.2.rar
2018 年 4 月 15 日	[注册客户端]京东注册 v18.04015.rar
2018 年 4 月 18 日	[注册客户端]京东注册 v18.0418.rar
2018 年 4 月 20 日	[注册客户端]京东注册 v18.0420.rar
2018 年 4 月 25 日	[注册客户端]京东注册 v18.0425.rar
2018 年 4 月 25 日	[注册客户端]京东注册 v18.0425.2.rar
2018 年 4 月 26 日	[注册客户端]京东注册 v18.0426.rar
2018 年 4 月 27 日	[注册客户端]京东注册 v18.0427.rar

除了增加新功能，修复 BUG 之外，频繁的版本更新是黑灰产从业人员跟业务安全团队攻防对抗加剧的体现。一个比较典型的场景：一款针对 X 厂商的工具软件发布一段时间之后，通过业务侧的数据和模型，X 厂商的业务安全团队感知到了由于工具软件产生的异常，并通过修复漏洞，改进检测模型等方式使工具软件失效；而工具软件的作者则需要重新找到新的突破口，然后发布新版本。

1.3 显著的逐利化趋向

如果说早些年的黑客工具软件多多少少存在炫技的成分，当下的黑灰产工具则已经变得非常“务实”，完全以利益为驱动。近些年互联网发展迅猛，尤其以短视频行业、自媒体行业和电子商务行业为首的一批互联网公司业务蓬勃发展；而寄生在这些公司业务上的黑灰产从业人员，有着非常敏锐的“商业”嗅觉。每当业务发展过程中

出现了一些薄弱点，很快就会出现利用此来攫取利益的工具软件，其中以针对营销活动的薅羊毛工具软件最为典型。美团在 18 年俄罗斯世界杯前夕推出了看球竞猜活动：

活动推出后不久，网络上就出现了 50 款以上针对该活动的工具软件，跟美团业务相关的工具软件中，竞猜类软件直接蹿升到第一位，如下图：

1.4 游走在法律边缘的灰色地带

自《中国人民共和国网络安全法》发布并严格执行以来，黑产从业者发生了两个明显的变化：一个是越来越多的人采用匿名通信，匿名交易的方式来隐藏自己；另外一个是明显触发法律的黑产工具，如盗号木马，远控木马，游戏外挂等，做的人越来越少。虽然也有铤而走险者，但更多的人还是会权衡风险和收益，做到最大化的趋利避害。以电商行业为例，虽然有人仍然利用一些木马类工具软件进行资金的盗取和诈骗，但更为活跃的是一些辅助类工具软件，比如商家辅助工具，提供数据采集和分析，店铺引流等功能。有些软件还在界面显著位置放置了免责声明（虽然不一定有用），如下图：

当然，随着法律的不断健全和完善，目前认为是法律边缘的“灰色”地带，未来某一天也可能不再会是“安全”地带，这也必然会再次带来从业人群，以及相关工具软件的集体迁移。

1.5 黑吃黑现象非常普遍

如果说黑灰产也是一个江湖，并不是所有的从业者都会遵守江湖规则，黑吃黑的现象非常普遍。这点在工具软件上，也体现得非常明显。在网络上传播的黑灰产工具软件中，很大一部分都存在各种各样的问题，对于刚进入这个江湖的“小白”来说，一不小心就会成为他人的盘中餐。根据我们的分析，有问题的工具软件主要有以下几类：

1、挂羊头卖狗肉类：这类工具软件根本没有其宣称的功能，却会在背后偷偷干其他一些事情。最典型的是一款流氓推广软件（注：运行之后会在后台下载并安装各种“全家桶”），以“刺激战场辅助外挂”，“流量宝疯狂刷量”，“抢红包神器”等名字在网络上传播量，每天的下载量超过 1 千以上；

2、买一送一类：简单来说就是二次打包，一些别有用心的人把正常的工具软件和病毒木马打包在一起，然后在放到网络上传播。由于黑灰产工具很多情况下都会被杀软报毒，所以即使真的有病毒，工具的使用者也会选择放行。经常使用黑灰产工具软件的人，其设备上往往也存在着各式各样的病毒；

3、请君入瓮类：一些黑灰产工具在使用之前，要先进行登录操作（比如针对腾讯业务的工具软件需要先登录 QQ 或微信，针对阿里业务的工具软件需要先登录淘宝），因为在一些情况下需要拿到登录态才能进行下一步的操作。然而，输入的账号和密码不仅仅用于业务的登录，还发送到了一些别有用心的工具软件制作者手里；

4、夸大其辞类：这种一般出现在收费类工具软件中。花大价钱买了所谓的牛逼工具，比如“百分百修改机器码”，“VIP 会员破解”，“全自动秒杀”等，用起来发现实际效果很差，甚至没有效果。工具的买家遇到这种情况肯定是投诉无门，只能咬碎了牙往肚里吞。

所以，奉劝一下打算进入这个江湖的人，黑产有风险，入行需谨慎。

二、不断进化的方法和手段

根据威胁猎人 TH-Karma 业务情报监测平台统计，每天互联网上新产生的各式各样的黑灰产工具软件，包括软件更新，超过 1 千款以上。这些工具软件伴随着互联网技术和 IT 技术的发展，也在不断的发展和进化中。

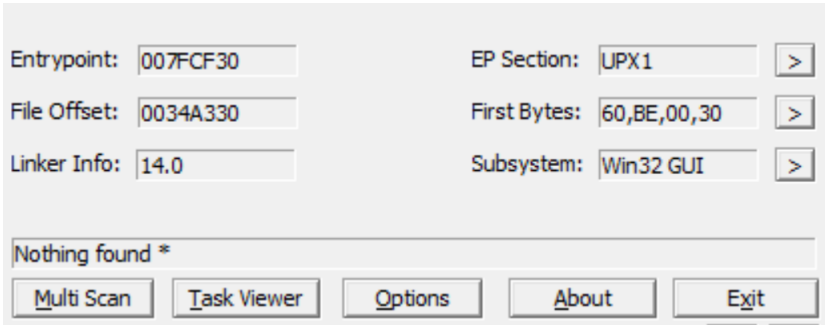
2.1 从模拟脚本到多种开发语言

黑灰产工具软件在早期，大多以通过模拟人工操作的方式实现攻击，比如基于按键精灵、大漠插件等编写定制化的脚本，就可以通过模拟点击完成注册，登录，刷金币等操作。这种方式简单，学习门槛低，但是使用的场景受限，效率也偏低。

后来也出现了基于 VB/C/C++等高级语言编写的黑灰产工具软件，这类工具软件不再基于模拟人工操作的方式，更多的是基于网络协议的破解和重放，直接攻击业务接口，从而可以在单位时间内发起更多的攻击次数，将利润最大化。不过这类编程语言开发难度较高，需要开发者具备比较好的编程能力。

如今的黑灰产工具软件，则多以易语言、C#、Python、Lua 等语言编写。这些语言由于功能化模块和框架比较完善，很多复杂功能通过一个简单的调用就可以完成，有着上手快，开发周期短的优点。尤其是易语言和 C#，我们过去几个月捕获的 PC 端黑灰产工具软件，超过 50%都是采用这两个语言编写。

除此之外，为了保护自己的核心代码逻辑不被他们发现，目前很多工具软件还会使用一些加壳软件给自己加壳。下图是一款基于 C#编写的破解百度网盘下载限速的工具软件，本身加了 UPX 壳：



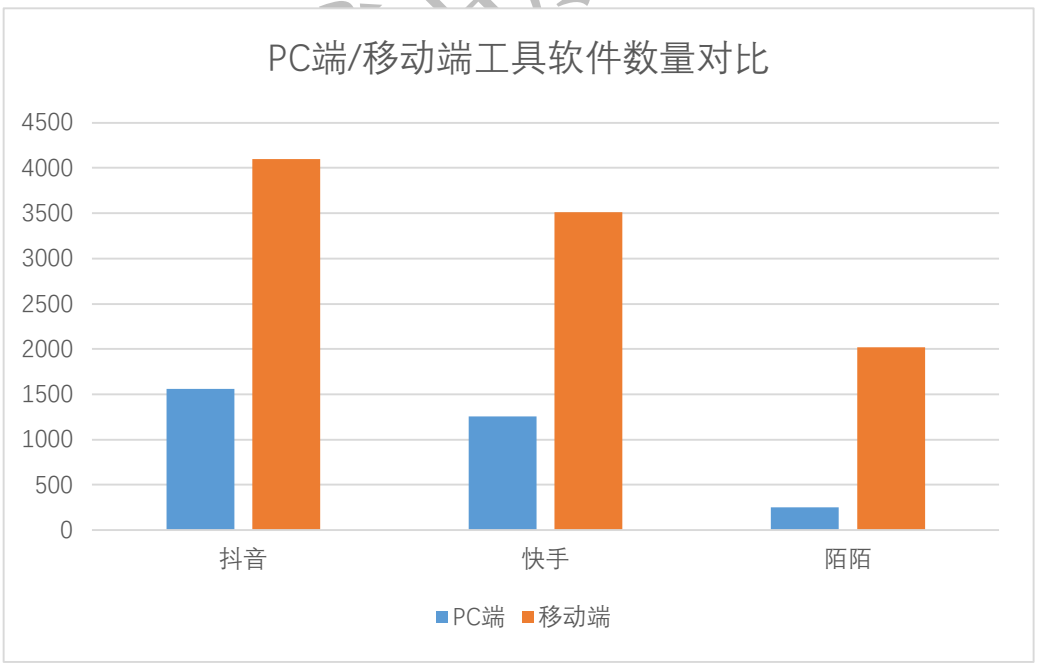
相对于 VMProtect，DNGuardHVM 等强壳，UPX 壳比较容易脱掉；脱壳之后，可以找

出其核心代码逻辑，下图是拼接百度网盘下载链接的代码片段：

```
value: function(e) {
                    var t = this.getPrefixLength();
                    for (var n in e) this.fileDownloadInfo.push({
                        name: e[n].path.substr(t),
                        link: location.protocol +
"//pcs.baidu.com/rest/2.0/pcs/file?method=download&app_id=250528
&path=" + encodeURIComponent(e[n].path),
                        md5: e[n].md5
                    });
                    return Promise.resolve()
                }
```

2.2 从 PC 端到多端支持

随着近年来移动互联网的高速发展，塑造了全新的服务体验和生活形态；互联网的产品、服务以及用户也从 PC 端更多的迁移到了移动端。对于黑灰产从业人员来说，他们所使用的工具软件，也从 PC 端发展到了移动端。从目前最火的短视频行业来看，过去几个月我们捕获了大量的黑灰产工具软件，移动端的数量已经远远超过了 PC 端，如下图：



相较于 PC 端工具软件，移动端工具软件可以通过外挂的方式，实现更低的对抗成本。经过我们分析，捕获的短视频行业黑灰产工具中，就有大量基于按键精灵安卓版

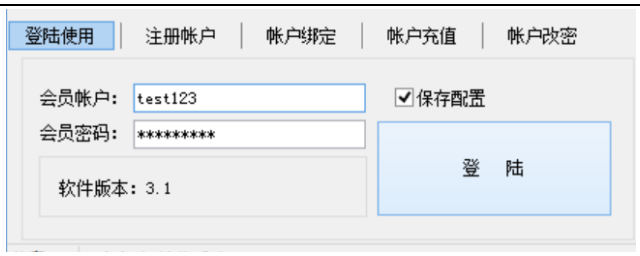
和易安卓编写的黑灰产工具，覆盖了注册，刷量，引流等黑灰产核心业务场景，如下图：

注册机	陌陌批量注册2018-05-01_015811.apk
注册机	陌陌批量注册2018-05-01_134610.apk
注册机	陌陌批量注册2018-05-01_170054.apk
注册机	陌陌批量注册2018-05-09_103551.apk
注册机	陌陌批量注册2018-05-10_130412.apk
注册机	陌陌批量注册2018-05-16_155650.apk
刷量	陌陌评论1.02018-04-09_024220.apk
刷量	陌陌评论1.22018-04-09_195258.apk
刷量	陌陌评论1.52018-04-14_193518.apk
引流	陌陌群组引流2018-05-17_163550.apk
引流	陌陌群组引流2018-05-17_172801.apk
刷量	陌陌刷直播间1.02018-03-18_160047.apk
刷量	陌陌刷直播间1.32018-03-18_200441.apk
刷量	陌陌刷直播间1.32018-03-18_200441.apk(1).1
引流	陌陌引流2018-01-27_195531.apk
引流	陌陌引流2018-05-11_002728.apk
引流	陌陌引流2018-05-11_111238.apk
引流	陌陌引流2018-05-13_101822.apk
引流	陌陌引流3.02018-03-15_234312.apk
引流	陌陌引流3.92018-04-02_174144.apk
引流	陌陌引流4.12018-04-13_142437.apk
引流	陌陌引流4.22018-05-15_150425.apk
引流	陌陌引流4.22018-05-15_150425.apk
引流	陌陌引流4.32018-05-16_060243.apk
引流	陌陌引流v4.02018-04-06_225322.apk
引流	陌陌引流-飞缘-4.22.apk
引流	陌陌引流脚本2018-03-18_172620.apk
引流	陌陌引流脚本4.102018-04-10_223129.apk
引流	陌陌引流脚本4月18号.apk
引流	陌陌引流脚本正式版.apk
引流	陌陌引流软件2018-03-14_223954.apk

图 1

2.3 从终端发展到云端

如果说黑灰产工具软件从 PC 端发展到移动端是现在的趋势，那么从终端走向云端则是未来的趋势，部分工具软件已经体现出来了这样的特点。以我们分析的一款刷视频播放量的软件为例，从今年 7 月份开始，终端的工具软件只保留了登录，注册，充值等基本功能，登录后可以发布任务，但刷视频播放量的核心逻辑已经放到了云端：



促成工具软件从终端往云端化发展，主要有两方面的原因：

1、黑灰产技术的发展，特别是群控/云控系统等技术的发展，使得部分黑灰产从业人员手中掌握了大量的帐号和设备资源，如下图：

图 2

对于这些人而言，不再需要开发专门的工具软件给到下游的终端设备上使用，下游只需要通过网页或者其他方式提交任务需求，所有动作都可以在其掌握的大量云端设备上完成；

2、终端的黑灰产工具软件，即使只是在小圈子内传播，也可以比较容易被外界获取到，然后通过逆向分析等方式获取到该工具的核心逻辑，从而被业务侧封杀，或者被他人模仿；云端化则将工具的核心逻辑隐藏到了后端，对于外界来说就是一个黑盒，想要封杀或者模仿的难度大大增加。

2.4 从机械执行到机器学习

早期的工具软件，执行的核心逻辑大多是 Hardcode 在程序代码里面，或者通过编写任务脚本的方式来指定。虽然编写简单，但都是机械的执行固定的逻辑，不仅缺乏扩展性和自适应能力，比如针对不同的屏幕分辨率，需要编写不同的脚本，也比较容易被检测和拦截。

随着 IT 技术的不断发展，特别是近些年机器学习和深度学习在图像识别等领域取得长足进展，黑灰产工具软件也完成了自身的技术升级。以验证码为例，厂商通过验证码来识别人和机器，从简单的字母/数字开始演变到现在流行的滑块验证码，甚至各种验证码组合使用；另一方面，发展到今天，黑灰产从业人员手里已经拥有了完整的基于深度学习的验证码识别系统，无论是从获取验证码的响应速度还是识别准确率都远高于传统的打码平台（注：传统的打码平台主要依赖于人工输入或者以针对某个网站生成的验证码识别库）。如图 3.1 和 3.2 所示：

图 3.1

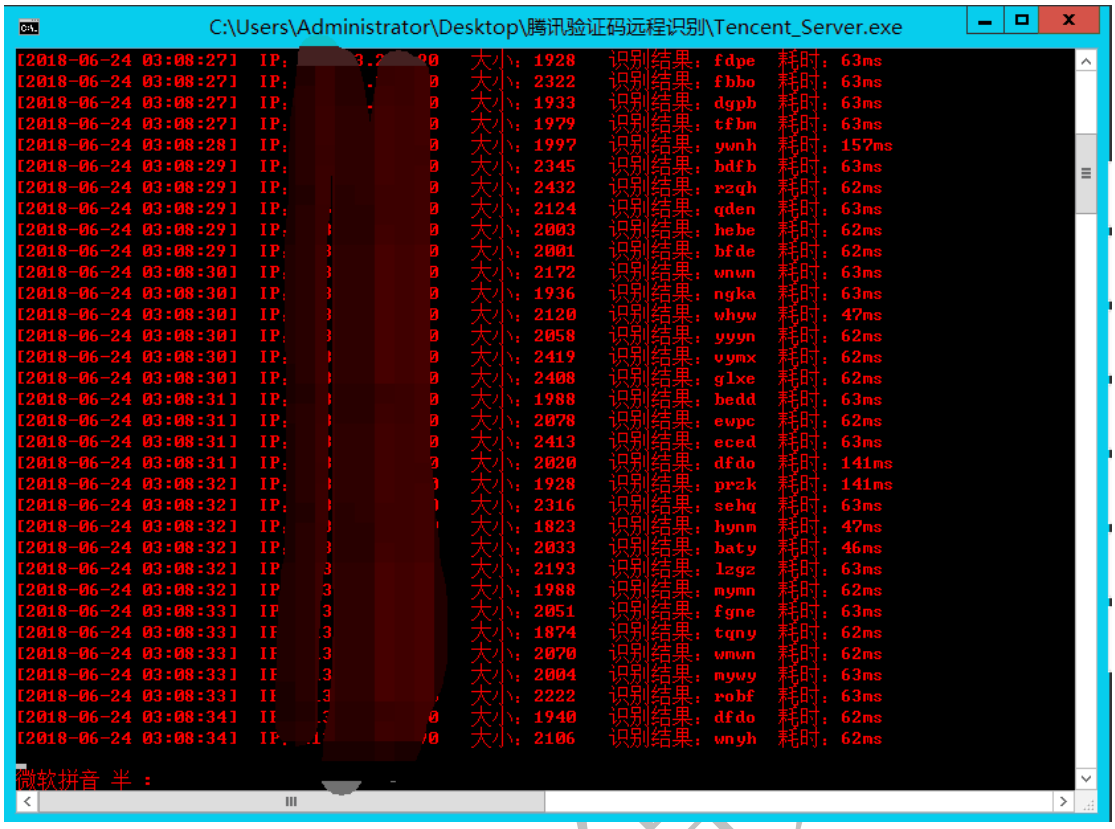
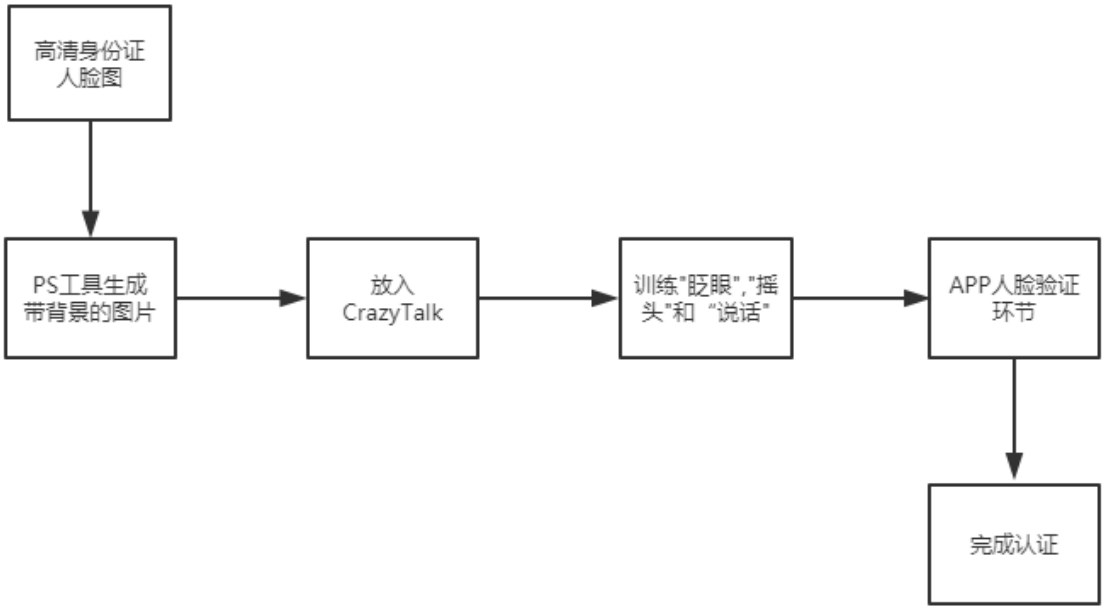


图 3.2

另一个典型的例子是过脸认证。专业的过脸认证软件可以通过简单的自拍照，快速生成 3D 人脸模型，以及快速模拟人脸做出简单的认证动作，从而绕过注册或登录环节的人脸识别。



三、业务安全中活跃的黑灰产工具

根据我们捕获的黑灰产工具软件情报分析，目前活跃的工具软件按照业务功能，大致可分为 5 大类：账号类、刷量类、薅羊毛类、内容爬取类和特定功能类。每种类型的工具数量占比如下图所示：

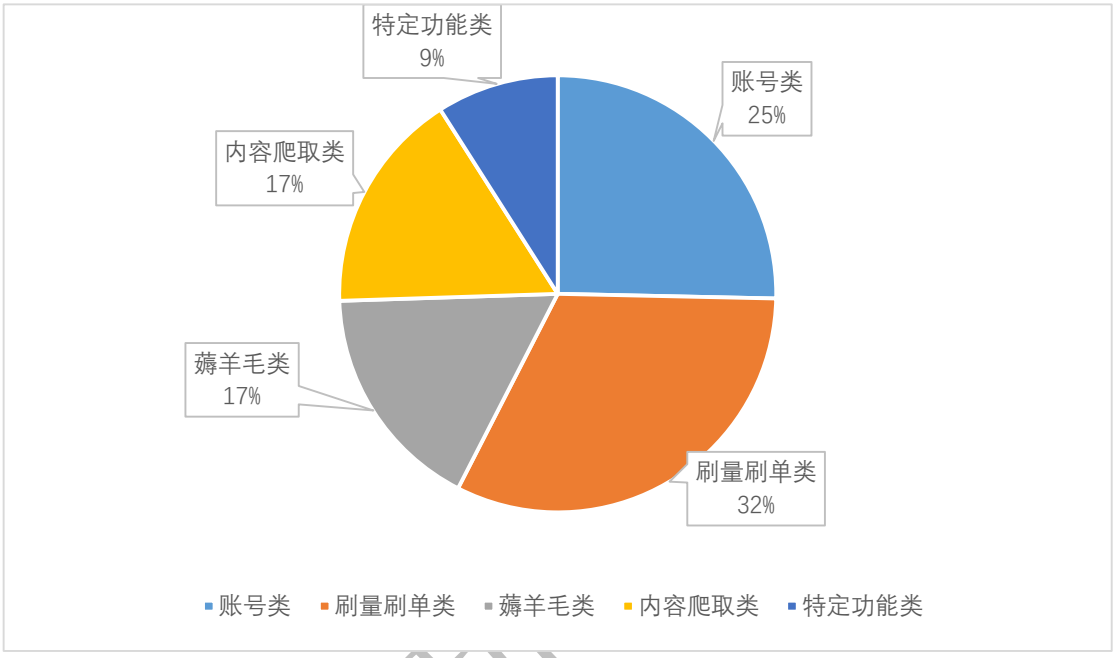


图 3-1 工具功能类型占比

在业务安全对抗中，刷量刷单类是黑灰产最常用的攻击工具，也是活跃度最高的一类工具，如刷文章阅读量、刷视频播放量、刷粉丝量和刷订单数量等，这类攻击集中体现在自媒体行业、电商行业和视频行业；除此之外，账号类、薅羊毛类和内容爬取类工具也活跃于黑灰产和厂商业务安全对抗中；特定功能类工具则主要包括模拟器、多开、改机和秒拨等功能性工具软件。

3.1 账号类工具软件

在大部分黑产链中，账号的质量和数量很大程度决定了黑产的投入产出比。账号类工具软件主要针对注册场景和登陆场景，实现的功能包括批量注册、扫号、鉴权和越权等。以“火牛注册扫号软件”为例，该工具直接和接码平台对接，用于接收短信验证码；同时内置 VPS 拨号功能用于绕过厂商的 IP 限制策略，从而完成帐号的批量注册和扫号。

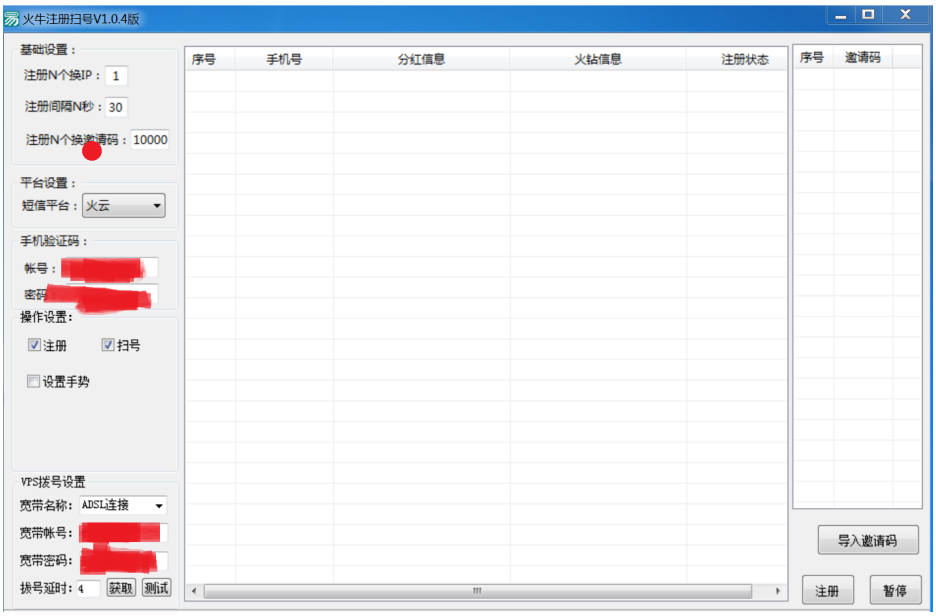


图 3-1-1 火牛注册扫号软件

帐号类的工具软件的牟利方式包括：1、直接对外出售批量注册的小号、对账号售卖有一定的分销制度，不同等级的代理拿货价格不一；2、通过将批量注册的小号用于刷量、引流的业务场景，像 qq、email、微博号本身对其他厂商的业务可做授权服务，这类账号称为跳转号，同时跳转号的成本低廉；3、批量针对厂商推广活动的定制化小号，结合接码平台、打码平台等完成全自动化欺诈作业，短时间内薅取大量用户奖金。

如今以账号为核心的黑灰产业链在各行业的发展都具有一定规模，尤其是在需要大规模账号刷量的业务场景，包括虚假注册、实名过脸、批量养号和刷量等。除去明显给厂商业务带来明显的薅羊毛伤害，更多的是虚假小号带来潜在的危害性。比如黄赌毒的传播，以及被使用于引流诈骗场景给厂商带来不良的舆论效果。下表是近期我们监控到的一些比较活跃的账号类工具软件：

工具名称	活跃度
百度云 PC 破解版	高
PanDownload	高
今日头条账号注册机	中
爱奇艺会员扫描器	中
火牛扫号查询	中

表 3-1-1 活跃的账号类工具

3.2 刷量刷单类工具软件

刷量刷单类工具软件主要活跃在电商、自媒体、短视频等行业，主要功能包括刷成交量、刷阅读量、刷播放量、刷关注量、刷粉丝量、以及刷评论量等。以“久久快手刷播放”为例，该工具首先批量加载一批快手小号的 Token，然后通过模拟网络请求的方式，访问指定的快手作品网址，最终可以成功刷取播放量。

图 3-2-1 久久快手刷播放

刷量刷单类工具软件的牟利方式包括：1、通过提供刷量、刷单服务对任务发布者收取佣金；2、针对电商平台对商家补贴的运费，通过结合空包物流服务，发起退货请求薅取补贴；3、将点赞和刷评论结合，在用户作品下置顶评论，通过个人介绍或是评论内容出粉，出粉价格按引入其他平台账号个数计数等。

下表是近期我们监控到的一些比较活跃的刷量刷单类工具软件：

工具名称	活跃度
快手刷粉丝软件	中
今日头条（关注+私信+评论）	高
招财空包网拼多多辅助	中
淘宝全自动刷单软件	中
拼多多自动发空包单软件	中

表 3-2-1 活跃的刷量刷单类工具

3.3 薅羊毛类工具软件

薅羊毛类工具软件主要活跃于营销活动、电商抢购、红包领取等场景。以“瓦力抢红包”为例，该工具通过开通辅助功能，模拟点击控件从而实现抢红包及自动回复等功能。

图 3-2-2 瓦利抢红包

薅羊毛类工具软件的牟利方式包括：1、直接出售工具软件获利；2、利用工具领取平台推出的优惠券或减免红包等，或者将优惠券、红包等转手出售；3、将抢购到的物品二次出售，从而赚取差价等。

下表是近期我们监控到的一些比较活跃的薅羊毛类工具软件：

工具名称	活跃度
刀锋京东抢购软件 V3.06	中
京东申请试用（撸实物）V1.0	中
京东火牛-下单抢购软件 1087	高
聚划算红包监控	中
京东火牛-查券领券软件 545	中

表 3-2-3 活跃的薅羊毛类工具

3.4 内容爬取类工具软件

内容爬取类工具软件主要通过爬虫程序，采集电商数据、短视频用户作品、招聘网站简历和自媒体文章等。近期我们就发现有多款工具软件对拼多多的商品信息、店铺信息、拼团信息等数据进行爬取。以“拼多多精灵”为例，该工具软件通过请求 apiv4.yangkeduo.com 下的接口来爬取拼多多数据， 提供开团提醒、关键词排名、类目排名、导出订单、物流监控、退款提醒、竞品对手监控等功能：

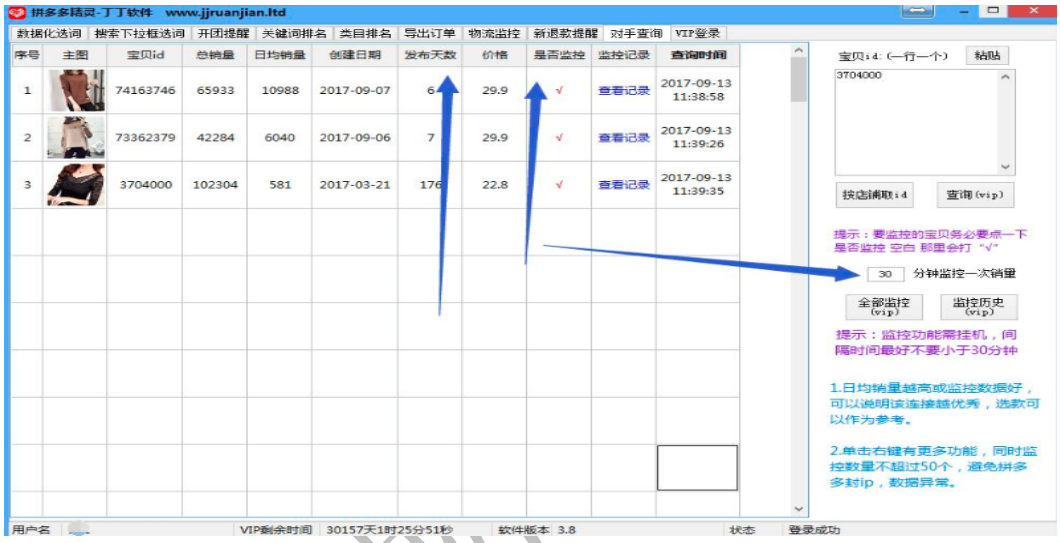


图 3-2-3 拼多多精灵截图 1

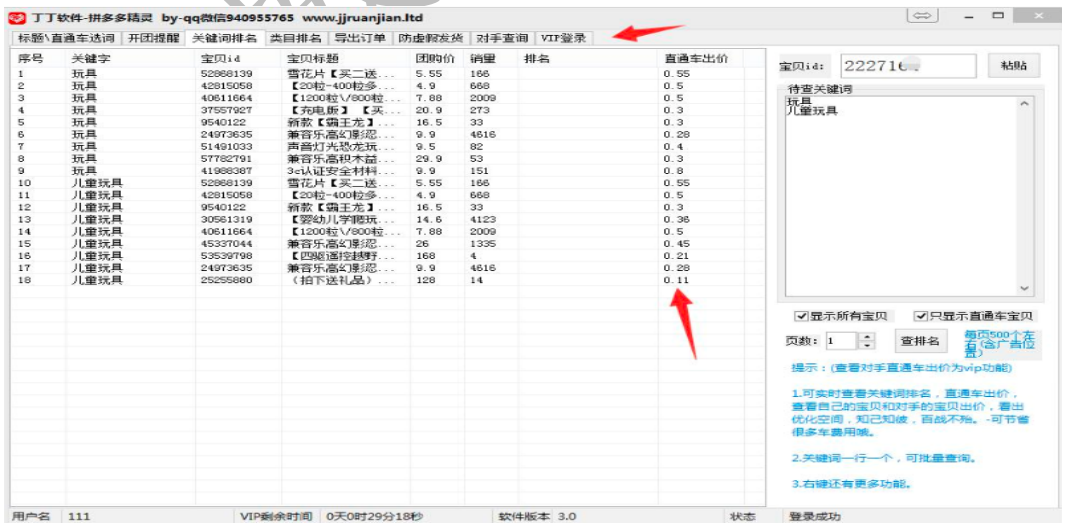


图 3-2-4 拼多多精灵截图 2

内容爬取类工具软件的牟利方式包括：1、利用采集的拼多多数据，提供数据分

析服务和店铺管理服务获利，包括关键词排名、商品排名、开团监控、一键下订单、一键发货和多个店铺管理等；2、当店家在使用这些工具时，很可能导致订单数据泄露，黑灰产可以通过出售这些数据或利用数据进行营销和诈骗等来获利。

下表是近期我们监控到的比较活跃的内容爬取类工具软件：

工具名称	活跃度
多多管家	高
多多参谋	高
麦兜兜/单手街/笨笨代购	中
多多易赞	中
神马上货助手	中

表 3-2-4 内容爬取类工具软件

3.5 特定功能类工具软件

特定功能类工具软件主要包括模拟器、多开、改机和秒拨等功能工具软件，常见应用于注册账号、邀请新用户领取红包、刷赞、刷分享、刷评分和刷榜等场景。特定功能类工具软件种类和数量不多，但是黑灰产业链中也发挥着极其关键的作用。

以改机软件“海鱼魔器”为例，在抖音引流这个场景，利用改机可以伪造位置，利用抖音附近视频的功能做引流，诱导附近看到视频的人添加微信小号。

图 3-5-1

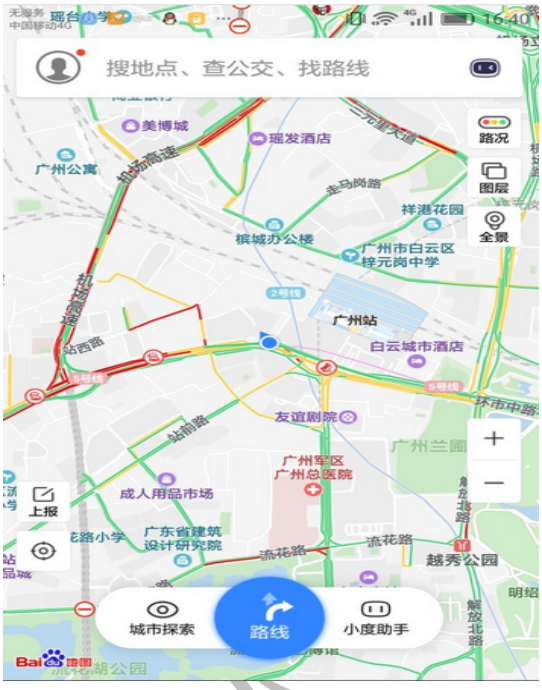


图 3-5-2

如上图，借助改机软件将所在地点修改到人流量多的广州火车站，然后通过抖音上传“精心”制作的美女视频或图片，并配上包含微信号的文字，最终将上钩的男性用户定向引流至销售男性用品的微商，或被诱导发红包观看色情视频，最终上当受骗。

特定功能类工具软件虽然不参与直接牟利，但提供的功能可以帮助黑灰产更好的攫取利益。比如改机工具，除了上面提到的引流场景外，在账号注册场景也很重要，可以实现一个设备多次复用的效果。下表是近期我们监控到的比较活跃的特定功能类工具软件：

工具名称	活跃度
深海鱼乐	中
iGrimace	高
007 改机	中
NTZ	中
AWZ	中

表 3-5　活跃的特定功能类工具

四、典型的黑灰产工具软件分析

过去半年我们对黑灰产工具软件做了大量的研究和分析，包括对其中一些工具软件做了深入的功能验证、动态调试和原理分析。我们选取几款比较典型的工具软件，进一步揭露其功能和原理。

4.1. B 站手机注册机 3.0

这是 6 月份捕获的一款针对 B 站的注册类工具软件，采用 C++语言编写。通过使用接码平台手机号接收手机验证码，同时内置深度学习框架 Caffe 识别图像验证码，完成帐号批量注册。 程序运行界面如下图：

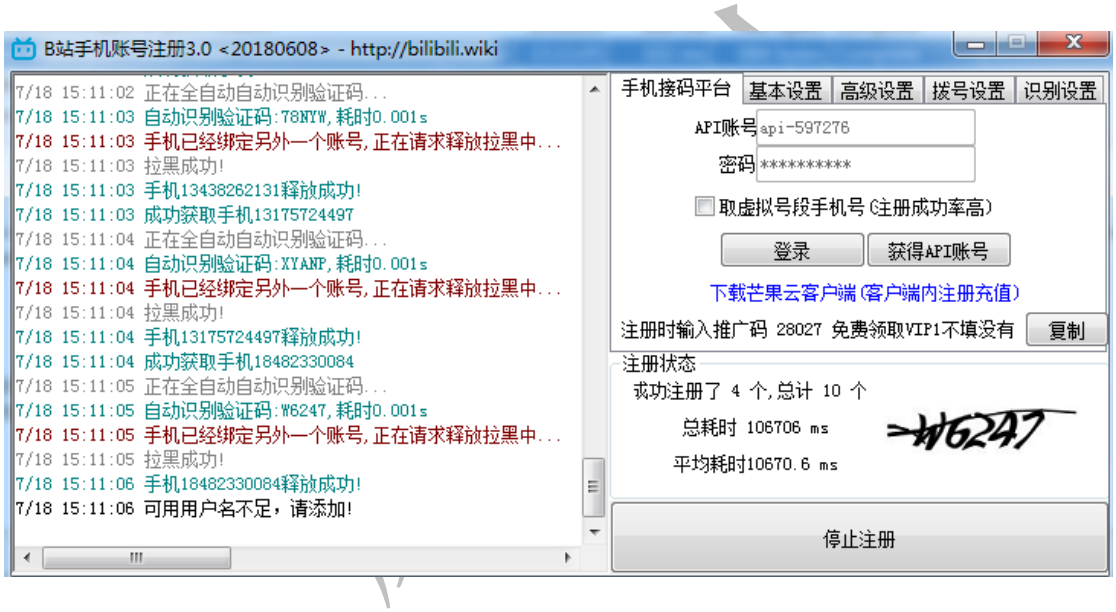


图 4-1-1 B 站手机注册机运行界面

程序会登录接码平台：

http://www.7gxyun.com:9000/soft.html

接收短信验证码，接着调用 B 站注册接口：

https://passport.bilibili.com/register/phone

以及验证码下发接口：

https://passport.bilibili.com/captcha

提取到验证码，如下图：

之后该工具会使用内置的深度学习框架 Caffe 识别图片验证码。识别验证码的过程会读取本地内置深度学习框架 Caffe 框架所需要的 3 个文件：deploy.prototxt，res_lstm_ctc_iter.caffemodel，label-map.txt。其中 deploy.prototxt 部分代码如下：

```
name: "Res_LSTM_CTC"
input: "data"
input_shape{
    dim:1
    dim:3
    dim:50
    dim:200
}
layer {
  include {
    phase: TEST
  }
    name: "indicator"
    type: "ContinuationIndicator"
    bottom: "data"
    top: "indicator"
    continuation_indicator_param {
        time_step:  25
        batch_size: 1
    }
}

#注解：dim:1表示对待识别样本进行数据增广的数量
       dim:3表示处理的图像的通道数RGB
       dim:50图像的长度
       dim:200图像的宽度
 res_lstm_ctc_iter.caffemodel：已经训练好的模型文件
```

图 4-1-2 deploy.prototxt 代码截图

图像验证码识别成功后，完成帐号注册。

该工具的亮点我们以往看到的工具不一样的地方的是用到了深度学习的图像识别能力，并且这个图像识别的准确率达到了 99%以上，平均完成一个账号的注册时间大约在 10 秒内。以往这一类的注册工具绝大多数会接一个打码平台或者内置一个针对目标网站的一个验证码识别库，无论是从识别准确率还是注册效率远比利用深度学习图像识别的低很多。

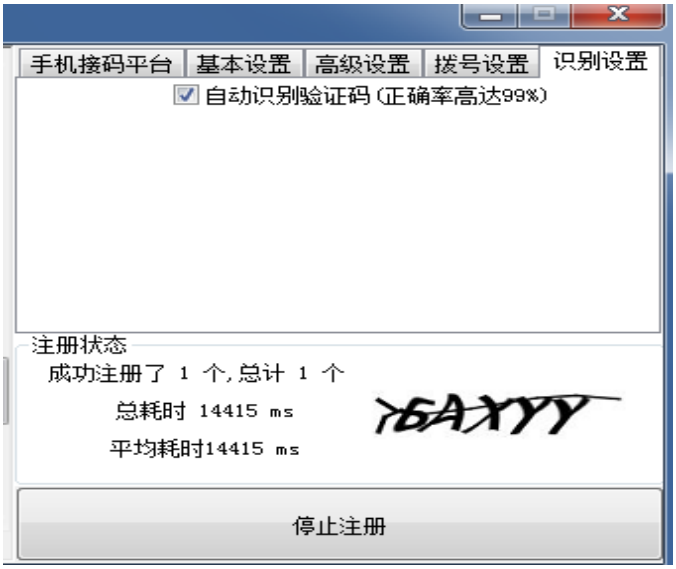


图 4-1-3 深度学习运用于验证码识别

4.2. 陌陌抢红包工具

这是 7 月份捕获的一款针对陌陌的抢红包类工具软件，基于按键精灵安卓版实现。通过自定义录制对手机屏幕的操作及重复次数等信息，按照一定模式进行对手机进行模拟操作从而实现抢红包等功能。工具运行如下图所示：

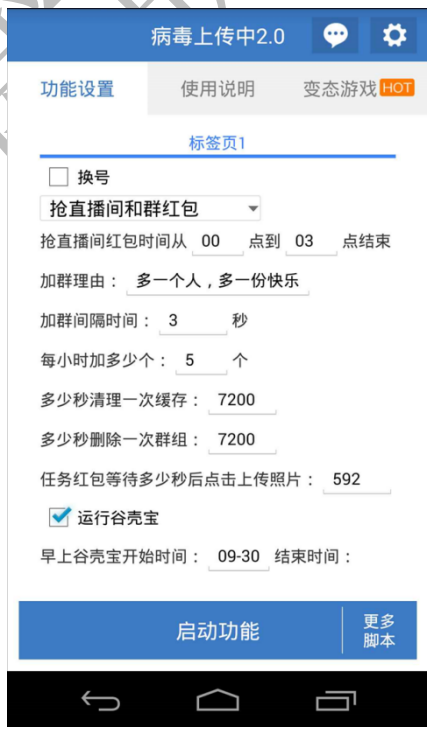


图 4-2-1 陌陌抢红包工具运行界面

黑灰产人员只需要在按键精灵安卓版上编写相关的逻辑脚本，即可实现模拟用户操作的动作去实现他们想要的功能，按键精灵安卓版运行界面如下图所示：

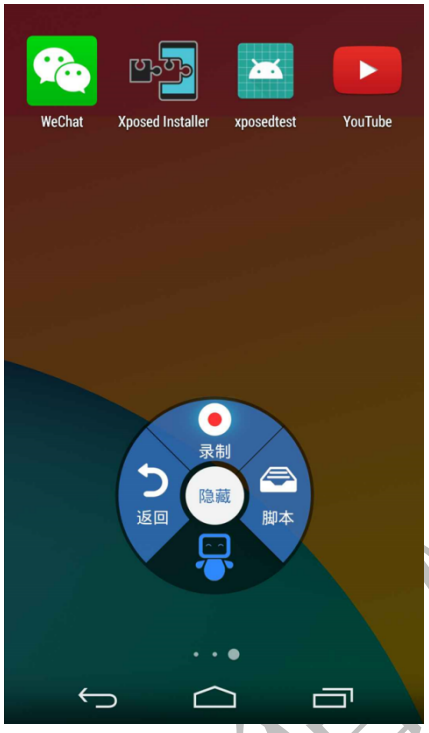


图 4-2-2 按键精灵安卓版运行界面

用户在点“录制”之后，就可以先手动操作一遍想要操作的功能，之后该软件会记录下用户操作的坐标轨迹，如下图所示：

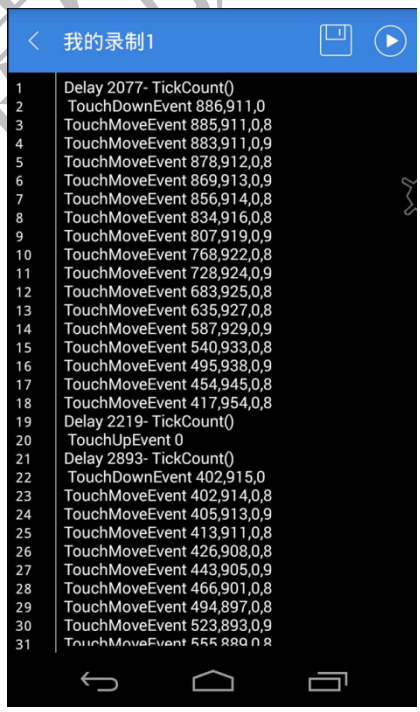


图 4-2-3 按键精灵安卓版运行界面

我们在分析的时候发现，该抢红包工具内置了工具需要的一些资源，包括识别出现红包时的图像，如下图所示：

图 4-2-4 陌陌抢红包工具内置的图片资源

软件在后台运行，通过查找整个手机屏幕上满足上述截图图像所在的坐标，然后再模拟用户去点击操作，从而达到抢红包的目的。

4.3.58 全职 VIP 发帖软件

这是 8 月份捕获的一款针对 58 同城的自动发帖类工具软件，该工具的原理是通过破解 58 发帖相关接口来实现。在调用相关接口的时候，软件会把接口所需要的参数拼接一起然后再向服务器请求。在该软件中实现调用的接口包括：登陆、发帖、获取展示中的帖子、未展示帖子、已删除帖子、审核帖子、获取未读简历等。我们以发帖这一功能来说明该软件的工作原理，其他接口调用类似。该工具软件运行的界面如下图所示：

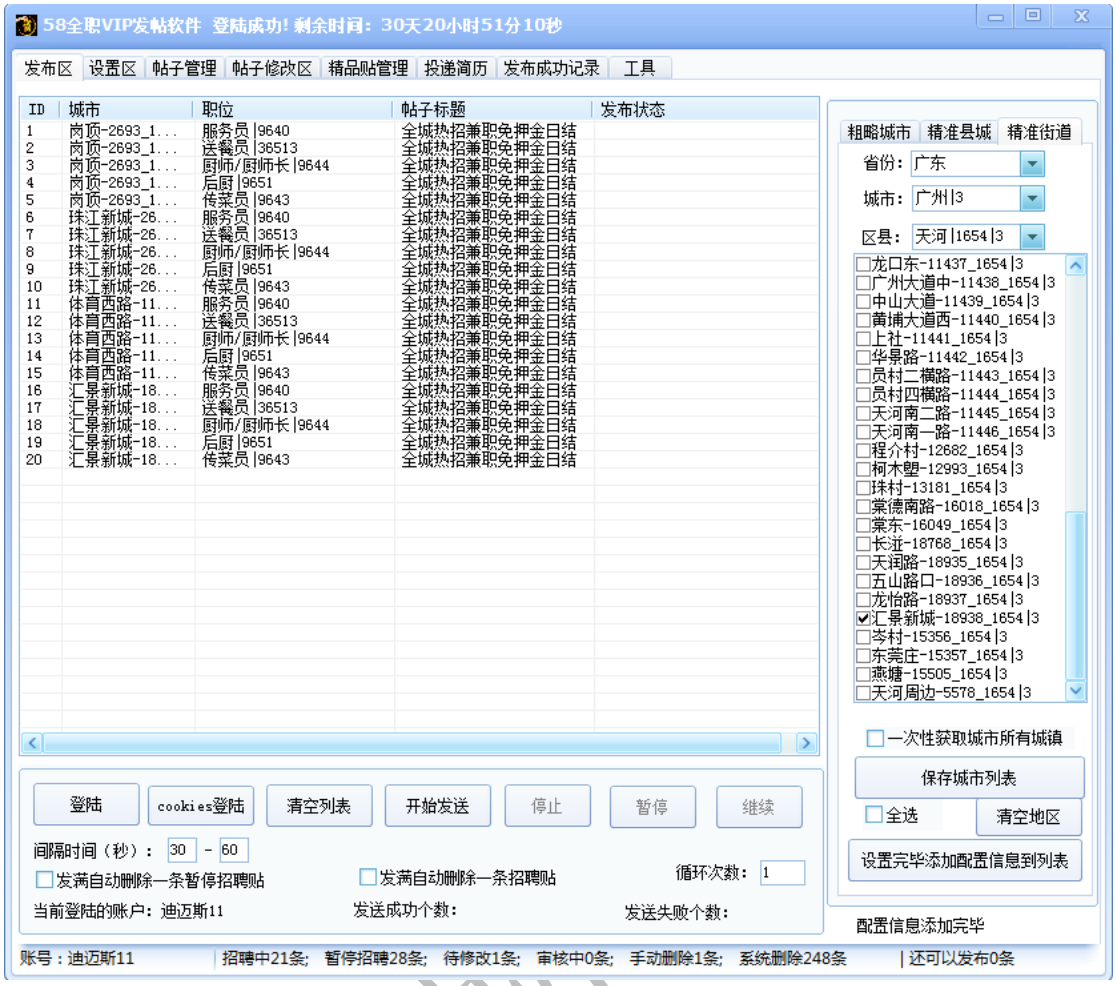


图 4-3-1 58 全职 VIP 发帖软件运行界面

界面上会有很多发帖的相关设置，这些设置是黑灰产人员在分析 58 发帖的接口之后提取出来的，用户需要操作的一些变量值（包含发帖的省份、城市、街道、帖子标题、帖子职位等接口所需要的一些参数）。如下所示为我们构造的 VIP 用户发招聘帖捕获到的接口信息：

```
POST /zhaopin/771/9640/s5/submit HTTP/1.1
Referer: http://zppost.vip.58.com/zhaopin/771/9640/s5/submit:1080
Accept-Language: zh-cn
Cache-Control: no-cache
Content-Type: application/x-www-form-urlencoded
origin: https://zppost.vip.58.com
Cookie:
PPU="UID=56216823046931&UN=%E8%BF%AA%E8%BF%88%E6%96%AF11&TT=8c9f19936449f8c0ed8
e15edafcc4018&PBODY=Vjytg7xzkXxnV5edPMI-NRUXoOF0F5VNpbpWkKygI_w8jUh8sAvJ3LwzbMj
dp32WYjbn968lobT0rtNXD3ybSSL0HUviwvXA5PSZtnb_nH4P6p6ENYc4fCs6EOcjyNpC3QcmFwIwq8
F2KWsMjQ8u3zu5mNmMN2RAf9adQO7QzbI&VER=1";
post_uuid=c1cc971d-cc29-4cf4-97e9-3ea1c94cdb88; id58=c5/nn1tw2Rw3ZTg4ChMDAg==;
58tj_uuid=192b5b03-07d0-48e2-924f-ea21ac06f638;
xxzl_deviceid=2CVEOtwqKJPOLFss2Ds1XQVIt%2F%2F6o8jEV43i7DROX3oDvwWeMdvWbzhG8KTG9
kBP; als=0; wmda_uuid=9523aee4d4a3f57acbd3b8c23b8e8743; wmda_new_uuid=1;
xxzl_smartid=1c324fb574ccf3e4223b69382c418682; showStatus=1695;
yxzwtip_common=1; bj58_id58s="WkFGRkgxczJsaWdWNDA3Mg==";
58home=gz; myfeet_tooltip=end; bangtoptipclose=1;
sessionid=51b6a460-a51e-4181-8e05-905a915948a2;
gr_user_id=6e35a225-20bd-437f-8250-9fd652a5c169;
wmda_visited_projects=%3B2286118353409%3B1731918550401%3B1731916484865;
58cooper="userid=56216823046931&username=%E8%BF%AA%E8%BF%88%E6%96%AF11&cooperke
y=ae19833887f30d969974fcb45f436409";
www58com="AutoLogin=false&UserID=56216823046931&UserName=%E8%BF%AA%E8%BF%88%E6%
96%AF11&CityID=0&Email=&AllMsgTotal=0&CommentReadTotal=0&CommentUnReadTotal=0&M
sgReadTotal=0&MsgUnReadTotal=0&RequireFriendReadTotal=0&RequireFriendUnReadTota
l=0&SystemReadTotal=0&SystemUnReadTotal=0&UserCredit=0&UserScore=0&PurviewID=&I
sAgency=false&Agencys=null&SiteKey=4E2D7FDC8FC545758AA9887A39348ECBAB802F961FAE
8AFC3&Phone=&WltUrl=&UserLoginVer=6132DEA395E09C43AA5CF48BC7145190A&LT=15341394
76115";
vip=vipusertype%3D11%26vipuserpline%3D0%26v%3D1%26vipkey%3Daac6d513cce8007f2079
6ac8bcbe8b9c%26masteruserid%3D56216823046931; new_uv=3; utm_source=; spm=;
init_refer=https%253A%252F%252Femployer.58.com%252Fcommonposition;
new_session=0; vpostedinfo=0;
bj58_init_refer="";
bj58_new_uv=6;
wmda_session_id_1731918550401=1534151687143-981d7eae-d074-c95e;
bj58_new_session=0;
ppStore_fingerprint=FE0CDBF5490ADCE4CDAE71C6365460AF6CA4479AA44FDC55%EF%BC%BF15
34152163928
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML,
like Gecko) Chrome/55.0.2883.87 Safari/537.36
Accept: */*
Host: zppost.vip.58.com
Content-Length: 2465
```

图 4-3-2 捕获到的接口信息

以下为接口需要 POST 的内容（由于该数据经过 UrlEncode 方式编码，为了方便阅读，展示的是编码前的明文数据）：

title=全城热招兼职免押金日结&jobcateID=13915&personnumber=10&eduid=1&experienceid=1&yingjiesheng=1&salary=5000_8000&content=

我们是谁？

广州佛跳墙餐饮管理咨询有限公司，主营各色餐饮业务，有大学食堂，5星酒店，海鲜超市，路边大排档，网红饭店等等只有你想不到，没有我们做不到的。现在业务扩展需要招聘如下人员
女：年龄18-32岁，身高160CM以上
男：年龄18-35岁，身高170CM以上
有无经验均可，公司提供入职培训！
有兴趣的请投建立或来电咨询报名！
可在线联系工作人员报名！期待你的加入！

&disablecheck=off&disabled=&welfareid=1|10|8|9|4|2|7&welfarestring=五险一金&s&2|包吃&s&2|包住&s&2|年底双薪&s&2|房补&s&2|饭补&s&2|加班补助&s&2&contact=Lilith&phone=13266887799&showphone=1&email=2034254642@qq.com&localcityid=3&localareaid=1654&localdiduanid=2693&addressid=10699378&isShowList=&isshowjz=false&captcha_input=&yzm=&jieshouyouxiang=2034254642@qq.com&phone2=&showphone2=1&cateid=9640&captcha_responseid=&captcha_encryptedKey=&post_captcha_biz=&teleprotection=&userid=56216823046931&jz_refresh_post_key=0&GTID=&daizhaogongsiid=&captcha_type_message=400

图 4-3-3 POST 的数据内容（编码前）

我们可以看出，上述大部分的内容为用户填写的信息，只要按照发帖的接口格式构造一样的形式数据就可以成功发出帖子，我们可以从这个接口所需要的相关参数看到，58VIP 发帖的接口需要的参数非常多，这就要求黑灰产人员具备较强能力的协议接口分析能力，能够分析出哪些是必须的参数，哪些是可有可无的参数，以及哪些是风控系统必须检测的参数，和参数的值是否加密。如果加密，则需要黑灰产人员破解加密算法之后，再计算出新的参数值以此绕过风控系统的检测。除了上述的发帖接口，其他接口调用的形式和上述大同小异。

五、结束语

黑灰产工具软件是网络黑灰产业发展的必然产物，黑灰产业会随着互联网的发展而发展，黑灰产工具软件也会随着黑灰产业的发展而发展。基于此，我们抛出以下观点，希望能引起行业共鸣，并与大家一起探讨和思考。

1、从黑产视角出发，建设黑灰产工具软件的全面监控和快速响应能力。通过对黑灰产业的长期跟进，我们对于黑灰产工具的传播链条和路径有了比较深入的理解和认知，可以第一时间捕获到网络中活跃的黑灰产工具，并第一时间分析其危害和原理。我们希望通过合作的方式，帮助更多的厂商建立这方面的能力。

2、建立黑灰产工具软件指纹库，增强风险设备识别能力。传统的设备指纹方案由于存在激烈的对抗，识别风险设备的效果并不理想；另一方面，风险设备往往会安装各种各样的黑灰产工具软件，通过提取这些黑灰产工具软件的特征作为指纹，可以有效的识别出风险设备。

3、建立行业的黑灰工具软件情报共享，最大化情报价值。根据我们的观察，工具软件的作者、传播渠道、以及使用者存在交集。以电商抢购为例，我们在跟进针对淘宝的抢购工具时，发现该工具的使用者，很多也会同时使用京东，苏宁，唯品会，华为等商城的抢购工具，从而达到利益的最大化。也就是我们第 2 点提到的黑灰产工具软件指纹库，其实是可以行业共享的，而我们也一直致力于解决黑灰产情报，包括工具软件情报的数据孤岛问题。

写在最后：

如果说黑灰产代表着黑夜，我们只有在黑夜中不断的探索和前行，才有可能迎来光明，与诸位共勉。

关注威胁猎人公众号，获取更多黑灰产研究报告