

黑产大数据

—— 威胁猎人汽车贷款欺诈风险研究报告 ——



目录

前言	3
一、汽车贷款欺诈风险概览	5
1.1 汽车贷款欺诈概览	5
1.2 汽车贷款欺诈热度区域分布	6
二、汽车贷款欺诈操作手法分析	8
2.1 目标客户招募	8
2.2 包装手法分析	9
2.3 车辆处置	11
三、威胁猎人金融贷款反欺诈服务	14
3.1 及时感知并预警最新信贷欺诈风险	14
3.2 结合群体画像提供业务风控应对策略	15
3.3 基于有效标签等数据定位恶意欺诈人群	15

前言

近年来，汽车金融市场持续扩大，汽车贷款欺诈也日益猖狂。威胁猎人调研发现，不法黑产打着“融车”、“0 首付购车”、“买车套现”的旗号，召集一些无法通过正常贷款融资但有资金需求的人群，如征信为白户、花户、黑户等，通过身份包装后进行“假购车、真套现”的合同诈骗、贷款诈骗。这些“融车”的人群中，不乏“职业背债人”的身影。



本文基于威胁猎人对汽车贷款欺诈产业链的深入研究，客观呈现车贷欺诈中客户招募手法、包装手法、车辆处置、不同区域欺诈热度，为银行等金融机构的贷款风控策略提供参考意见。

01

汽车贷款欺诈风险概览

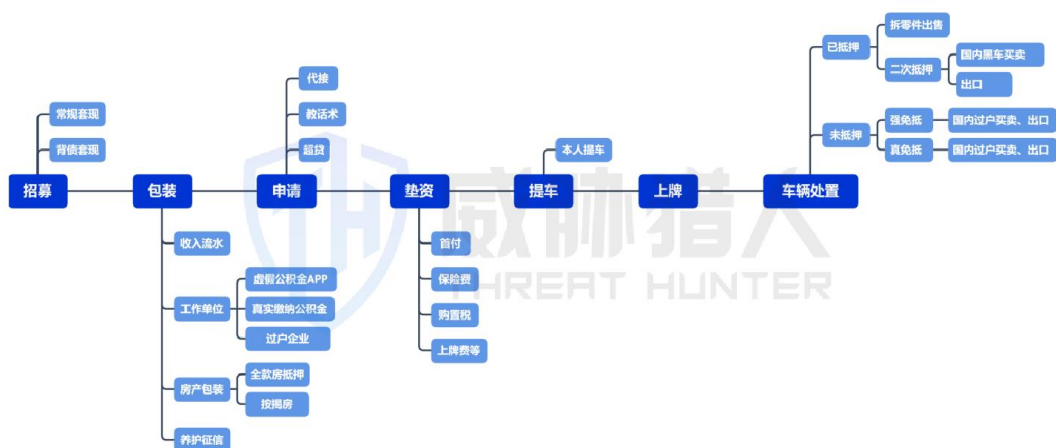
一、汽车贷款欺诈风险概览

1.1 汽车贷款欺诈概览

威胁猎人了解到，黑产通过招募一些无法通过正常贷款融资但有资金需求的“客户”，对其进行一系列包装和专业指导，帮助他们通过金融机构贷款买车，客户提车上牌后，通过第三方渠道把车辆抵押或出售进行套现换钱（这类车往往是准新车、“0公里二手车”）。“三天操作一台车，一人可做多笔车贷，甚至同一辆车可以申请多笔贷款”，最后这类汽车通过层层转卖至外地，在国内出售或洗白后出口。

完成贷款后，客户可以选择“要钱不要车”，也可以选择“要车也要钱”。融车套现后，客户到手金额为车辆总价值的40%至60%，甚至更少，剩余款项被黑产进行层层分赃。黑产为了延缓骗局被识破，一般会留下一部分钱帮客户还款或嘱咐客户正常还款3至6个月，逾期后再以其他不可抗因素或突发状况为由拒绝还款，以此麻痹金融机构以及逃避公安机关打击。

以下为融车风险在招募-包装-申请-垫资-提车-上牌-车辆处置等环节的操作流程：



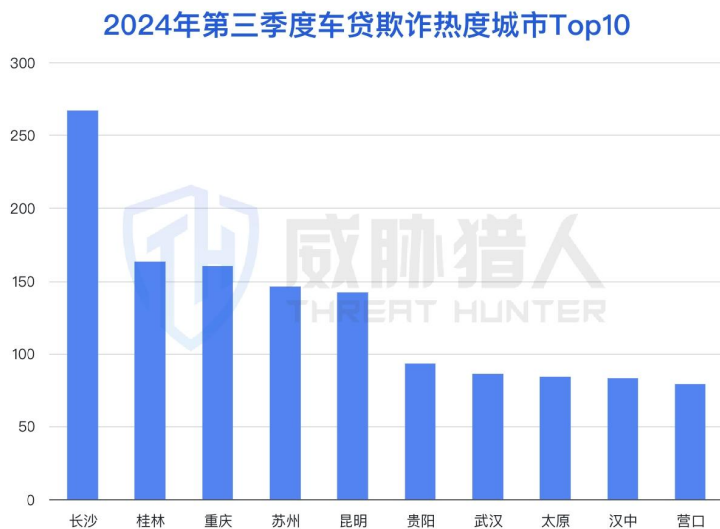
1.2 汽车贷款欺诈热度区域分布

威胁猎人对 2024 年第三季度汽车“融车”贷款欺诈情报分析发现，在省份分布中（含直辖市），广东、湖南、广西三个省份的汽车贷款欺诈热度较高，在城市分布中（含直辖市），长沙、桂林、重庆三个城市欺诈热度最高，且长沙的车贷欺诈热度远高于其他城市。

2024 年第三季度车贷欺诈热度最高的三个省份：广东、湖南、广西



2024 年第三季度车贷欺诈热度最高的三个城市：长沙、桂林、重庆



02

汽车贷款欺诈 操作手法分析

二、汽车贷款欺诈操作手法分析

2.1 目标客户招募

2.1.1 招募方向

黑产招募方向主要分为分为两种，一种是常规套现招募，目标客户为有资金需求但无法正常通过抵押、信贷方式贷款的客户，这种客户希望通过车贷套现后满足个人紧急资金需求，有主观偿还意愿、不以骗贷为目的的贷款，但还款能力不足；另一种是“职业背债”套现招募，通过“房/信/企/车”多类型组合贷款，如通过车贷套现，在同周期前后操作个人信贷、房贷、企业贷相关贷款，这种客户没有还款意愿、以骗贷为目的的贷款。

2.1.2 招募手法

黑产、黑中介一般通过社交软件及小视频平台在全国范围内搜集征信为“白户”、“小花户”或无法抵押信贷但有资金需求的客户，年龄在 25-50 岁左右，要求能说会写、能应对放款方贷款审批，能沟通并能执行黑产专项要求。

黑产将符合条件且有融车意愿或背债意愿的客户集中到车贷操作区域并短期居住，以便配合黑产各项操作。这类客户一般被安排住在宾馆、简陋居民房或简易酒店内，黑产实行包吃、包住、包路费“三包”政策。

如果是背债客户，在车贷办理后，就会根据黑产要求转移到其他城市继续操作房贷、信贷或企业贷款。此外，还有一些汽车销售人员也会发布一些销售广告，与贷款中介、黑产合作获客，默认甚至协助客户融车。

以下为黑产招募广告：

2证1卡； 3天1台；25-50W，只要优质客户，贷后多，查询少，半年不超6，无集中查询，大数据70以上，能说会写，面签标准！25-50岁；落地三包；1台1结；不扣杂费！（没有驾照也可以；）高点位结算，符合条件直接秒票	□抵押信贷都贷不出来的！ ♣轻松融车变现20-200W □有广东社保一年包批！ ♣有广东房半年+执照包批！ cn港澳台户籍好批50-100W 征信花黑呆账案件做不了	全国户籍汉族 25-48 纯白 小白 小花 半年查询不超6负债不超10 房企 信企 车企 3-6 个月额度300-700 一证一卡（有信用记录带n） 两证一卡 大量收	实力一条龙，车，企，房，信，25-45周岁，小花/白户/小白，全国可做 500-1500w，南京操作，无前期费用，费用三包，客户自行选择，三到六个月毕业，房企源头，超高佣金
--	---	--	---

目标客户确定后，客户甚至不用去车行看车选车，黑产直接给客户选好贷款车型，客户后续只需要配合即可，如客户可以异地操作预审，预审通过后再到车行城市操作后续贷款流程。黑产在给客户申请贷款前，会做好一系列的准备工作，如客户身份包装、流水包装等，确保车贷顺利下款。从申请贷款到落户提车一般 1 至 3 天就能完成一笔车贷。

2.2 包装手法分析

不管是常规车贷套现还是背债套现，黑产在操作贷款前，会根据客户的基本情况做不同情况的包装，包装手法主要体现在对客户身份的包装，如垫资买房包装成房产户主、通过企业过户包装成企业主、给客户缴纳社保公积金包装成工薪族等，另体现为给客户包装虚假收入流水，还体现为给客户养护征信等等。

2.2.1 身份包装手法

身份包装分为虚假包装和真实包装。虚假包装指通过虚假信息进行包装，如通过填写虚假的工作单位、虚假的社保公积金、个税 APP 等包装工作身份；真实包装指通过“真实”的动作进行包装，如通过真实购房、真实过户企业、真实缴纳社保公积金、定时转账到客户工资卡上作为工资等。

真实身份包装过程中，黑产需要大额垫资或通过给客户做一笔前期贷款（信贷/房贷）作为前期的包装成本，这种操作方式需要大额的资金成本，但也能贷款出更高的额度，巨大的利润驱动，构成了高成本高收益的“房信企车”大额综合背债业务。黑产通过给客户包装房产、企业作为增信条件，往往能够申请高价位的汽车贷款，甚至可以一车多贷、一人多贷。

2.2.2 收入流水包装手法

对于客户整体资质较好，比如征信条件、大数据资质基本符合金融机构车贷进件要求，但客户没有社保公积金、没有稳定收入的情况下，会影响车贷的通过率及审批额度时，贷款中介可以通过低成本对客户收入流水进行包装。

根据不同金融机构对车贷客户收入的核验方式不同，中介也有不同的包装方式，如社保公积金、个税、银行流水、微信流水、支付宝流水等均能体现出客户收入情况，中介会联合专门制作虚假流水的黑产，以几百元上千不等的成本，根据放款金融机构的核验要求，定向制作虚假纸质版、电子版、银行 APP 版等流水材料，用假流水绕过风控，成功申请车贷业务。

2.2.3 养护征信包装手法

黑产针对免抵押客户手里有《机动车登记证书》（以下简称大本）可以正常过户套现，且套现利润大。

目前一些黑产会召集目标客户到一些有免抵政策或对抵押政策松弛的区域办理车贷业务套现，如新疆、陕西、宁夏、甘肃、青海等地。如果客户资质不足以操作免抵车贷，黑产会根据客户情况，对客户进行包装或养护征信，养护周期为 3-6 个月，根据客户征信查询等情况进行人为调优，如把客户征信查询养护到近 6 个月内查询次数不超过 3 次，给客户包装工作单位等，客户资质达到车贷要求后，给客户操作车贷套现。

2.3 车辆处置

不同金融机构的车贷产品对后续车辆管控有不一样的处置方式，**主要分为两种情况：一种是免抵押，另一种是需要抵押。**

免抵押：是指客户通过贷款买车后，不需要将车辆抵押给放款金融机构，大本直接由客户自行保管；**抵押**是指客户通过贷款买车后，放款金融机构为把控贷后风险，需要客户把车辆抵押给放款金融机构，大本上交给放款金融机构保管，直至客户结清后金融机构归还大本给客户。

根据车辆是否真实抵押给放款金融机构，分为真免抵和假免抵：

真免抵：是指一些金融机构的免抵押车贷产品或一些金融机构对征信条件特别好、优质单位的客群实行免抵押的贷款方式。

假免抵：也叫强免抵，是指通过按揭贷款购买的车辆，按照贷款流程要求，汽车上牌后应把购买的汽车抵押给放款金融机构，但黑产联合客户在金融机构抵押期限之前把车辆卖给第三方并过户给第三方，汽车无法抵押给金融机构的行为。这种不是真正意义上的免抵押车贷。

根据金融机构对车辆后续管理方式的不同，融车后黑产对车的套现手法也有所区别，车辆转卖流向为国内销售或洗白出口或拆零件出售。套现手法主要为以下两个方面：

第一，已抵押给金融机构的车辆再次抵押给销赃汽贸公司或第三方套现或拆零件出售。这种车因无法过户，只能做黑车使用，套现成本高，客户到手金额为车辆价值的 20%-30%，甚至更少。另外，由于这种黑车出售价格低，利润少，有些黑产直接联合第三方把车辆拆卸，把相关零件出售给汽修公司或 4S 店。

第二，未抵押给金融机构（免抵车或还未到抵押期限的车）的车辆，只要客户手中有大本，就可直接出卖给销赃汽贸公司或第三方套现，这种车手续齐全，可以正常过户，客户到手金额为车辆价值的 60%-80% 成。这种套现方式利润高，已成为主流的套现方式。

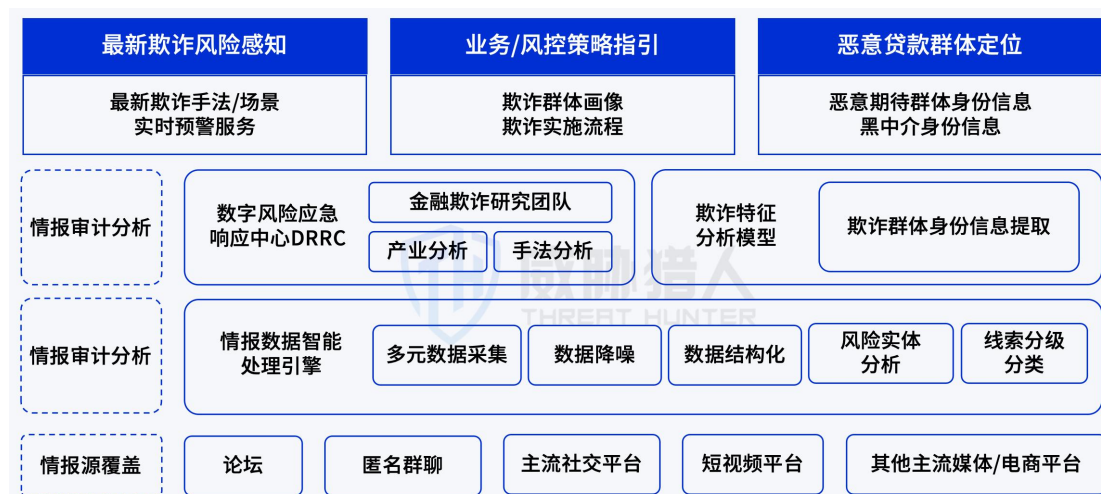
03

威胁猎人金融贷款 反欺诈服务

三、威胁猎人金融贷款反欺诈服务

“融车”行为不管是常规套现还是职业背债套现，黑产基本都会对客户进行包装、美化资质后再申请贷款，存在团伙攻击风险。这类客户非金融机构目标客群，且还款能力极低，甚至可能没有还款意愿，贷后逾期风险极高，会给放款金融机构造成不可估量的损失。

威胁猎人聚焦金融黑灰产攻防对抗领域，通过覆盖各类情报渠道源，主动获取大量信贷黑产/黑中介数据，基于欺诈特征分析模型自动化提取目标欺诈群体特征，同时结合数字风险应急响应中心（DRRC）专家的深入分析，为金融机构构建从最新欺诈风险感知、业务/风控策略指引、到恶意贷款群体定位的信贷反欺诈闭环。



3.1 及时感知并预警最新信贷欺诈风险

威胁猎人全面监测金融机构的信贷业务以及各业务环节，信贷欺诈情报专家针对全网信贷风险线索进行主动运营，及时感知黑产/中介的最新的欺诈风险，包含欺诈手法、欺诈场景等，如涉及房产信用/企业/车/现金/装修/消费贷/美容贷等贷款业务的欺诈风险监测。

3.2 结合群体画像提供业务风控应对策略

威胁猎人信贷欺诈情报团队深入不同的信贷欺诈场景,以攻击者的视角分析并复现欺诈全流程,包括为金融机构提供指定作弊环节的手法分析,如获客手法、包装手段、业务操作流程等,通过不同场景分析报告为金融机构建立欺诈人群的业务行为特征等,为风控策略提供可解释的依据。

信贷欺诈手法-美容贷	信贷欺诈-中介违规代扣收费调研	企业信贷欺诈手法-白户背债	信用欺诈手法-债务重组	中介线上获客手法调研
一、黑产手法 1. 获客手法 二、操作流程 2.1 筛选客户 2.2 合作医院 2.2 操作流程 二、黑产案例 一、黑产案例一 1.1 操作手法 1.2 贷款目标 二、黑产案例二 2.1 客户条件 2.2 操作手法 三、黑产案例三 3.1 客户条件 3.2 操作手法	一、中介收费方式 - 代扣主要的2种方式一是通过贷款资金 二、代扣手段 一) 合量数据 1. 操作流程 1) 录入信息流程 ①按百分比 ②按固定金额 2) 授权流程 3) 客户认证流程 4) 扣款流程 c、扣款页面输入扣款金额 5) 提现流程 2、风险性 二) 催收付 1. 操作流程 1) 录入信息流程 2) 授权流程 3) 扣款流程 4) 提现流程 2、风险性 三、代扣风险建议	一、黑产手法 1. 获客手法 2. 包装手法 2.1、过户 2.2、包装流水、税票 二、黑产案例 一、黑产案例1 1.1、符合背债人的条件 1.2、包装手法 二、黑产案例2 2.1、业务范围 三、黑产案例3 2.2、包装手法 1) 限制客户自由 2) 企业包装 3) 黑产代还 三、风险及建议 1、风险性 2、风险特征 2.1、异地性 2.2、场景相似性 2.3、形象差异性 3、风险建议	一、债务重组手法 1. 债务重组目标客户 2. 债务重组操作手法 2.1 获客手法 2.2 操作流程 2.2.1 精选客户 2.2.2 垫资还款 2.2.3 把控客户 2.2.4 养护征信 2.2.5 办理贷款 二、风险案例 1、风险案例一 2、风险案例二	一、中介线上获客手法 二、中介线上获客模式 1、百度广告商投放模式 1.1 广告投放方式 1.2 投放费用 1.3 搜索效果 2、小视频广告商投放模式 2.1 广告投放方式 2.2 投放费用及效果 3、中介自主发布短视频模式 4、中介广告获客模式 三、中介营销客户方式 1、中介触碰客户方式 2、中介营销客户方式 2.1 了解客户基本信息 2.2 保证下款 2.3 低息低手续费吸引客户

3.3 基于有效标签等数据定位恶意欺诈人群

基于对信贷欺诈产业链的持续监测及关联分析,威胁猎人可获取大量有效欺诈团伙的群体特征信息(如身份信息、银行卡信息等),可帮助金融机构在大数据模型等安全检测措施的基础上,基于恶意特征标签进行关联分析,精准定位欺诈人群。

04

相关名词解释 及“黑话”释义

四、相关名词解释及“黑话”释义

白户：通常指那些信用记录较少或没有信用记录的人。这种情况下的个体，由于没有过去的借贷历史，使得银行或贷款机构难以准确评估其信用风险。在黑灰产产业链中属于物料类，常在 TG、推特、potato 上售卖。欺诈者可能会利用这种“白户”的身份来进行信贷欺诈，比如通过虚构信用资料或伪造文件申请贷款。这种策略使得他们能够在银行和金融机构缺乏对其信用历史的了解的情况下，获得信贷，这些参与背债的人也被称为“白户背债人”或“职业背债人”。

花户：指频繁申请信用卡或贷款的人。这种行为可能会被金融机构视为风险较高的特征，因为频繁申请信用卡或贷款可能表明该个人的资金需求较为紧迫，或者其信用管理存在问题。

“花户”通常会在个人信用报告中显示大量的信贷查询记录，这可能会对其未来的信用申请产生负面影响。“花户”也可能被黑产用于信贷欺诈，如“债务重组”中，黑产通过前期垫资帮助用户还清债务，再让其背负更高额度的贷款。

小花/小花户：是花户的一种，是相对于大花户而言，大花户是指征信查询次数多、贷款数多、征信花的客户，小花户则是指征信查询次数、贷款数相对较少、征信相对普通的客户。

黑户：通常指那些有不良信用记录，被银行拉黑信用的人。这些人可能因为拖欠贷款、违约或其他不良信用行为而被金融机构列入黑名单，意味着他们很难再通过正规渠道获得贷款或信用卡。黑户的账户有时会被黑灰产业者用来进行洗钱，即通过这些账户转移非法所得，以掩饰资金的非法来源。黑灰可能会利用黑户的个人信息尝试在不同的金融机构中进行撞库攻击，查看这些信息是否能够用于成功申请贷款或信用产品。

融车：常指以虚假信息或欺骗手段来获取汽车贷款或租赁的行为。黑产通过“包装”个人信息、财务状况、就业状况，以非真实购车需求绕过风控并获得汽车贷款，再把车辆处置套现，即“融车套现”。另指一种伪装交易的手段，即通过虚构的汽车销售交易来欺骗贷款机构。例如，以虚构的汽车买卖合同为依据，申请贷款或租赁，实际上并没有真实的汽车交易发生。

大本：在车贷欺诈中，指机动车登记证书，也称“绿本”。

真免抵：是指一些金融机构的免抵押车贷产品或一些金融机构对征信条件特别好、优质单位的客群实行免抵押的贷款方式。

假免抵：也叫强免抵，是指通过按揭贷款购买的车辆，按照贷款流程要求，汽车上牌后应把购买的汽车抵押给放款金融机构，但黑产联合客户在金融机构抵押期限之前把车辆卖给第三方并过户给第三方，汽车无法抵押给金融机构的行为。这种不是真正意义上的免抵押车贷。

点位：指黑产团伙抽取的费用，通过风险级别判断点数大小，放料方资金风险越高，黑产的点位就越高。



关注“威胁猎人”

深圳永安在线科技有限公司（品牌名：威胁猎人）

☎ 官方服务热线：400-809-3699

✉ 官方合作邮箱：marketing@threathunter.cn

🌐 官网地址：www.threathunter.cn