网络借贷诈骗新途径及解决对策研究

摘　要

中国经济产业的转型升级让中国金融产品及消费借贷应用得到了普及，并由此衍生出了无需物质抵押，依托个人消费记录的电商消费类借贷产品，以及无需物质抵押，依托个人征信的小额借贷产品。

但是随着金融市场借贷习惯的养成，在用户体量不断增多的同时，大量的网贷欺诈事件也时有发生，包括高额砍头息的“714 高炮”、冒充知名借贷平台的虚假平台等一系列新骗局新手段，也给网络借贷诈骗的打击防范带来了全新的挑战。

关键词:网络借贷诈骗;诈骗诱因;打防对策

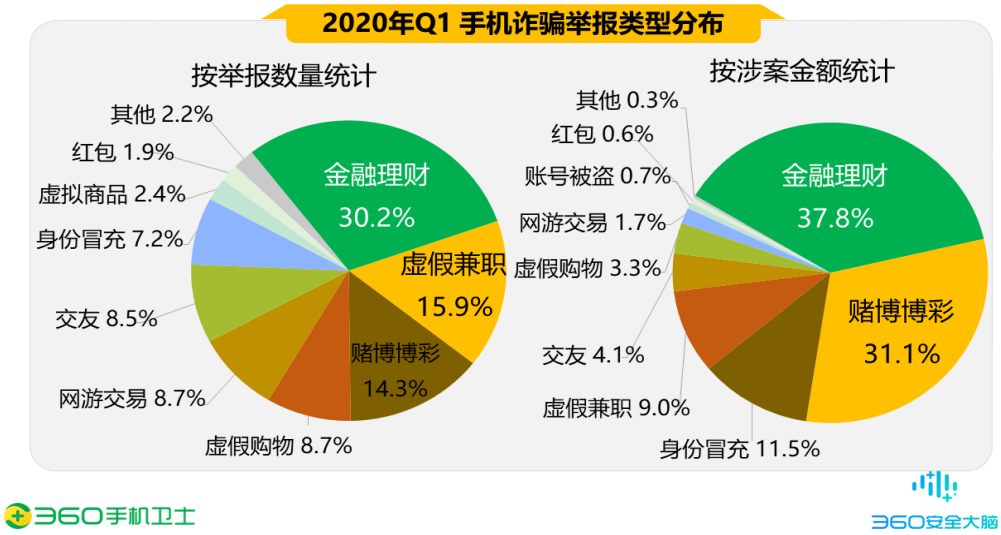
目　录

第一章 网络借贷诈骗现状分析

一、网络借贷诈骗现状

2020 年第一季度，360 手机先赔共接到手机诈骗举报 856 起。其中诈骗申请为 414 起，涉案总金额高达 340.2 万元，人均损失 8218 元。在所有诈骗申请中，金融理财占比最高，为 30.2%；其次是虚假兼职（15.9%）、赌博博彩（14.3%）、虚假购物（8.7%）、网游交易（8.7%）等。从涉案总金额来看，金融理财类诈骗总金额最高，达 128.5 万元，占比 37.8%。

下图为 2020 年第一季度手机诈骗举报类型与涉案金额分布情况：



从金融理财诈骗类的细分项目来看，其中网络借贷诈骗占比 86.4%，影响程度可见一斑。

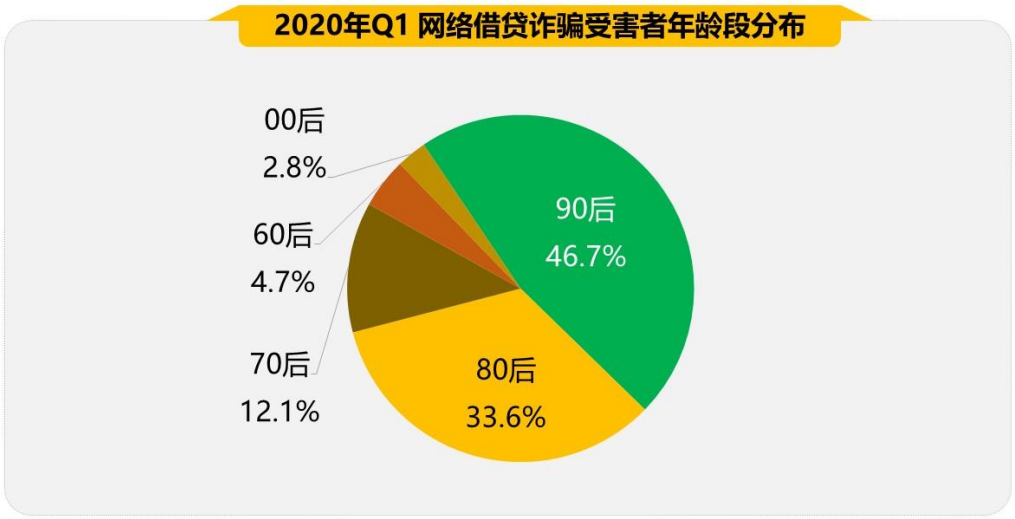
随着近几年网络借贷平台数量在国内的迅速增长，其门槛低、渠道成本低、交易便捷等优势已受到用户的大量青睐并逐渐发展为当下的一种潮流趋势。但网络借贷的普及也让不少不法分子有机可乘，其中最典型的借贷诈骗手法就是以贷款包装费、征信不足、银行交易流水不足为由，引导用户进行转账。在 2019 年发现的借贷诈骗案件中，不法分子就大多使用了虚假“借贷 APP”来吸引用户申请贷款，并要求用户向指定账号转账缴纳贷款流水费。

二、虚假网络借贷受害者性别与年龄

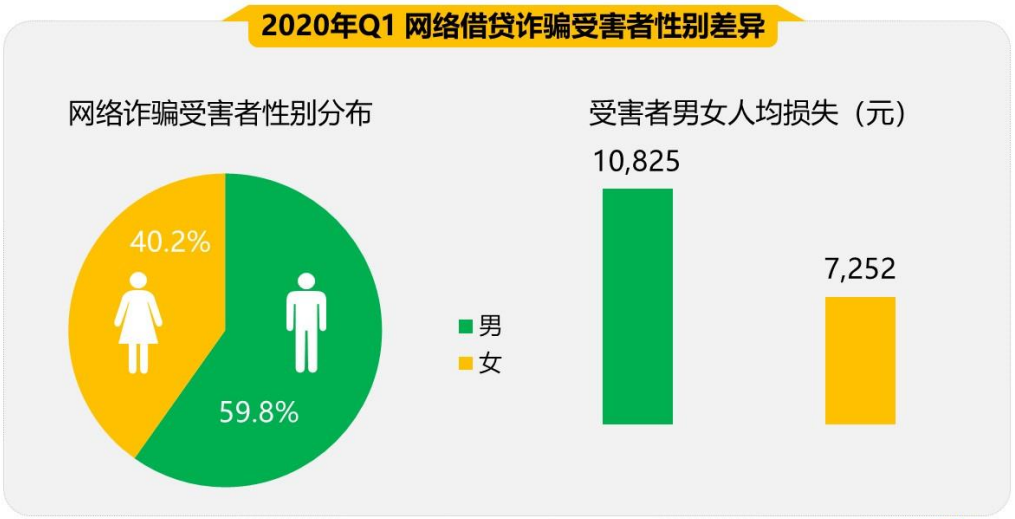
1） 90 后占比男性占比最高，为手机诈骗的重要目标

从 2020 年第一季度网络借贷被骗网民的年龄段上看，90 后手机诈骗受害者占所有受害者总数的 46.7%；

其次是 80 后，占比 33.6%，70 后占比 12.1%，60 后占比 4.7%，00 后占比 2.8%。其中尤其值得注意的是，90 后遭遇网络借贷诈骗增多明显，未来随着 90 后年龄的增加，对资金的需求也会不断增大，90 后正成为网络借贷诈骗的重要目标。

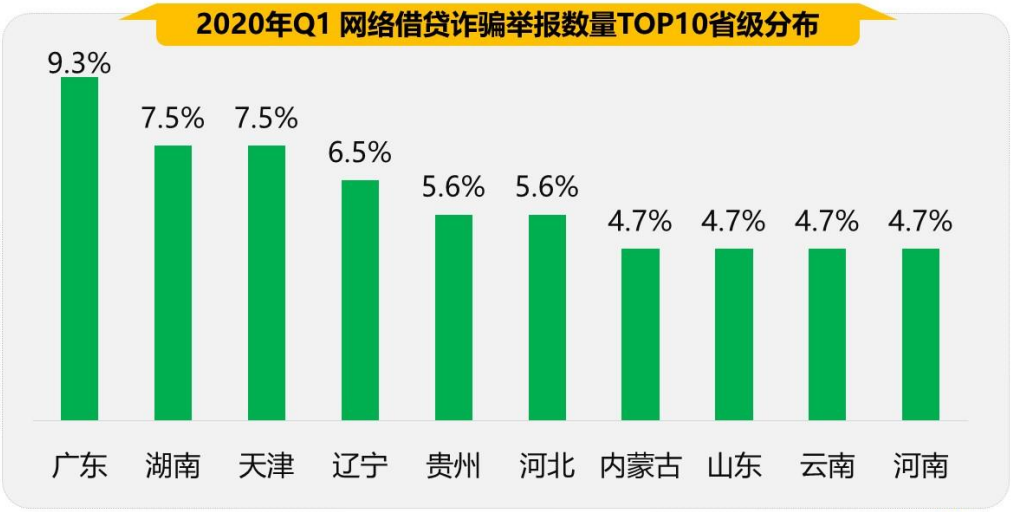


从网络借贷诈骗举报用户的性别差异来看，男性受害者占 59.8%，女性占 40.2%，男性受害者占比高于女性。从人均损失来看，男性为 10825 元，女性为 7252 元。可见男性在面对借贷诈骗时，更愿意相信对方所描述的“陷阱”，向对方转账。

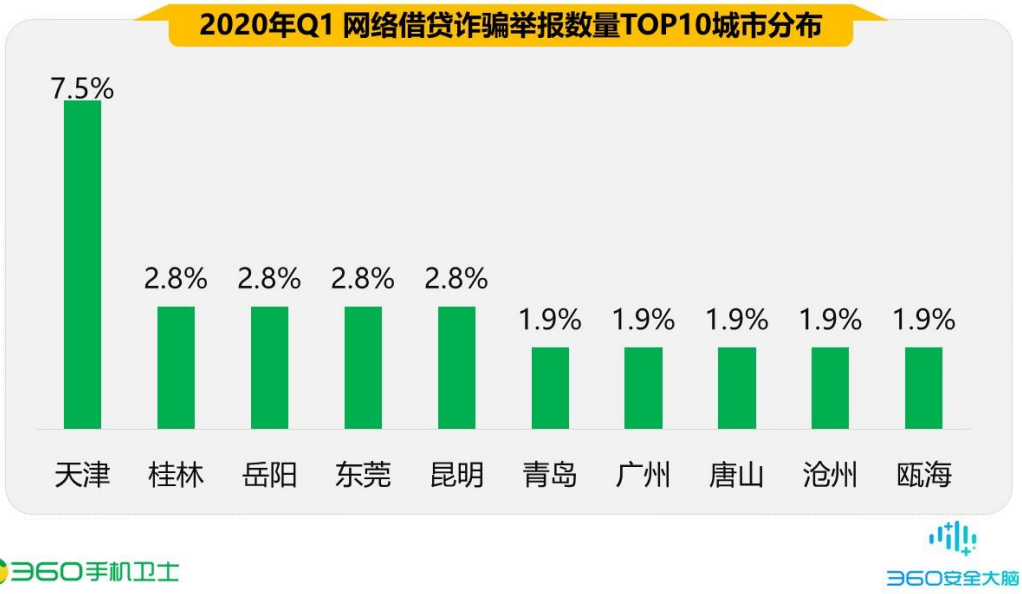


2） 省级分布中广东省占比最高，市级分布中天津被骗用户最多

从 2020 年第一季度网络借贷诈骗中用户举报数量的省份分布情况来看，广东（9.3%）、湖南（7.5%）、天津（7.5%）、辽宁（6.5%）、贵州（5.6%）、河北（5.6%）这 6 个省级行政区的被骗用户最多。举报数量约占全国用户举报总量的 42%。下图给出了 2020 年第一季度网络借贷举报数量省份 TOP10：



细分到各城市的网络借贷诈骗举报情况来看，天津是举报人数最多的城市，占比 7.5%，其次为桂林 2.8%，岳阳 2.8%，东莞 2.8%，昆明 2.8%。下图给出了 2020 年第一季度网络借贷举报数量城市 TOP10：

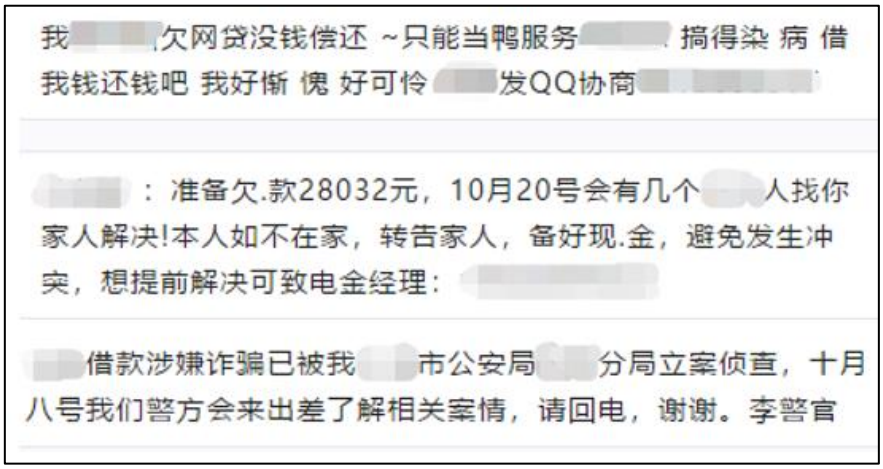


第二章 网络借贷诈骗新途径解析

一、借贷者永远偿还不完贷款的 “714 高炮”

中国互联网的快速发展推动了互联网技术的普及，开发并推广一款互联网产品已变得十分容易。借助互联网技术，传统的线下“高利贷”放贷者纷纷转型入场“线上”开发现金贷平台，并借助“贷款超市”的力量迅速推广。此类现金贷平台的产品具有放贷周期短、放贷金额低、申贷利息高的特点，即借贷 1000 元到账 800 元，须在 7 天或 14 天左右归还 1000 元，逾期会产生更高的利息费。表面看起来本息金额不是很大，但利息已远远高于国家规定的最高贷款利率 36%。同时，放贷平台还会通过一些手段诱导用户续贷，在多次续贷后利滚利产生的利息往往远高于借贷本金，但此时多数用户已无力偿还本息。紧接着平台方会给申贷者推荐其他现金贷平台，通过拆东墙补西墙的方式还款。最终申贷者将完全落入平台的“圈套”，即借的平台越多，欠的利息越多，贷款永远偿还不完。

虽然随着执法部门重点打击清理市面违规的现金贷平台，众多“714 高炮”平已台纷纷离场，但在离场之际大多会将借贷合同打包贩卖给职业贷款催收公司，彻底“压榨”申贷人。由于借贷者“早已身无分文”，催收平台为迫使还款，使用群呼电话、短信等手段轮番轰炸。如下图展示催收短信极尽侮辱之词，甚至冒充公检法给用户发送催收短信。



二、借贷者永远借不到贷款的网络借贷诈骗

金融市场的火热让各大知名互联网公司及传统知名的线下实体企业也都纷纷加入小额借贷市场，推出各类小额贷款产品。这些产品由于有知名企业做背书，一经推出便具有较强的知名度，用户通过平台图标和平台名称便可联想到对应的企业平台。同时随着互联网运营行业的发展，众多的新型的营销方式也能更有效的帮助产品快速推广。但用户在面对海量网络借贷产品时，由于众多的客观条件，无法鉴别平台真伪，

容易被虚假平台骗取资金，以下通过几个典型的诈骗案例进行展示。

案例一 使用虚假借贷应用，冒充知名借贷公司

冒充知名借贷平台给用户发送赠送放贷资格的短信，引导用户安装指定的借贷 APP。待用户在平台上传完个人信息后，给用户推送资质审核成功短信，引导用户在平台提现。当用户在平台提现时，如下图显示用户银行账户错误，账户被冻结，要求用户缴费解冻，即使用户按照要求向对方转账，对方还有用户征信不足等一系列话术要求继续转账，到最后也不会给予用户放款。

案例二 使用虚假借贷合同，冒充知名借贷公司

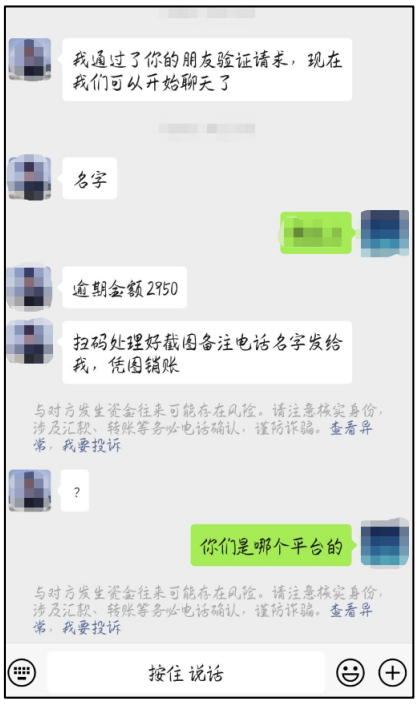
电话联系用户并取得用户信任后，先以资质审核为由，索要用户身份证正反面照片、银行账号等个人信息。再引导用户签订借贷合同（电子版），随后以用户征信和银行流水不足为由，要求用户向指定银行账户转账刷流水，如果用户不按照要求操作，则表示用户违约，会向当地法院起诉，如果用户听从要求转了10%的流水，后续也还会要求继续转账 20%的流水，但所贷资金却始终见不到。

案例三 以注销贷款为名，引导用户在多个借贷平台申贷，骗取所贷资金

冒充知名借贷平台，电话联系用户谎称“其在大学期间有借贷记录，由于国家政策严禁在校大学生在借款平台上有任何账号，否则会影响个人征信，因此要求受害者把之前的借贷平台账户注销。注销的流程为在各大借贷平台借贷，并将借贷资金转给对方。”一旦用户听信进行转账后，对方就会失联。

案例四 冒充借贷催收平台，骗取借贷还款

互联网黑灰产通过个人信息贩卖渠道获得借贷人员信息，随后冒充借贷平台，以用户贷款逾期为由，要求用户还款。若遭到用户拒绝，则通过“轰炸通讯录”方式联系亲友进行催收。此类欺诈由于不法分子事前已掌握用户基础信息，用户对于自己是否逾期的问题，存在疑虑。在不法分子施加恐吓后，则听信对方，并向对方转账[①]。



[①] 360 手机卫士,360 互联网安全中心. 2019 年第三季度中国手机安全状况报告[R]. 360 研究报告官网,2019

第三章 探究网络借贷诈骗泛滥背后的原因

通过对网络借贷诈骗案例进行梳理，我们常会产生一些疑问：受害人为什么那么轻易就相信骗子的话？受害人为什么难以识别骗子营销的虚假借贷产品？受害人为什么反复向骗子转账而无法抽身？为什么借贷诈骗在重拳打击下仍死灰复燃？

一、个人信息泄露严重

不管政府、企业如何宣传科普安全意识，国内信息泄露问题一直随着中国互联网的发展而存在。究其原因主要是因为以下两个方面，首先网民对于个人信息保护不到位，随意在互联网上传个人信息；另一方面是虎视眈眈盯着用户个人信息的黑灰产团伙，通过社会工程学、“服务器脱库”、“返照认证接口”等方式获取个人信息。通过这些方式网络黑灰产人员掌握了大量有借贷需求人群的个人信息。

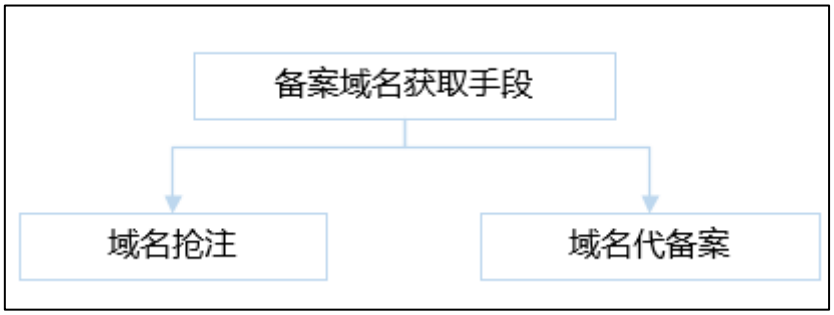
二、虚假借贷支撑平台泛滥

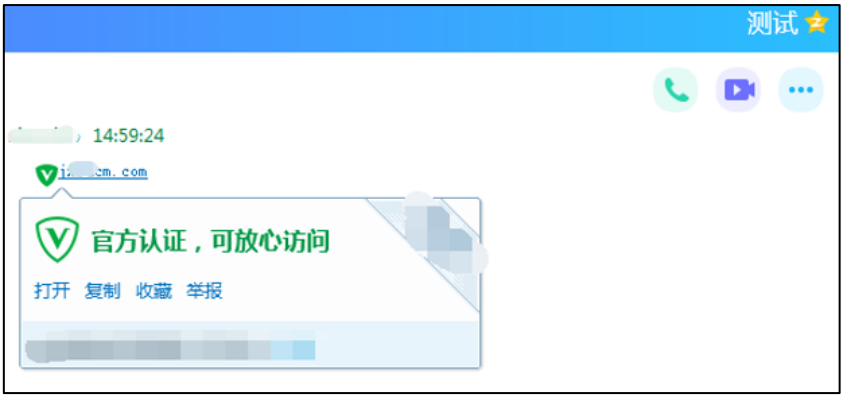
中国移动互联网的快速发展，在造就大量的互联网“人才”的同时，也衍生了众多的互联网黑灰产业务。含备案信息的域名批发商城、免备案的境外服务器、“免费”使用的计算机程序、“快速”搭建平台客服的第三方客服应用、一键生成及推广 APP 的封装封发平台、躲避金融风控及“洗钱”的第四方支付平台（含资金池）等。这些资源在互联网各个渠道疯狂“野蛮”生长。依托这些互联网现有成熟资源，批量开发虚假借贷平台已不是技术难题。

1) 含备案信息的域名批发商城

在黑灰产攻防的早期，一些传统企业仅依托域名备案信息确认平台真伪。黑灰产从业人员使用含备案信息的域名传播钓鱼网站时即可躲过安全检测。

含备案信息的域名批发商城，可以简单理解为一个域名“贩子”，专门售卖一些含备案信息的域名，并延展出特定攻防的域名，如“绿标”域名（域名通过社交软件发送时，提示绿色的官方认证，可放心访问标识）。如下图展示，这些域名商城通过域名抢注（域名过期后，原备案信息还存在）、使用个人/企业信息进行域名代备案等方式掌握到获取大量备案域名，并将此类域名根据域名性质（企业、个人）、域名接入商、社交软件/网络安全厂商是否拦截进行分类并售卖。





域名	价格	接入商	备案号	性质	介绍	到期时间
z c.top	120元	景安	豫icp备1 542号-8	企业	景安备案,微信无拦截!	2020-11-20
nor net.com	170元	其他	吉icp备15 314号-1	企业	其他备案,微信无拦截!	2020-12-10
gor wang.net	200元	西部	皖icp备17 42号-1	个人	西部备案,微信无拦截!	2021-01-15
lar ji.net	200元	西部	苏icp备17 42号-6	个人	西部备案,微信无拦截!	2021-01-23
kn ts.com	150元	其他	滇icp备16 3号-1	个人	其他备案,微信无拦截!	2020-07-11

2) 免备案的境外服务器

免备案服务器，顾名思义就是指使用时无需提交个人信息或企业信息进行认证的服务器。一般来说国内正规的云服务商提供服务时按照国家规定需要使用者进行严格的身份认证，但是由于该政策只针对中国大陆的云服务产品，于是各类中小型云服务商借助中国香港或境外的服务器钻政策空子，提供免备案服务器。

3) “免费”使用的计算机程序

20 年前，中国计算机资源缺乏，开发难度大成本高，为降低开发成本难度，出现了一些帮助企业快速建网站的程序 CMS。近些年中国互联网的快速发展让互联网共享精神得到推广，各类开源程序在互联网涌现。于是在互联网随处可见各类借贷 CMS、借贷源码。

4) “快速”搭建平台客服的第三方客服应用

第三方客服系统类似于 CMS，本身是帮助企业解决平台客服接入管理问题。通过平台接口的方式接入企业平台，降低企业研发和运营成本。但由于国内安全监管的升级，黑灰产人员使用的 QQ、微信等社交账号存在易被查封关停的风险，为解决查封问题黑灰产人员盯上了第三方客服系统，利用“虚假”的企业认证信息，将第三方客服系统接入到黑灰产平台，提供客服服务。

5) 一键生成及推广 APP 的封装封发平台

互联网进入中国已经很多年，伴随着互联网发展的除了数不胜数的网站外还有众多建设网站的教程。相较于手机 APP 产业，网站开发产业成熟度和规模都大的多，将 WEB 直接转成 APP 成为了开发 APP、降低开发难度及成本的首选。于此同时，对于黑灰产人员而言，WEB 转 APP 还可以批量生成多个虚假平台。如下图展示，在封装平台提交网站信息、需生成的 APP 图标、APP 名称后，即可将 WEB 页面封装成 APP。

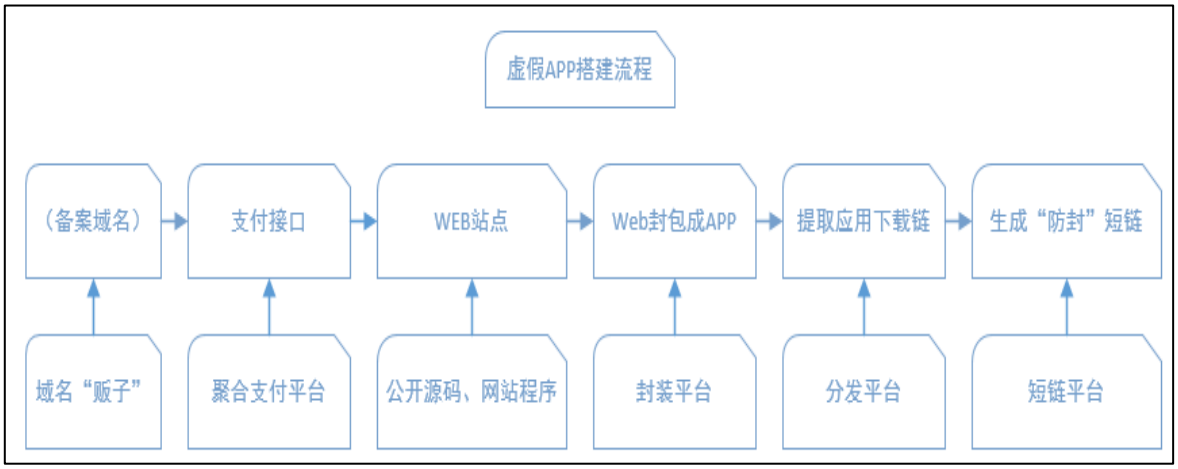
APP 分发平台是一种应用托管服务，开发者可以将应用上传至分发平台，由平台提供应用下载链方便应用开发者将应用进行传播。此种平台原意是为了解决 app 短暂无法上架 app 应用商店的问题，但由于其无需像传统的手机应用商店需要严格的应用风险审核和身份验证，因此近年来多被黑灰产利用。如下图展示的应用分发平台，在平台注册（无需实名）后，上传应用安装包后，即可生成应用下载链。

6) 躲避金融风控及“洗钱”的第四方支付平台（含资金池）

“第四方支付平台”指的是未获得国家支付结算许可、通过大量注册商户或个人账户非法搭建的支付通道，非法对外提供支付结算服务。虚假 APP 由于无法使用正规的支付接口，多采用第四方支付平台提供的接口。如下图展示第四方支付网站，提供的支付接口服务包括支付宝扫码、支付宝 H5、云闪付扫码、微信扫码等。

可见借助以上成熟的互联网资源开发推广并运营一个平台，已变得十分容易。通过对虚假借贷 APP 逆向分析，我们梳理出虚假网络借贷 APP 制作流程。

APP 搭建人员首先从域名“贩子”手中购买大量（备案）域名或境外域名，然后使用公开的源码或网站框架，接入第四方支付接口搭建网站。最后通过一些 web 封装平台将网站封装成 APP 并将 APP 上传至应用分发平台获得应用下载链，在短链平台将应用下载链转换成短链接。如下图展示虚假 APP 制作过程。



三、虚假借贷平台推广方式多样

虚假 APP 完成后，为了吸引更多的人群使用，需要将 APP 进行推广。依托于近些年中国互联网运营玩法，通过短信群发、电话群拨、黑帽 SEO、短视频引流等方式帮助产品快速推广。

1) 短信群发

短信作为功能机时代的必须品，进入智能机时代后也变得更加重要。平台注册、交易信息校验，用户无时无刻都在与短信打交道。近年来，随着短信技术的发展，各类短信营销方式迸发，出现了卡池短信平台、运营商短信通道平台。

卡池短信平台，可以理解成一个能够安装大量手机 SIM 卡的盒子，接入电脑后，可以使用此些号码群发短信。运营商短信通道则是通过运营商提供的短信发送接口，实现与客户指定号码进行短信批量发送和自定义发送。黑灰产人员在获取大量短信发送渠道后，会在发送短信时进行一定包装，一方面在内容上模仿正规借贷平台发送的营销短信，一方面在内容上以“立马可以借到贷款”字样引起用户注意，给接收短信方营造出一种这是真实平台发送的短信及可以快速借到贷款的假象。

2) 黑帽 SEO

随着国内应用商城的愈加成熟，大部分用户会使用应用商店搜索应用。但对于以贷养贷的人员而言，其本身征信已经下降，常规借贷平台无法借到贷款，于是就需要通过搜索引擎搜索黑户包过贷款信息。而黑帽 SEO 则是根据这一现象，利用搜索引擎禁止使用的作弊收录手段，快速提升虚假借贷 APP 在搜索引擎的收录排名；同时借助广告联盟的力量，通过高佣金实现广告投放推广。

四、虚假借贷话术剧本多样

虚假借贷平台频频得手的原因在于其深入研究了借贷人员的几个心理：急于借贷、急于提现、害怕影响个人征信。在设计诈骗场景时，根据这些特征分别设置了不同的环境。申贷过程与正常借贷流程一样，填写个人身份信息，填写收款银行账户，收到审核进度短信，通知用户申贷成功。当用户得到贷款后选择提现时，则告知用户其填写的收款银行账户错误，导致放款失败，此时用户会怀疑自己是否真的填错了，然后主动联系平台方确认，平台就顺势引导出缴费服务。若用户不愿意缴费，则抛出影响用户征信的话术，迫使用户最终缴纳费用；若用户缴费，则告知用户流水不足，未满足放款条件，要求用户再次转账。

通过对虚假借贷产业链内部分工分析，就可以解释本章最初提及的几个问题。用户信息泄露后，骗子知道了用户详细的个人信息和借贷需求，通过冒充知名借贷平台或自称可以给“黑户”放贷吸引用户关注，使用高仿的借贷 APP 或网站取得用户的信任；在放贷过程中设置陷阱持续引导用户转账；由于事前做了一定的隐蔽手段，加上平台开发成本低，可以快速重建，所以即使平台被打击也能迅速死灰复燃。

第四章 黑灰产进阶之路-攻防策略

伴随着互联网行业从 PC 互联网时代发展到移动互联网时代，黑灰产业也从 PC 互联网时代的“单兵”作战向移动互联网时代的“集团化”作战转变。随着黑灰产行业的“集团”化和人员分工的“链接”化，其网络安全技术及攻防策略不断演进升级。一方面不断提升欺诈环境的仿真度，防止被用户识别。一方面借助攻防策略的升级来躲避网络安全、社交软件等产品对欺诈样本的识别。鉴于此，攻防对抗将是互联网行业与黑灰产“企业”不断厮杀成长的一场持久战。以下通过传播渠道、诈骗应用、实施诈骗三个环节对网络借贷诈骗攻防策略及演变进行解读。

一、传统渠道之短信内容的攻守之道

随着互联网的发展，从日常沟通到身份验证都离不开短信的身影，手机短信已成为生活中必不可缺的工具。正因如此，黑灰产也时刻紧盯着短信这块传播渠道的“蛋糕”。2020 年 1 月份，诈骗短信平均每日被 360 拦截量约为 270 万条（数据来源：360 发布的 2020 年第一季度 中国手机安全状况报告）。若按照每人 1 条短信计算，相当于每日有 270 万人遭受诈骗短信的“洗礼”，可见诈骗短信的影响程度之深。黑灰产在大量传播欺诈短信的同时，还不断升级短信攻防策略，以应对安全厂商对欺诈短信的识别拦截。

方式 1：短信内容伪造、内容“混淆”

由于传统的网络借贷平台在推广过程中会使用短信进行推广，因此黑灰产常采用冒充知名网络借贷平台的方式传播模仿知名借贷平台短信内容的虚假短信。但随着大数据算法的发展，仅仅通过短信内容模仿已无法突破网络安全厂商的短信识别。

于是网络黑灰产开始升级自身短信内容，采用“混淆”短信内容的方式，将短信文字进行简繁体转换并对内容进行语义混淆，如短信内容“【温馨提醒】您友柴晶卫苓娶 请加 Q:(1399*****1) w.ur***.cn/***”，这句话潜在含义就是“您有资金未领取”。随着大数据算法的再次升级，此种方式又无法突破算法的识别。

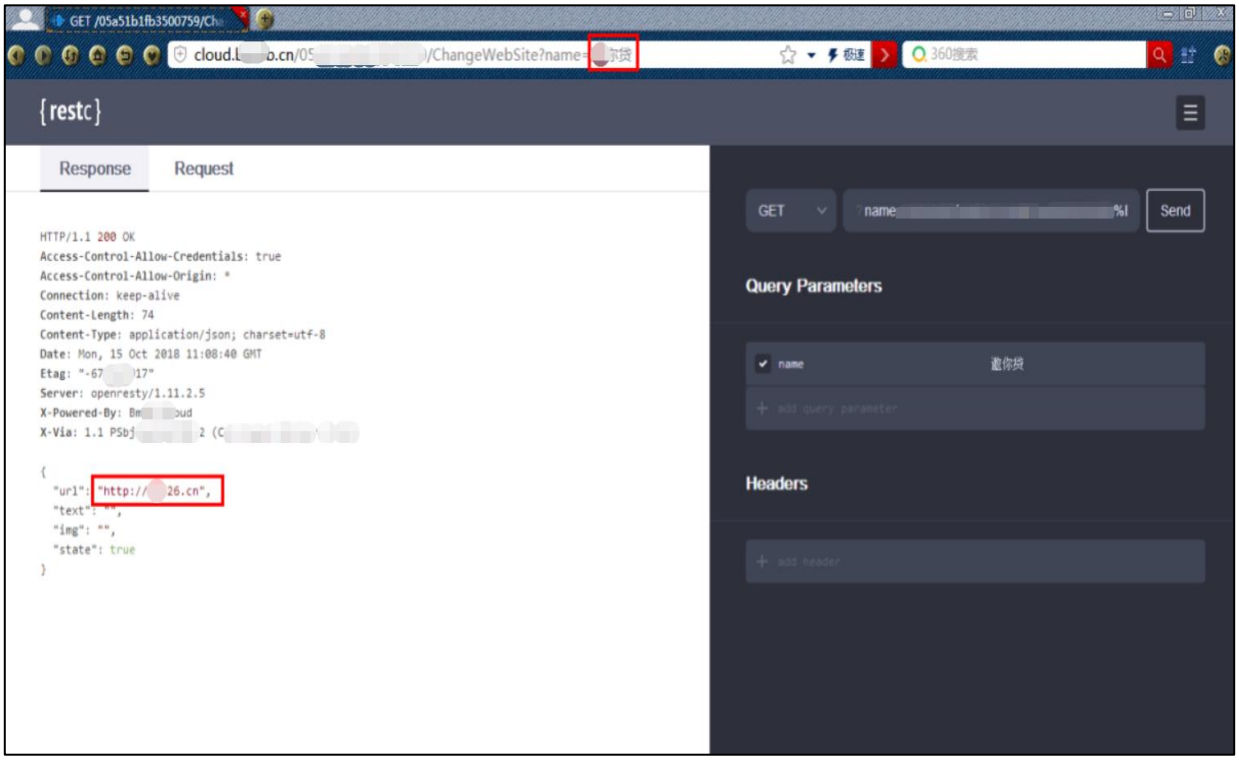
方式 2：短信内钓鱼网址伪装

因此网络黑灰产转而盯上了钓鱼网站本身，一方面通过在钓鱼网站页面对非移动设备访问设置限制，另一方面对虚假应用的真实下载地址进行隐藏，试图躲避短信识别模型对于短信内钓鱼网址的识别。随着网址模型+短信算法模型的再次升级，此种方式再次被识别。

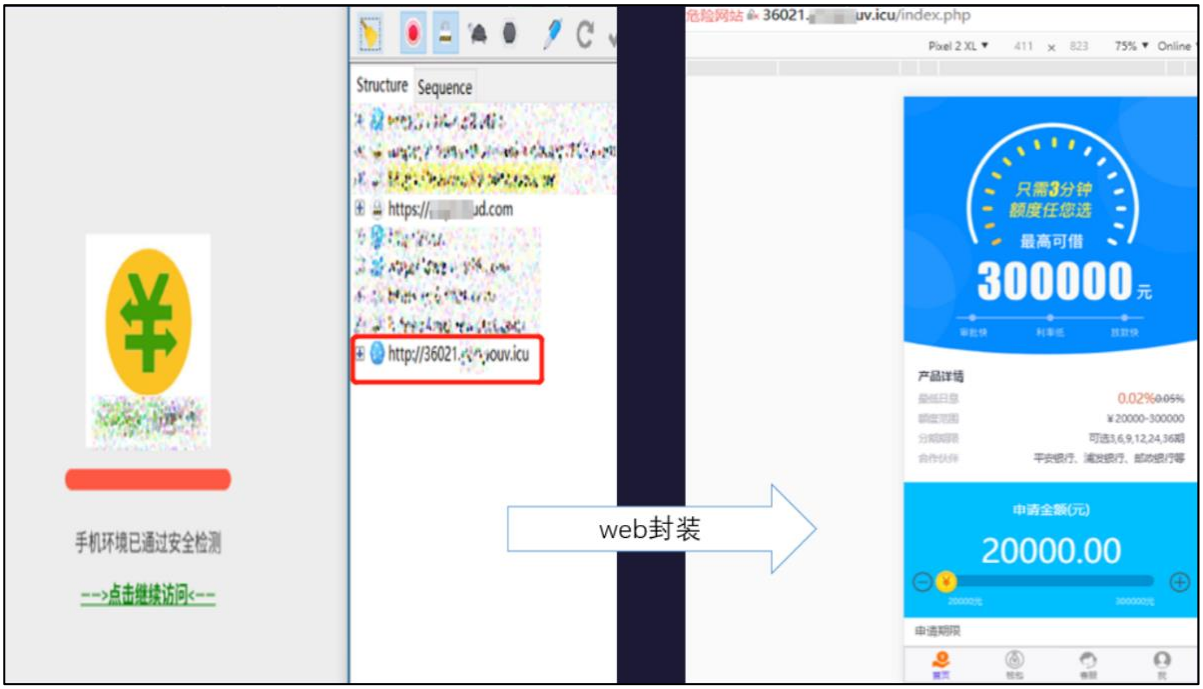
二、从云控应用与子域名群站

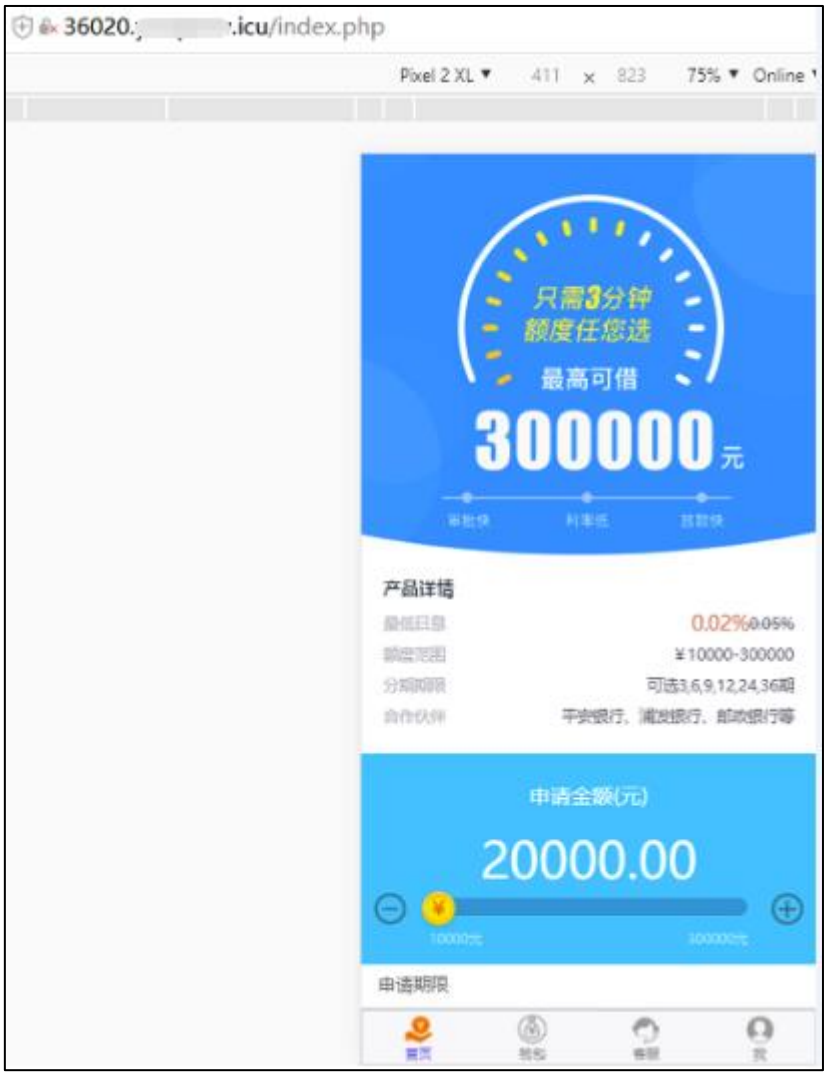
2018 年，在对部分虚假借贷应用逆向分析时，发现一部分应用通过网址封装生成，APP 显示的内容与网站内容一致。当网站无法访问时，APP 也会直接报错。通过下图可看出部分虚假 APP 调用的网址及报错情况：

在对部分关联的网址深入分析时，发现其通过 WEB 接口提供商，批量生成不同名称的虚假借贷 APP。如“京小贷”APP 调用的请求网址为：（http://cloud.b***.cn****=京小贷），不法分子通过更改 bm***.cn 的链接参数，使得 APP 调用不同的 APP 链接。如参数设置为京小贷时，APP 调用京小贷的 URL，设置为*你贷时，APP 调用*你贷的网址。通过查询发现“b***.cn”为一个提供后端服务的平台，为云服务提供商，提供 APP 源码、数据库、短信验证码等服务。不法分子通过对服务平台的滥用，实现了对虚假借贷 APP 的批量化生成，使得诈骗类软件的变化更难以控制。



2019 年，在对应用逆向分析的过程中，我们发现大部分虚假借贷类应用仍通过网址封装生成，但由云控的方式转向通过不同子域名的方式生成不同的网址。如下图展示的应用，其平台使用的网址为 36021.****.icu，在对域名深入分析的过程中我们发现，其子域名 36019、36020、36022、36023 也为虚假借贷平台。相较于云控方式，子域名形式，其服务器与解析方式可控，不法分子可将子域名解析至不同服务器中的不同的 web 页面，实现单一网站被拦截后快速上线新网站的目的。





云控应用及子域名生成的应用，虽然最终产生的网址不同，但其本质都是调用同一个 host 域名，一旦判断出该主网站（host）是虚假借贷平台服务时，拦截其主网站（host），即可拦截其运营的所有关联域名。

三、“第三方在线客服平台”代替传统社交软件，或成孵化诈骗的温床

中国互联网的发展推动了在线社交行业的发展，QQ、微信等社交平台由于其便利性、用户群体众多等特点，常被不法分子在实施诈骗的过程中进行使用，与用户进行沟通。但随着 2019 年国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室组织开展专项打击行动，对缅北部分电信网络诈骗活动严重区域的 QQ、微信、支付宝、POS 机等社交和支付账户采取封停措施后，大量诈骗团伙使用的社交账号已遭到停用。

于是不法分子转而将目光盯上了第三方在线客服平台。第三方客服系统类似于 CMS（网站内容管理系统），本身是帮助企业解决平台客服接入管理问题。通过平台接口的方式接入企业平台，降低企业研发和运营成本。但随着网络安全监管的升级，黑灰产人员使用的 QQ、微信等社交账号存在易被查封关停的风险。

为解决查封问题，黑灰产人员盯上了第三方客服系统，利用“虚假”的认证信息，将第三方客服系统接入到黑灰产平台，为虚假平台提供在线客服服务。

第五章 网络借贷诈骗防范与治理对策

消费借贷市场的蓬勃发展在促进金融市场发展的同时，也吸引了网贷黑灰产业的进场。网贷黑灰产业的发展与升级，不仅影响了金融产业的良性发展，更给正常借贷用户带来了资金损失。针对网贷黑灰产业的肆虐，可以从以下几个角度进行治理[①]。

一、个人建立信息保护意识、企业建立客户隐私保护机制

从信息泄露的来源来看，一方面来源于用户的主动性泄露，一方面来源于企业的被动性泄露，黑客入侵企业服务器，获取企业的用户信息。对于用户的主动性泄露，用户需要养成个人信息保护的安全意识，不轻易上传包含个人信息的照片。对于手机、电脑等存在个人信息的设备，丢失后进行远程擦除。设备在二手平台出售前，通过专业软件消除保留的个人资料或去除存储媒介后售卖。对于企业的被动性泄露，企业建立业务逻辑测试模型，挖掘出业务可能存在的漏洞与不足并及时修补。同时时刻关注行业风险动向，及时调整自身的云端风险监控模型与机制，防止自己基础数据被黑灰产入侵，发生信息泄露事件。

二、平台审核机制规范化，加大二次校验力度

虚假网贷诈骗事件多发，究其原因，一方面是由于黑灰产资源售卖渠道多、开源程序多、制作教程多，搭建成本低、搭建难度低。通过搜索引擎、电商平台等渠道可以找到众多的源码。作为渠道入口的平台，需要对此些违规产品进行过滤，降低其在搜索结果中的权重，降低可能造成的影响。

另一方面是由于第三方技术平台对于其服务的使用者没有进行完善的资格审核和二次校验。比如使用第三方客服平台的注册人为某科技有限公司，但实际使用此第三方在线客服服务者是虚假借贷平台。平台需要在前期校验购买服务的资格后，持续对使用者进行监督，防止平台被利用。

三、全行业加强技术管控、遏制虚假网贷快速发展趋势

黑灰产在技术、话术等多方面，不断完善其自身的诈骗手法，防止在实施诈骗的过程中被识别。如诈骗团伙在使用未含备案信息的域名被安全厂商识别出诈骗特征后，转而开始利用含有备案信息的域名来躲避安全厂商对于欺诈类域名的识别，双方呈现出动态博弈的特征。

面对此种现象，安全厂商不能仅仅“盯着”实施诈骗的样本本身进行事后拦截，还需要从黑灰产业链的角度看待诈骗事件。如针对诈骗团伙使用的备案域名，需了解备案域名的来源、原理、买卖方式。一方

[①] 360 企业安全,360 手机卫士,360 安全大脑.2019 年手机安全状况报告[R]. 360 研究报告官网，2020

面拦截售卖渠道、一方面通过域名 WHOIS 历史节点、同源（IP）网站内容特征、历史节点内容快照等多种方式，实现对网站的识别，而非仅仅通过域名的备案信息判断网站真伪。

四、加强企业内部管理和渠道管控，促进移动转售行业持续健康发展

针对卡号商贩的违规办卡，违规收卡，运营商可以加强办卡过程中的身份认证，防止黑灰产从业人员假借他人身份或利用空卡公司大量办卡。针对违规借贷欺诈短信，运营商需要加强短信通道号发送内容审核，防止短信通道号被利用；另一方面网络安全厂商、手机厂商、运营商也要通过短信关键词、短信语义，短信画像等方式提升虚假借贷短信识别的能力。