威胁猎人
THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

黑产大数据

2023年第三季度互联网黑灰产研究报告

THREATHUNTER

目录

Contents

前言

近年来黑灰产业链不断成熟壮大，其攻击技术、资源快速更新，企业与黑产的对抗愈发激烈。“面临哪些黑产攻击”、“黑产会使用哪些技术/资源进行攻击”、“面临哪些风险”等问题仍然困扰着企业内部安全运营人员。

依托于黑产情报的长期监测、挖掘以及黑产攻防研究，威胁猎人针对企业潜在风险，从 2023 年第三季度黑灰产攻击资源、业务欺诈场景、数据泄露场景等维度进行全面梳理及分析，期望帮助更多企业深入了解黑灰产业，有效防控各类攻击风险，避免损失。

01

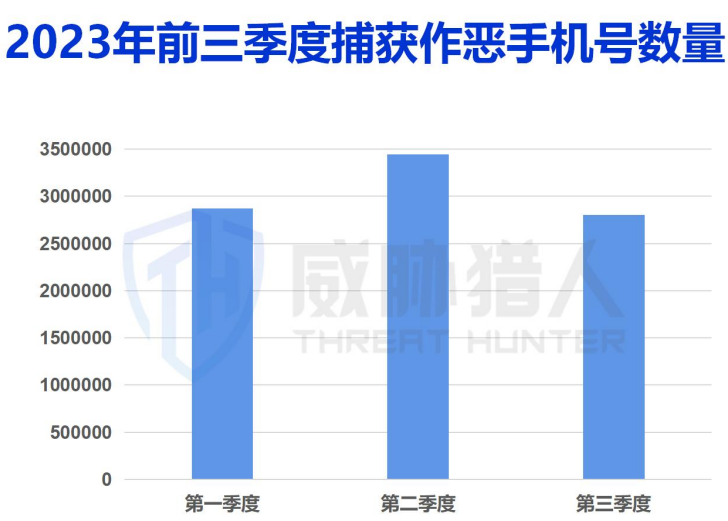
2023 年第三季度
黑灰产攻击资源分析

一、2023 年第三季度黑灰产攻击资源分析

1.1 第三季度黑手机卡新增量分析

1.1.1 第三季度黑手机卡捕获总量较第二季度下降 26.27%

据威胁猎人业务风险情报平台数据显示，2023 年第三季度黑手机卡捕获总量较第二季度下降 26.27%。



经威胁猎人情报专家分析，持续下降的主要原因是：

8 月初某头部接码平台被关停，导致大量黑手机卡供应商和使用黑手机卡的黑产团伙无法正常供应和使用黑手机卡，从而影响了黑手机号的流通。受此影响，第三季度黑手机卡“每月新增量”亦持续下降。

2023年第三季度每月新增作恶手机号数量

1.1.2 第三季度拦截卡新增数量持续下降

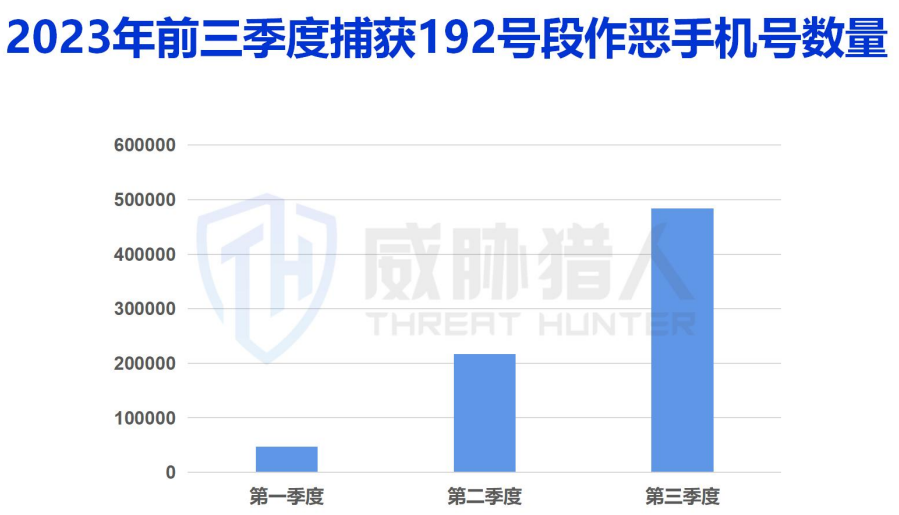
2023 年第三季度拦截卡新增数量持续下降，第三季度拦截卡新增数量仅为第二季度的 47%。

2023年前三季度新增拦截卡作恶手机号数量

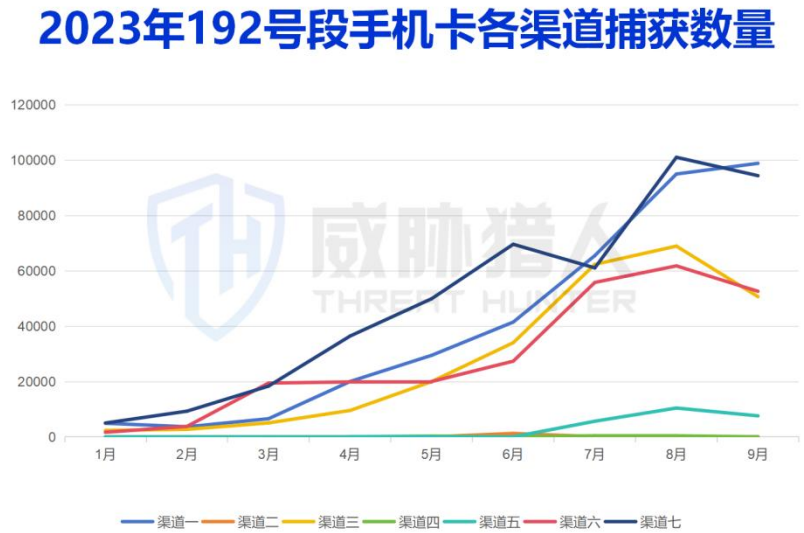
经威胁猎人情报专家分析，下降的主要原因是：自 2023 年 4 月起，三个头部接码平台提供的新拦截卡数量持续减少，进而导致新增的拦截卡数量持续下降。

1.1.3 第三季度季度 192 号段使用量较第二季度上升 123%

据威胁猎人业务风险情报平台数据显示，2023 年第三季度，192 号段黑手机卡的使用量是第二季度的 2.23 倍。



经威胁猎人情报专家分析，第三季度新增量较大的主要原因是：自第一季度起，各黑卡供应渠道持续投入新的 192 号段手机卡。同时自第三季度开始，有 4 个供应渠道进一步增大 192 号段手机卡的投入规模，使得第三季度新增量进一步增加。



1.2 第三季度风险 IP 捕获量分析

1.2.1 第三季度风险 IP 捕获总量较第二季度上升 2.8%

2023 年第三季度风险 IP 捕获总量较第二季度上升 2.8%，数据并未出现明显波动。

1.2.2 木马伪装成正常软件后将正常用户 IP 上传至代理平台

威胁猎人研究人员在第三季度发现正常用户 IP 出现在代理 IP 平台的 IP 池中，并呈现出明显上升的趋势。该情况会导致一个 IP 在短时间内的操作行为同时包含正常用户行为及黑产作恶行为。

这类 IP 在业务上的表现为：大部分时间是正常用户进行操作，如点击、充值、浏览等行为均正常，少量时间会出现短暂的作恶行为。**因此对于甲方风控来说，平台会认定该用户为正常用户，进而忽视其短暂的作恶行为，给黑产可乘之机。**

同时，威胁猎人研究员溯源到了背后的作恶工具，这类工具将木马伪装成正常软件供用户下载使用。用户安装并首次运行工具后，木马即可上传正常用户的 IP 至代理平台供黑产作恶使用。

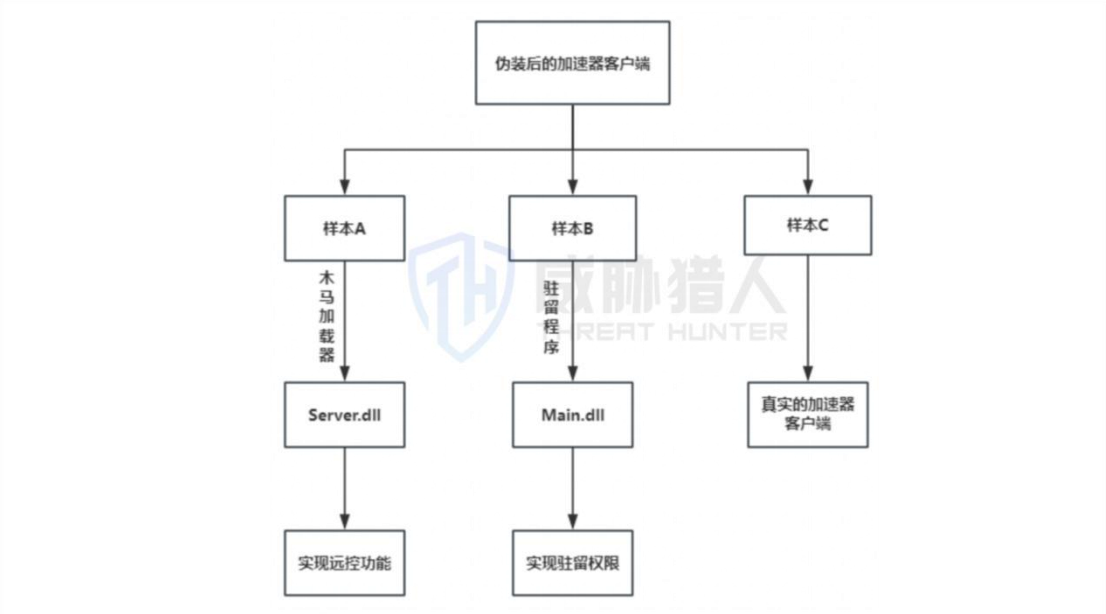
以捕获到的一个“xx 加速器”工具为例，其作恶流程为：

（1）正常用户在电脑上安装"xx 加速器"后，程序释放木马文件到指定位置；

（2）木马对特定进程进行注入，劫持用户 IP 进行任意操作；

（3）木马通过特定方式维持其运行权限，达到“加速器关闭后木马仍能运行”的目的；

（4）运行真正的加速器程序，供用户使用。



研究人员通过技术分析提取出三个可执行程序，分别记作样本 A、B、C：

样本 A：一个实现木马加载功能的可执行程序

样本 B：一个维持木马驻留权限的可执行程序

样本 C：一个真实的加速器客户端

样本 A：

通过分析，从功能上可以判定样本 A 是一个木马加载器，它具备解密二进制代码、内存加载 PE 的功能。

功能	解释
功能一	解密二进制数据，然后通过内存加载的方式，将解密后的PE代码加载到进程空间
功能二	手动转存解密后的二进制数据，发现是一个DLL，该DLL是Farfli木马家族的远控DLL，具备远控木马的完整功能

样本 B：

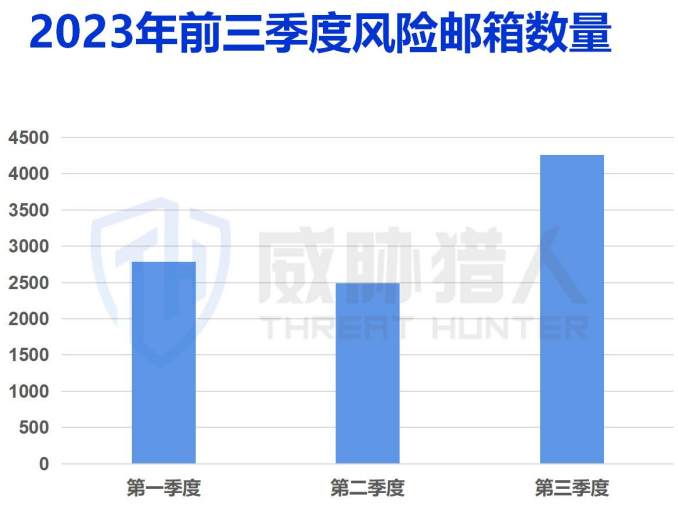
通过分析，从功能上可以判定样本 B 的主要功能是创建服务，维持木马驻留权限。

功能	解释
功能一	解密出C2地址：hackerXXXXXX.XXXXXX.net:8088，在受害者机器上线前使用互斥体来判断是否存在多个运行实例，防止重复上线。
功能二	维持木马驻留权限。 方法一：创建名为GUpdate的系统服务，设置注册表路径，添加一段假装为系统核心服务的描述以及服务名称，设置成功则表示驻留权限完成，随后该执行程序退出。 方法二：伪造以svchost为宿主的系统服务，创建隐藏桌面，并从程序设置中的C2地址下载并执行程序，以达到设置驻留权限的目的。

1.3 第三季度风险邮箱捕获量分析

1.3.1 第三季度风险邮箱捕获总量较第二季度上升 71.16%

2023 年第三季度，威胁猎人持续覆盖及监测临时邮箱网站，统计发现第三季度风险邮箱捕获总量较第二季度上升 71.16%。

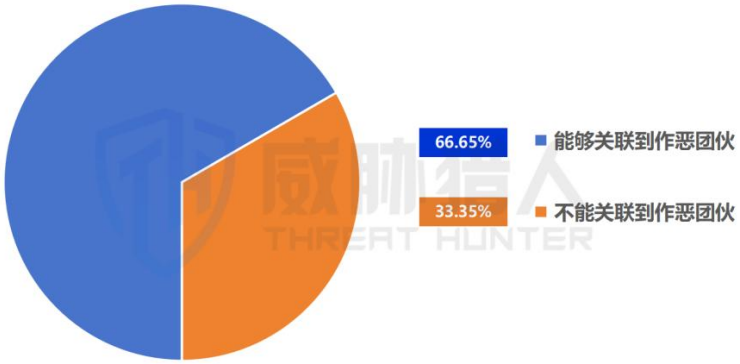


1.3.2 被黑产用来作恶的临时邮箱，呈现明显的团伙聚集性

在海外，电子邮箱注册依旧是主要的账号注册方式之一。而临时邮箱由于具有低成本、可匿名、一次性等特点，成为了黑产对企业海外业务实施攻击的首选物料。

威胁猎人研究人员针对捕获的 46737 个有效临时邮箱域名样本进行 MX、IP 及域名注册信息分析，发现有 66.65%（共计 31150 个）邮箱域名均存在特征共性，能关联到多个作恶团伙。

风险邮箱关联作恶团伙占比



对上述 31150 个邮箱域名进行团伙分类，可整理出六个黑产团伙，且相同团伙下的多个临时邮箱往往呈现出特征的聚集性。有的团伙是“强关联”特征，只要出现就可以判定是来自同一团伙；有的团伙是“弱关联”特征，需要多个特征结合来判定：

强关联	弱关联
• 邮箱域名解析的MX一致 • MX解析的IP一致	• 注册机构一致以及注册时间间隔很短 • 域名服务器一致 • 登记人信息一致

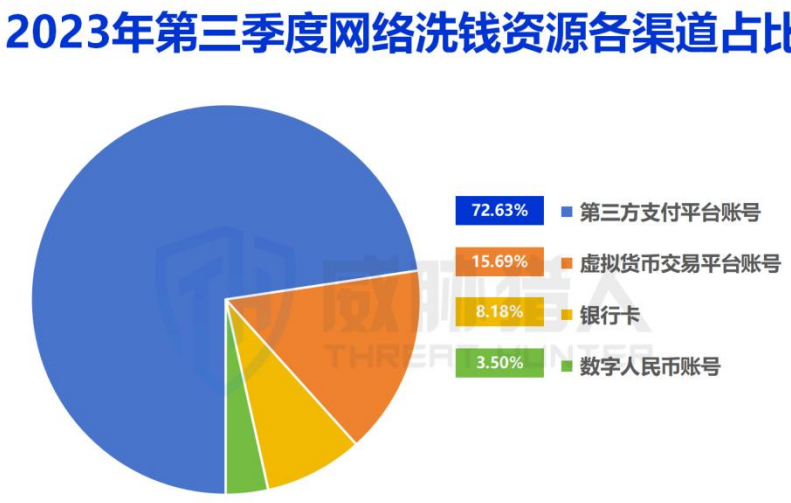
以关联临时邮箱最多的一个团伙为例：**有 10085 个邮箱域名解析到同一 MX（mail.***.kr），邮箱后缀基本为 xxx.kr，可直接判定来自同一团伙。该团伙关联到的邮箱特征如下：**

团伙	强关联特征：邮箱域名解析到的mx	弱关联特征：邮箱域名的二级域名	弱关联特征：登记人	弱关联特征：注册邮箱	弱关联特征：域名服务器
临时邮箱团伙A (邮箱1~邮箱10085)	均为mail.***.kr	二级域名有66个，格式均为xxx.kr	Y**N	ax*****d@gmail.com	***.tad.cc、***.tad.cc
		nice***.com	ju****suk	***@naver.com	N***.HO***NG.CO.KR
		ho*****.com			N***.HO***NG.CO.KR
		ba*****.com			N***.HO***NG.CO.KR
		hig*****.com			N***.HO***NG.CO.KR
		sap*****lur.xyz	未公开	未公开	***.NS.CLOU***ARE.COM ***S.NS.CLOU***ARE.COM
		ss*****ne.me	未公开	未公开	****.domai****trol.com ****.domai****trol.com

1.4 第三季度网络洗钱资源分析

1.4.1 第三季度网络洗钱资源各渠道中，第三方支付平台占比达72.63%

2023 年第三季度洗钱资源渠道中，占比最高的为第三方支付平台账号，其次为虚拟货币交易平台账号、银行卡、数字人民币账号。



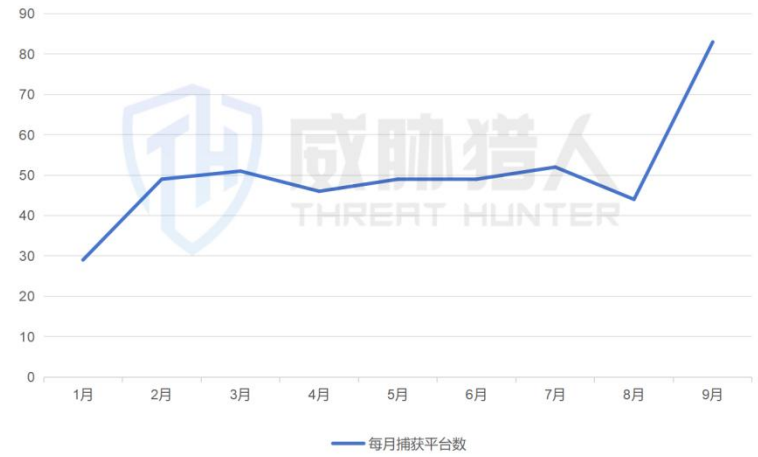
1.4.2 第三季度数字人民币捕获量在 9 月出现明显增长，月增幅超 270%

威胁猎人发现黑产利用数字人民币进行洗钱的情况整体呈上升趋势，尤其是 9 月，月增幅超过了 270%。

经威胁猎人情报专家分析，出现较大增幅的主要原因是：9 月份出现了大量新的支持数字人民币洗钱的四方支付平台，较 8 月份增加了 39 个平台。

此外，虽然第二季度的四方支付平台数量与第一季度相近，但威胁猎人情报专家发现：自 5 月起，已有部分四方支付平台开始增加数字人民币这一渠道的洗钱频率，使得数字人民币洗钱记录捕获数开始上升。

涉及数字人民币洗钱的四方支付平台数量



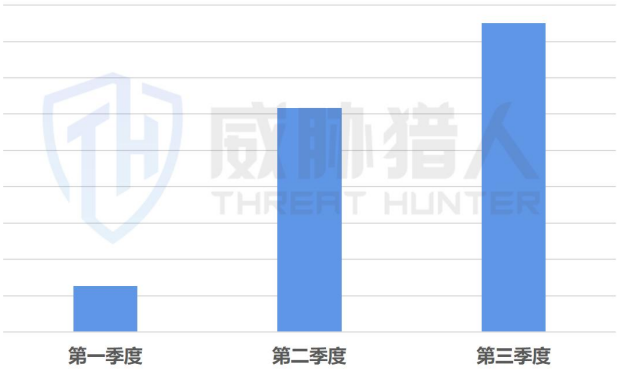
1.4.3 第三季度涉及洗钱的对公账户捕获总量较第二季度上升37.86%

银行对公账户具有收款额度大、转账次数多等特点，这使得“对公账户”常常作为黑钱转账的集中点及发散点，在黑产洗钱链条中担任极其重要的位置。

在打击洗钱犯罪过程中，银行对涉及洗钱的对公账户进行风控也是十分重要的一环。因为一个对公账户的收款额度往往在几百万到几千万不等，及时发现涉嫌洗钱的对公账户并进行针对性风控，往往能中断某个黑产团伙的某一洗钱链条。

自2023年3月起，威胁猎人持续覆盖及监测黑产在洗钱过程中所使用的银行对公账户资源，发现涉及洗钱的对公账户数量持续上升。

2023年前三季度
涉及洗钱的对公账户捕获数量



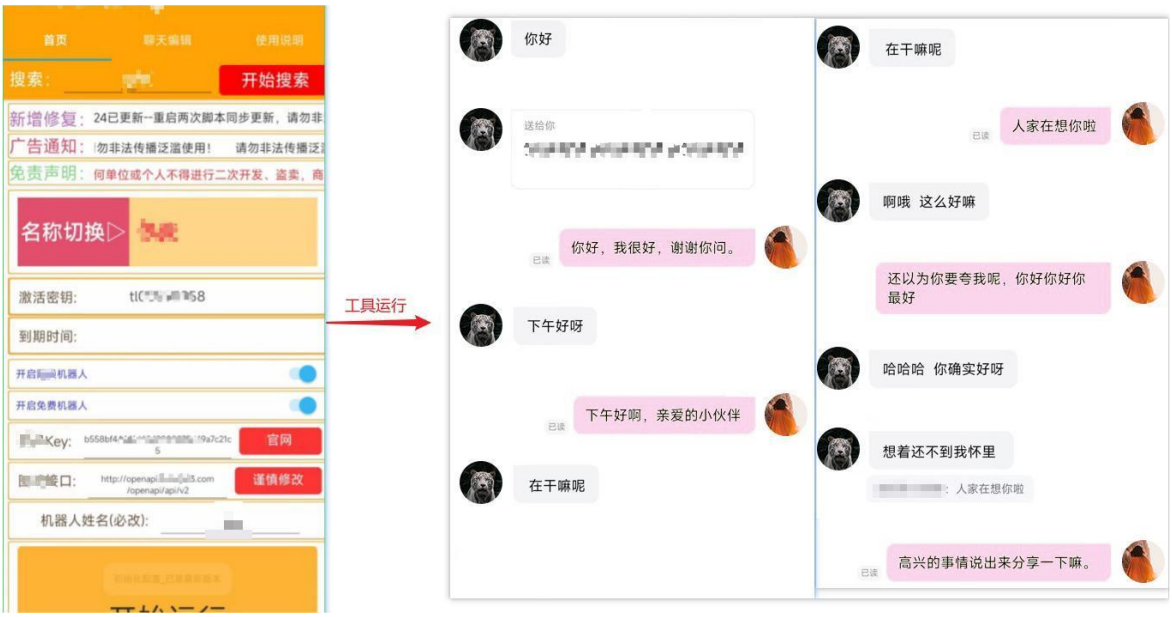
02

2023 年第三季度
业务欺诈场景分析

二、2023 年第三季度业务欺诈场景分析

2.1 黑灰产接入 AI 机器人，社交引流话术更智能

威胁猎人情报研究员在第三季度发现，黑灰产在社交引流场景已经接入 AI 机器人，使得引流聊天更智能。以捕获的一款自动聊天工具“AiTuLing”为例，该工具除了常规的“基于预设话术进行引流”外，还支持接入 AI 机器人，同时该工具**支持市面上近百个社交平台的自动引流。**



与传统的预设话术进行回复引流相比，两者的特点如下：

	预设话术	AI机器人
特点一	相同的平台只能挂一个社交账号（由于话术固定，挂多个账号会导致账号回复内容相同，引起平台风控）	相同的平台，能同时挂多个社交账号
特点二	每换一台手机设备，话术文件需保存在手机存储目录上	直接在引流工具中填入机器人的接口及key值即可
特点三	回复速度慢，回复内容固定	回复速度快，更接近真人

在使用成本上，AI 机器人的接入成本也极为低廉，**最低只需 19.9 元/月即可。**目前此类引流工具多被黑灰产用于社交场景上的引流下载、色情诈骗目标的初步筛选，对社交平台的内容风控提出了新的挑战。

2.2 AI 发展使得换脸成本降低，人脸验证安全性需警惕

针对近期热度较高的基于 AI 换脸技术进行诈骗的案例，威胁猎人研究人员对相关作恶工具及作恶流程进行了研究，并最终成功绕过某银行的人脸认证。

公安机关侦破“AI换脸”相关案件79起 抓获犯罪嫌疑人515名

2023-08-10 12:01:15 来源： 新华社

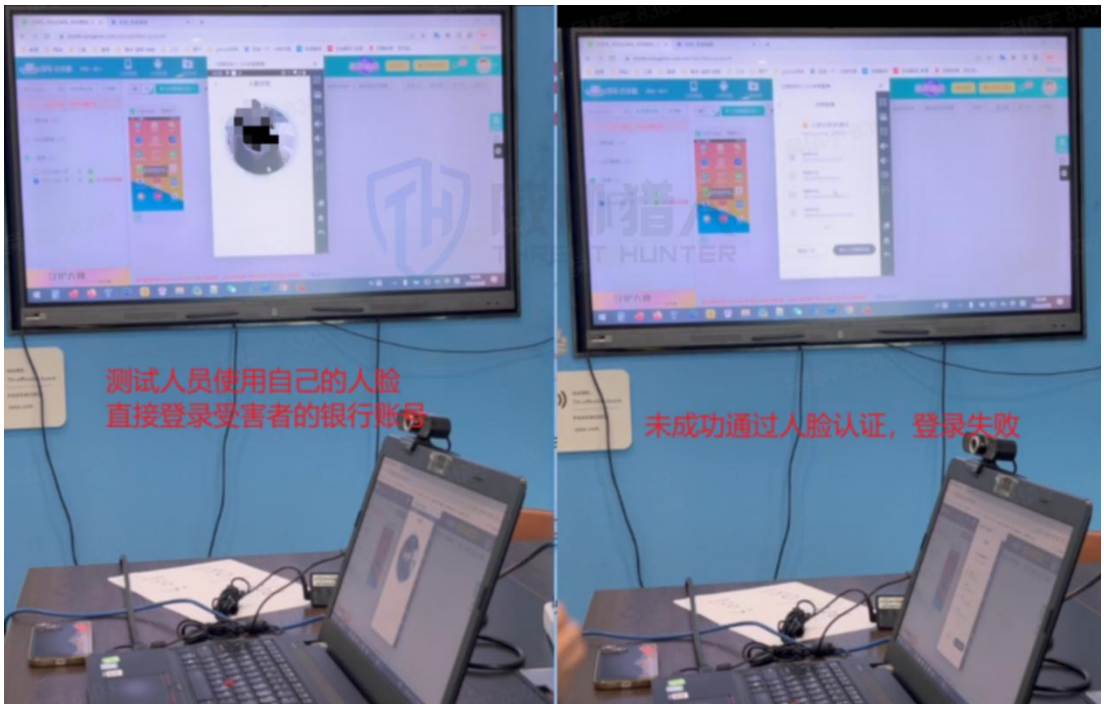
公安部8月10日在京召开新闻发布会，通报公安机关打击侵犯公民个人信息违法犯罪成效情况。公安部网安局政委孙劲峰介绍，针对“AI换脸”导致群众被欺诈的问题，公安机关发起专项会战，侦破相关案件79起，抓获犯罪嫌疑人515名。

研究发现，黑灰产在作恶时使用的工具如下：

作恶工具类型	工具作用
AI换脸软件	基于目标人物的多角度图片或视频，进行换脸训练，并输出训练好的换脸模型及视频。
AI实时直播换脸软件	基于AI换脸软件输出的换脸模型，能把直播过程中直播者的人脸实时替换成目标人物的人脸，并输出对应的预览窗口。
视频录制和直播软件	把预览窗口作为画面输入源，输入到虚拟摄像头中进行直播或视频会议；或者通过rtmp推流到具体服务器地址中进行直播。

威胁猎人研究员的攻击复现流程如下：

（1）首次登录，测试人员使用自己的人脸模拟攻击者登录受害者银行账号，未成功通过人脸认证。



（2）第二次登录，测试人员使用受害者的 AI 换脸视频，并通过特定方式使得“换脸视频的画面”作为登录设备摄像头获取到的画面，再次登录受害者的银行账号，最终通过人脸认证并成功登录。

2.3 黑灰产账号注册及绕过检测形式愈加多样化

账号是黑灰产针对平台实施攻击的基础，但由于 APP 之间登录方式不同、APP 的风控程度松紧不一等原因，不同的“账号使用方法”会使得账号在平台上的使用寿命长短不一。为了最大限度延迟作恶账号的使用时间，黑产针对不同的情况推出不同的账号注册、绕过检测的方法。

以下为威胁猎人整理的部分黑产作恶账号使用方式：

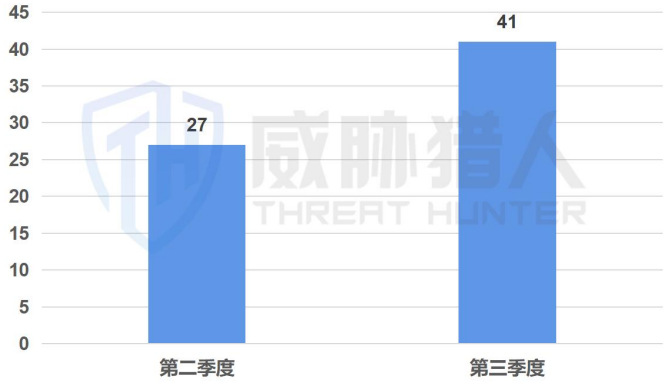
账号类型	说明	登录方式
账密号	登录账号+登录密码，最常见的登录方式。	直接使用账号密码即可登录。
通讯录号	部分 APP 支持手机通讯录进行登录校验，部分黑产会在售卖账号+密码的时候，再提供一个存有通讯录信息的 vps 文件。	黑产只需在攻击设备上导入 vps 文件，再进行账号密码登录，并在遇到登录验证时选择通讯录验证即可。
串码号	串码即手机号串码（IMEI），是手机的身份证号。注册账号的黑产通常会把注册的账号及注册账号的手机设备的串码一起售卖。	攻击者通过特定工具修改手机的串码，让平台误以为攻击设备是一个安全的设备（非新设备）后，直接使用账号密码即可避免触发登录验证而登成功。
备份文件号	注册账号的黑产在注册成功一个账号后，会通过改机工具把目标 APP 的账号信息、缓存文件、设备参数备份为一个文件。	攻击者获取到备份文件后，只需要借助改机工具即可把备份的信息在攻击设备上还原，使平台误以为攻击设备是一个安全的、已登录账号的设备（非新设备）。
备份包号	利用手机自带的数据备份功能，对特定 app 进行数据备份，并生成备份包。	购买备份包后，放置到手机特定目录下；再通过手机自带的数据回复功能即可进行账号的登录。

以备份包号登录社交 APP 为例，其使用流程如下：

2.4 黑灰产结合贷款平台和虚拟货币，转移洗钱风险

威胁猎人研究员在 2023 年第二季度发现部分黑产开始利用贷款平台进行洗钱，涉及贷款平台 27 家，在第三季度发现受影响平台上升至 41 家，较第二季度增长 51.85%。

2023年第二及第三季度
被黑产利用进行洗钱的贷款平台数量

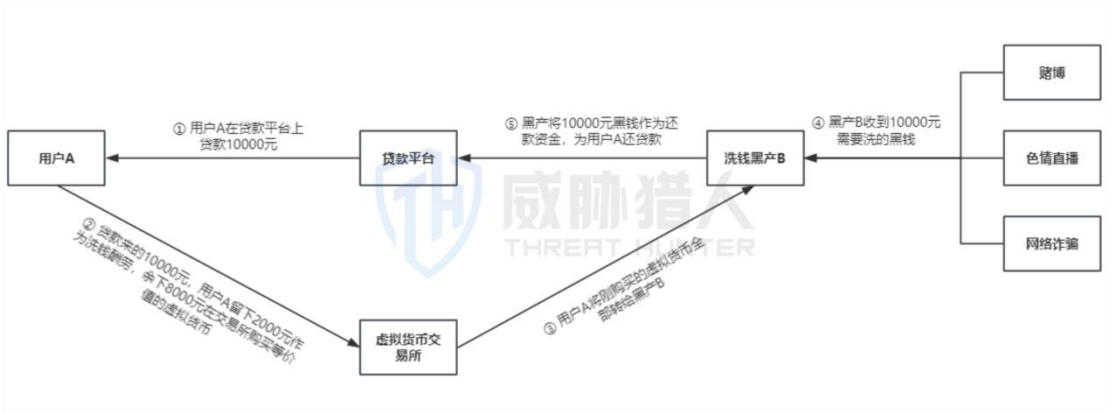


黑产将贷款平台与虚拟货币结合，借助第三者协助，将贷款平台贷出来的钱用于购买较难监管的虚拟货币，再把黑钱作为还贷资金，转账给贷款平台，将洗钱的风险转嫁至贷款平台处。

在过往的洗钱方式中，会存在黑产直接使用黑钱在虚拟货币交易平台中大量购买虚拟货币的情况，这使得黑产的虚拟货币账户很容易被交易平台发现并进行风控。

基于“将贷款平台与虚拟货币结合”的方式，黑产能将购买虚拟货币这一操作转移到第三者身上，同时由于第三者用于购买虚拟货币的资金来源渠道是正常的，能极大降低虚拟货币交易平台察觉的可能性。

关于此类洗钱方式，威胁猎人研究员总结的流程如下：



该洗钱方式带来的最终结果是：

用户A	通过协助他人洗钱，获利2000元
洗钱黑产B	通过损失20%的资金，把黑钱转换成受监控风险较低的虚拟货币
贷款平台	被洗钱黑产利用，对公账户中收到黑钱

2.5 黑灰产利用云手机平台提供的 iOS 云设备，降低 iOS 群控成本

威胁猎人研究员发现部分黑产使用 IOS 云手机进行作恶，针对此情况，研究人员对目前市面上提供 IOS 云手机服务的云手机平台进行了相关调研。调研结果如下：

平台	IOS 云手机价格	能否通过 app store 或爱思助手安装应用	是否为越狱设备	能否安装越狱插件	是否自带改机功能
平台一	88 元/月	能 通过 app store 及爱思助手均可以安装应用	是	能 无需平台审核就能直接安装（如佐罗）	有
平台二	77 元/月	能 通过其自带的应用市场能进行应用的安装	暂无法确定	暂无法确定	无
平台三	iphone8 88 元/月 iphone8p 108 元/月 iphoneSE2 138 元/月	能 通过 app store 及爱思助手均可以安装应用	是	能 但安装的插件需要先经过平台审核	无
平台四	77 元/月	能 通过 app store 及爱思助手均可以安装应用	是	能 但安装的插件需要先经过平台审核	无

iOS 云手机作恶带来的风险如下：

（1）黑产获取 iOS 设备进行攻击作恶的成本降低。以往进行攻击，往往需要购买几百到上千元不等的真实 iPhone，而现在只需花费几十元/月租用 iOS 云手机即可。

（2）节省了黑产安装、配置作恶环境所需的时间，提高了黑产的攻击效率。购买的 iOS 云手机已越狱、能安装不同的越狱插件，还自带改机工具，节省黑产安装、配置作恶环境的时间。

此外，由于 iOS 系统对应用权限申请的严格限制，使得大部分互联网公司在 iOS 设备上获取设备信息的难度远大于安卓端设备，这在一定程度上可能会使得平台在 iOS 设备上进行风控识别的难度更高，具体表现为：相同的攻击流程下，黑产使用 iOS 设备进行攻击被平台发现的可能性更低，**导致黑灰产把 iOS 云手机作为主要的攻击设备之一。**

针对此类情况，威胁猎人建议企业应及时获取此类平台样本，进行相关样本分析和防御。

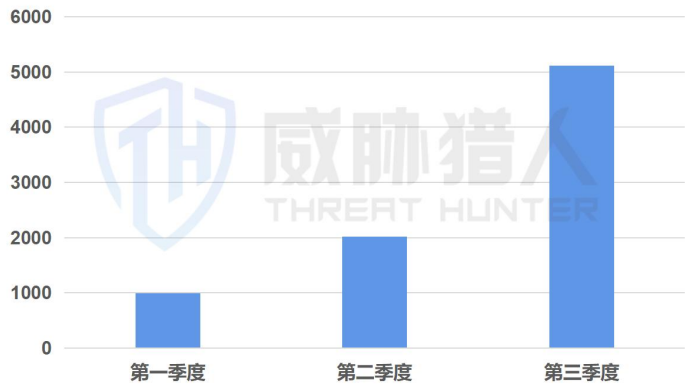
03

2023 年第三季度
数据泄露场景分析

三、2023 年第三季度数据泄漏场景分析

3.1 第三季度数据泄露事件较第二季度季度增加 153%

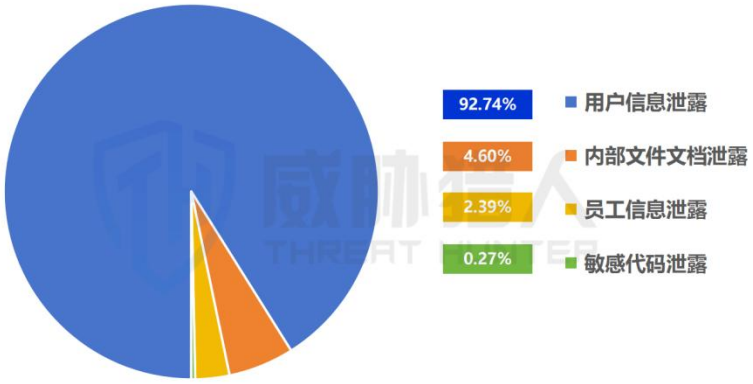
2023 年第三季度，威胁猎人风险情报平台监测到数据泄露相关情报 7300 多万条，梳理出有效的数据泄露事件共计 5110 起，较第二季度增加 153%。



3.2 第三季度数据泄露类型仍以用户信息为主，占比达 92.74%

第三季度发生的数据泄露类型仍以用户信息为主，占比达 92.74%。此外还有内部文件文档、内部员工信息及敏感代码等泄露信息类型。

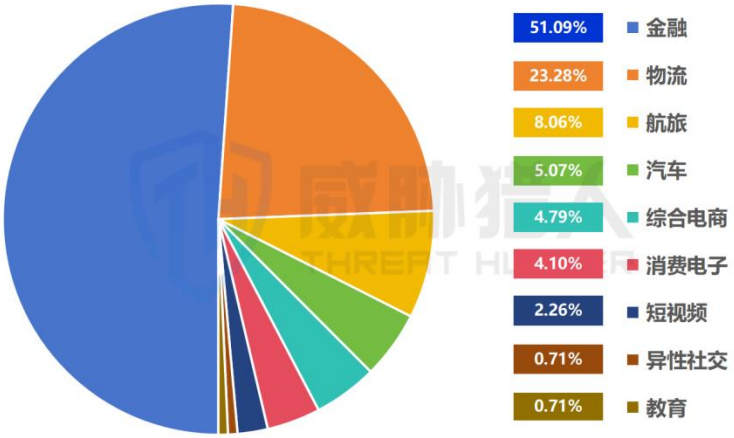
2023年第三季度数据泄露信息类型占比



3.3 第三季度数据泄露涉及行业广泛，金融、物流行业仍是重灾区

从行业分布来看，第三季度数据泄露事件涉及多个行业，其中金融和物流行业依旧是重灾区。

2023年第三季度各行业数据泄露事件数占比

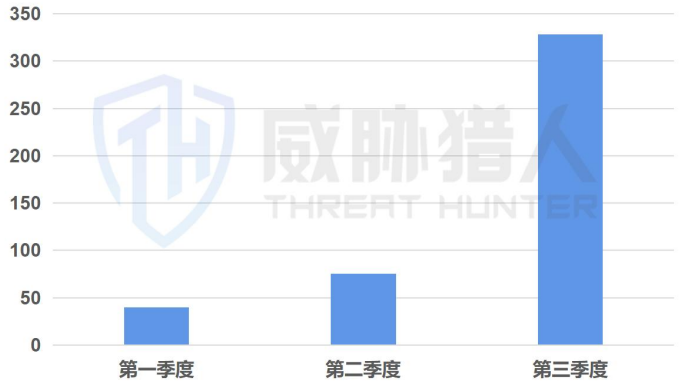


3.4 第三季度航旅行业的数据泄露事件数量持续上升

航旅行业的数据泄露事件数较第二季度增加 253 起，增幅 337.33%。

经威胁猎人情报专家分析，持续上升的主要原因是：受旅游市场复苏的影响，国内国际航班火爆，黑产围绕航空行业的攻击持续不断增多，特别是针对各大航空企业的供应链、代理商等环节。最终带来的影响是大量不法分子利用航空数据进行诈骗。

2023年前三季度航旅行业数据泄露事件数



3.5 第三季度典型数据泄露事件分析

3.5.1 案例一：企业员工邮箱信息泄露，导致员工被钓鱼邮件诈骗

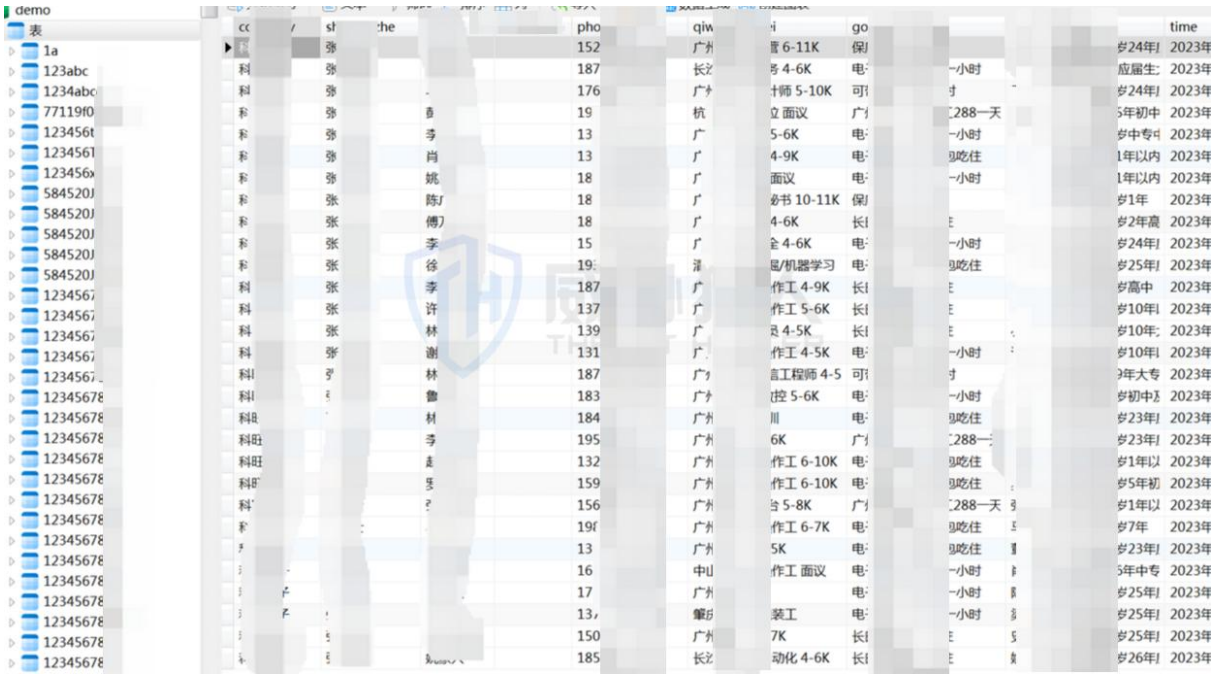
2023 年 8 月，威胁猎人在 Telegram 上发现国内某金融投资企业的员工邮箱信息泄露，导致员工被下游黑产进行邮件钓鱼诈骗。

据威胁猎人研究员分析，本次数据泄露主要原因为：该企业邮箱存在 API 安全漏洞，黑产借助漏洞暴力破解该企业邮箱并盗取员工邮箱信息。

3.5.2 案例二：第三方平台违规存储招聘网站简历，涉及简历数超 20 万

2023 年 8 月，威胁猎人安全研究员发现某招聘网站简历遭第三方平台违规存储，**涉及简历总数超过 20 万**，其中包含大量招聘者个人敏感信息。

第三方平台将爬取到的简历违规存储到了自己租用的服务器上，并提供工具供其平台用户查看爬取的简历信息。由于**工具内置了访问服务器数据的逻辑，包括数据库地址、账号密码等**，且**工具可公开下载**，故职业黑客能对该工具进行分析，获取数据库地址、数据库账号密码等信息，轻松**盗取服务器上的所有简历。**



因此，威胁猎人建议企业慎用小众开发的管理软件和工具，由于对数据存储的安全系数欠缺，很可能被获取到敏感数据。

04

结语

四、写在最后

黑灰产日渐猖獗，让各行业企业深受其害。**从 2023 年第三季度黑灰产大数据整体趋势来看，企业需要重点关注以下风险：**

1、木马伪装成正常软件后将正常用户 IP 上传至代理平台

这类 IP 在业务上的表现为：大部分时间是正常用户进行操作，如点击、充值、浏览等行为均正常，少量时间会出现短暂的作恶行为。**因此对于甲方风控来说，平台会认定该用户为正常用户，进而忽视其短暂的作恶行为，给黑产可乘之机。**

2、AI 聊天、AI 换脸等技术被黑产利用，攻击成功率大幅提升

① 对社交平台来说，AI 聊天技术的应用会使得黑产在进行引流操作时更难以识别，而 AI 换脸技术则会让黑产使用视频聊天这一功能进行诈骗的成功率大幅上升。

② 对于金融、支付等平台来说，大部分平台目前都将人脸认证作为转账等敏感操作的安全验证措施之一，AI 换脸技术的普及亦会使得平台人脸认证被绕过，用户资金被盗的情况频发。

3、金融行业数据泄露事件数持续上升，超越物流行业成为受数据泄露影响最大的行业

该情况会使金融平台的用户遭遇诈骗的概率大幅上升，备受监管压力的同时，给平台带来负面舆论影响。

针对以上作恶事件，企业应及时了解其作恶流程及细节，并结合自身业务场景建立具体的风控规则。此外，企业也需要意识到与外部黑产的对抗是动态的、持续性的，故此时可依托第三方黑灰产情报数据实现：

（1）在与外部黑灰产持续的对抗中，通过全网多渠道监测及时感知攻击风险，分析提炼出黑灰产具体的动向、作恶工具等攻击信息，及时进行针对性的防御。

（2）黑灰产发起具体的攻击必然需要用到基础的攻击资源，如手机号、IP、邮箱等，利用威胁猎人丰富的黑灰产情报数据，提取出黑灰产攻击模式及资源特征，与企业业务中的异常流量进行匹配，快速识别风险。

借助“情报”能力，企业可以从全局视角出发，全面、及时感知黑灰产团伙的轨迹及动向，精准预警并输出攻击者的 IOC 情报，然后联动风控系统、WAF 等快速处置攻击风险。面对日益严峻的黑灰产风险挑战，做到从容应对，有力反击。

威胁猎人 THREAT HUNTER

以 情 报 构 筑 数 字 化 安 全 基 石

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）

总部地址：深圳市南山区科华路3号讯美科技广场3号楼1609

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