

黑产大数据

2025年KYC攻击风险研究报告



关于威胁猎人

威胁猎人 Threat Hunter（深圳永安在线科技有限公司）成立于 2017 年，以黑灰产情报能力和反欺诈技术为核心，专注于及时、精准、有效的业务欺诈风险的发现和响应。

公司围绕不同行业在数字化发展过程中面临的业务欺诈、数据泄露、钓鱼仿冒、API 攻击等风险场景，提供成熟多样的产品与服务，并多次入选 Gartner 技术成熟度曲线报告、IDC 威胁情报领域代表厂商。

公司总部在深圳，在北京、上海、重庆、新加坡等地设有分公司，并在深圳和重庆两地建立数字风险应急响应中心（DRRC），为客户提供 7*24 小时全天候数字风险应急响应和及时、优质的服务支持。截至目前，公司已为金融、政务、物流、互联网、科技、零售等行业的 300 多家客户提供安全服务，覆盖 85% 头部互联网企业，每年帮助客户减少数十亿资金损失。



目录

一、2025 年 KYC 攻击风险态势	6
1.1 KYC 攻击呈现明显的金融行业聚集情况	6
1.2 KYC 攻击信息在暗网交流渠道上呈现上升趋势	7
1.3 KYC 攻击行业高度成熟，并根据产业链层级分化出不同类型的 KYC 攻击黑产	8
1.4 KYC 攻击范围广泛，欧洲、南美洲、非洲、东南亚是 KYC 攻击最活跃的四大湾区	9
1.5 KYC 绕过物料类型中，地址证明成为黑产售卖最为频繁的 KYC 攻击物料	10
1.6 KYC 个人攻击物料价格平稳，但企业证明类物料上升波动最大	12
二、2025 年 KYC 攻击产业链	14
2.1 产业链综述：从“作坊式”走向“精密工业化”	14
2.2、KYC 攻击上游分析：物料来源的“AI 化”与“定制化”	15
2.3、KYC 攻击中游分析——技术支持	19
2.4、KYC 攻击下游分析——KYC 代过组织“SaaS 化”运作	23
2.5、KYC 攻击变现环节分析——获利手段	25
三、2025 年 KYC 典型攻击案例	28
3.1 2025 年 KYC 产业攻击链结构	28
3.2 2025 年 KYC 产业链新型手法	29
3.3 KYC 攻击在电商行业的典型案例	30
3.4 KYC 攻击在金融/信贷行业的典型案例	34
3.5 KYC 攻击在虚拟币交易所行业的典型案例	37
四、结语	41

前言

随着数字化业务的全面铺开，KYC（Know Your Customer，身份认证）已成为金融、虚拟资产、电商与平台型业务中最关键的信任起点，也是风控体系的“第一道关口”。

然而，近年来黑灰产正持续整合数据泄露、伪造证件、AI 换脸等手段，围绕 KYC 认证流程形成高度成熟的攻击链条。从身份物料生产、技术绕过服务，到成品账号交易与资金变现，KYC 攻击已不再是零散的个体行为，而是一门具备规模化供给、标准化流程与高 ROI 的黑色产业链。

威胁猎人将基于全球黑灰产情报监测数据，从攻击目标行业分布、暗网与社群活跃度、产业链分工、区域风险以及核心绕过物料等多个维度，系统还原 2025 年 KYC 攻击的整体风险态势，揭示当前身份认证体系所面临的真实压力与结构性挑战。



01

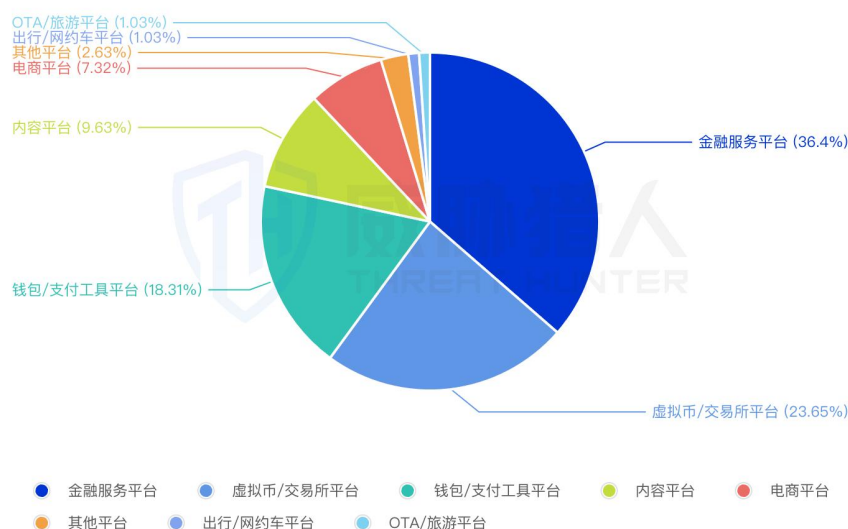
2025 年

KYC 攻击风险态势

一、2025 年 KYC 攻击风险态势

1.1 KYC 攻击呈现明显的金融行业聚集情况

2025年KYC攻击事件的行业分布情况



2025 年，KYC 攻击目标呈现出显著的行业集中趋势，金融服务、虚拟货币/交易所以及钱包与支付工具平台合计占比超过 78%，金融行业成为黑灰产最核心的攻击对象。

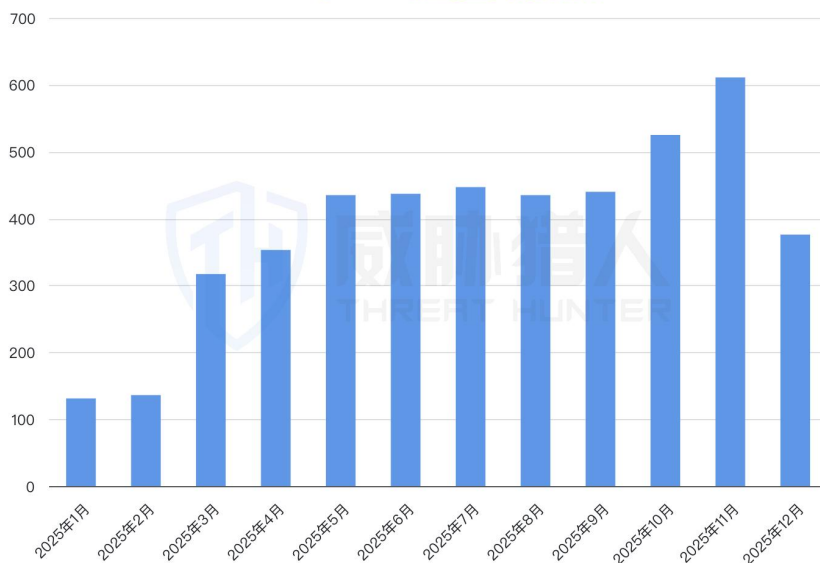
- 其中金融服务类平台被攻击的占比达 36.4%，黑产攻击此类平台主要用于跨境收款洗钱等业务；
- 虚拟货币/交易所平台、钱包/支付工具平台被攻击的占比分别 23.65%和 18.31%，黑产攻击此类平台除了用于收款外，还涉及平台的营销活动作弊，如注册批量账号，自动化撸空投奖励。

此外，内容平台和电商平台也同样成为黑产攻击的目标；前者主要涉及无人直播、水军刷量，后者则是跨境电商、无货源售货等作恶场景。

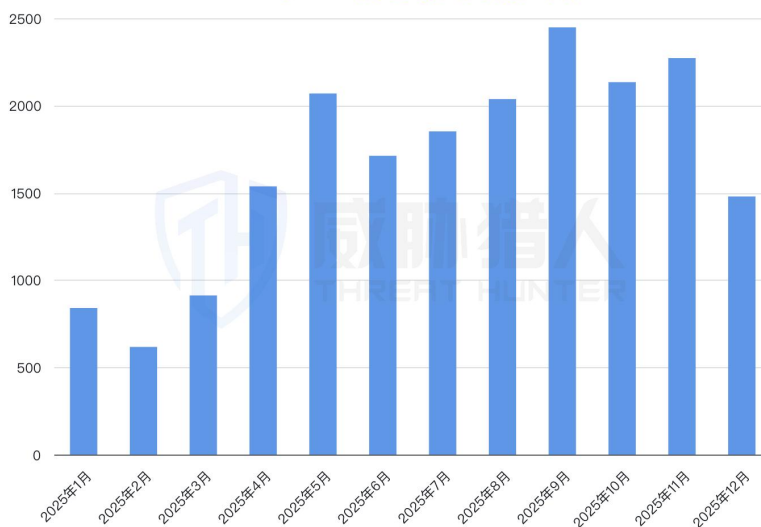
各行业 KYC 攻击情报量 TOP5 平台					
行业	平台TOP1→TOP5				
虚拟币/交易所平台	b***t	m***c	b***t	o**	b***e
金融服务平台	r***t	x*	b**a	t***c	n**
钱包/支付工具平台	w**e	s***l	p***r	p***l	n***r
内容平台	t***k	b***5	c***t	b***e	m***y
电商平台	a***n	e***y	t***u	s***y	e***o
其他平台	u***k	s***l	c***r	k***p	p***c
出行/网约车平台	u**r	g***b	b***t	k***a	g***e
OTA/旅游平台	a***b	t***r	s***g	b***w	b***m

1.2 KYC 攻击信息在暗网交流渠道上呈现上升趋势

2025年KYC攻击社交群聊数



2025与KYC作恶有关的黑产数

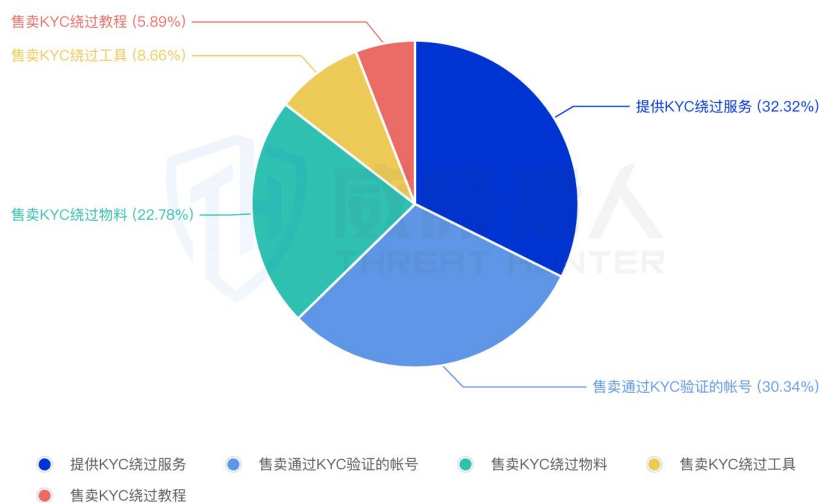


根据威胁猎人反欺诈情报平台的监测数据统计：

2025 年，KYC 攻击群聊数量及黑产数量整体呈现上升趋势，这表明越来越多的黑产参与到 KYC 攻击中，并不断的建立群聊进行攻击经验的交流、攻击服务的宣传售卖。

1.3 KYC 攻击行业高度成熟，并根据产业链层级分化出不同类型的 KYC 攻击黑产

2025 年 KYC 黑产服务类型分布



KYC 攻击行业的发展高度完善，按照攻击产业链中的层级，已分化出不同服务类型的社群聊及黑产。

- 上游：作为黑产生态的基础设施，提供绕过 KYC 验证所需的技术、物料和教程。在整体黑产类型中占比高达 37.33%，说明上游供给高度集中且规模化。
- 中游：是连接供需的关键枢纽，承担服务交付、信息共享和社区维系的作用。中游黑产提供 KYC 绕过服务典型为 B2C/C2C 服务模式，包括代做 KYC、批量注册账号、协助通过人脸识别等，具有高频率、低单价、强需求的特点，在黑产交易中数量最多（占比 32.32%），其活跃度极高。
- 下游：是黑产的最终变现环节，主要是将已完成 KYC 验证的账号出售给下游犯罪使用。其中，售卖已验证账号的黑产类型中占 30.34%，仅次于绕过服务，这表明终端账号需求旺盛，市场已趋成熟。

1.4 KYC 攻击范围广泛，欧洲、南美洲、非洲、东南亚是 KYC 攻击最活跃的四大湾区



不同地区KYC攻击情报数TOP5国家					
区域	国家TOP1→TOP5				
欧洲	波兰	西班牙	德国	英国	罗马尼亚
南美洲	墨西哥	阿根廷	哥伦比亚	秘鲁	智利
非洲	埃及	摩洛哥	肯尼亚	尼日利亚	南非
东南亚	印度尼西亚	泰国	菲律宾	马来西亚	越南
南亚	斯里兰卡	孟加拉国	印度	巴基斯坦	尼泊尔
中东	土耳其	沙特阿拉伯	约旦	阿曼	卡塔尔
北美洲	美国	加拿大	/	/	/
中亚	格鲁吉亚	亚美尼亚	哈萨克斯坦	乌兹别克斯坦	吉尔吉斯斯坦
东亚	中国	韩国	日本	蒙古	朝鲜
大洋洲	澳大利亚	新西兰	巴布亚新几内亚	萨摩亚	斐济

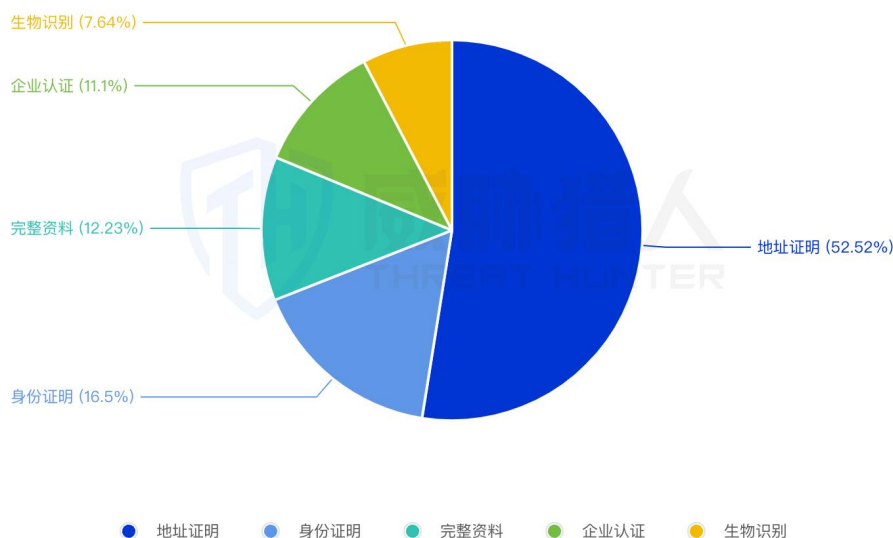
KYC 攻击呈现明显的欧美非高频、东南亚集中的特征，攻击者正高度聚焦于金融体系成熟或黑产业链条完整的地区。

根据威胁猎人反欺诈情报平台的监测数据显示：

2025 年，欧洲、南美洲、非洲、东南亚是 KYC 攻击最活跃的四大湾区（总计占比 82.93%），主要因为这几类地区金融数字化转型快、存在规模化黑产业链条且从部分公开的新闻上来看，部分地区的身份验证监管存在漏洞。

1.5 KYC 绕过物料类型中，地址证明成为黑产售卖最为频繁的 KYC 攻击物料

可售卖的KYC攻击物料类型占比



身份证明：主要包含有护照、身份证或驾照的正反面高清扫描件/照片，是个人身份材料的基本证明。

地址证明：主要包含有水电煤账单、银行流水单或税务信件，用于辅助验证用户的真实居住地。

生物识别：主要包含有手持证件照、点头/眨眼视频或 3D 人脸数据，用于突破 kyc 认证中的活体检测认证。

完整资料：主要包含有包含证件、手持自拍、地址证明甚至个人信息的整套数据包（俗称“全套/Fullz”）。

企业证明：主要包含有营业执照、税务单据、法人驾照等企业资质文件，用于通过企业账户、跨境电商店铺或对公业务的认证。

威胁猎人研究人员针对黑产售卖的 KYC 绕过物料进行分析，可以将其进一步细分为地址证明、身份证明、完整资料、企业证明、生物识别五种类型。

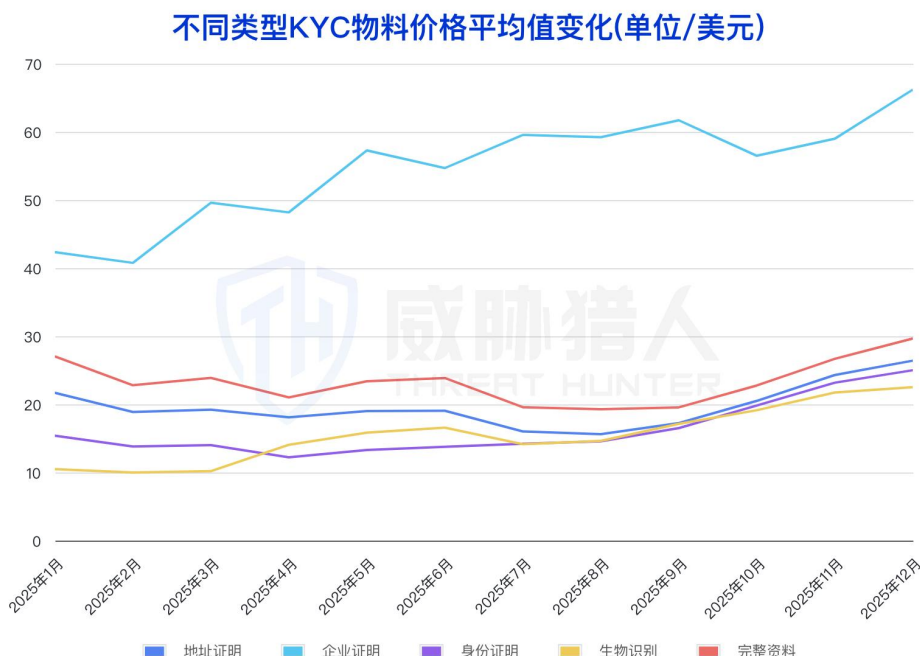
其中，“地址证明”类绕过物料的售卖最泛滥，主要原因有以下几点：

- 多数平台要求近 3 个月内的账单，而身份证长期不变，地址证明需要频繁更新、反复购买
- 地址证明多为水电账单或银行对账单的 PDF 文件或照片，模板化程度高，借助 AI 可低成本批量生成，导致市场供给过剩。

- 同时，“身份证明”类信息，作为绝大部分地区进行身份认证时所需的证明信息之一，也存在大量的售卖情况。

1.6 KYC 个人攻击物料价格平稳，但企业证明类物料上升波动最大

2025 年，KYC 攻击物料的售卖价格在呈现全面的上升趋势。



威胁猎人研究人员监测发现：

企业类证明的售卖价格最高，其主要原因为其绕过流程涉及到企业注册等相关操作，导致其绕过流程会比个人用户的 KYC 绕过更为复杂。

同时，与个人 KYC 认证相关的物料，如地址证明、身份证明、生物识别、完整资料等全年价格相对平稳，这反映了个人身份信息市场的高度饱和与工业化程度，供应源极其充足，即使在需求旺季，价格也很难产生剧烈跳动。



02

2025 年

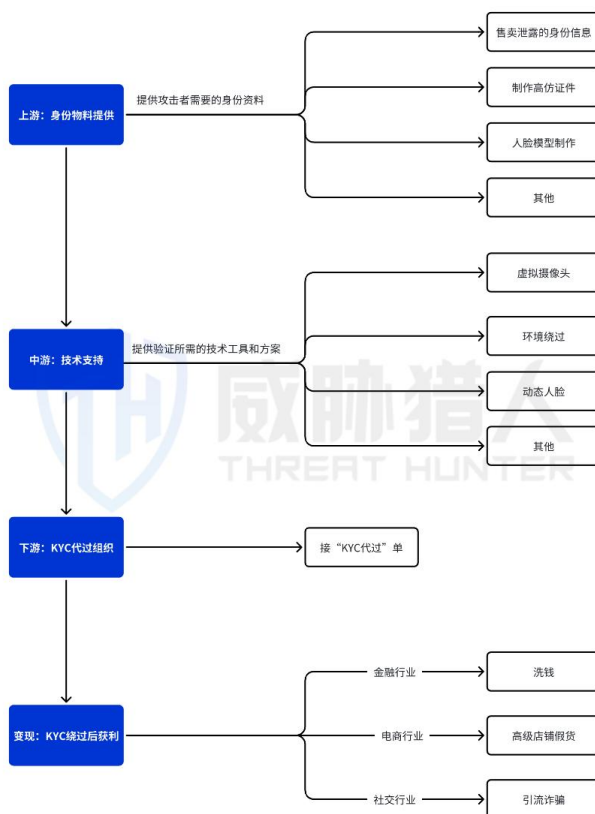
KYC 攻击产业链

二、2025 年 KYC 攻击产业链

2.1 产业链综述：从“作坊式”走向“精密工业化”

2025 年的 KYC 攻击不再是个体的单打独斗，而是一个分工严密、紧密咬合的地下产业生态。这一生态已形成标准的“产-销-用”闭环：

- **上游负责“原材料”的规模化生产（身份物料）；**
- **中游负责核心“武器”研发（绕过技术与工具）；**
- **下游负责市场化运作（代过服务）；**
- **终端则实现流量与资金的变现。** 这种链条化的运作显著降低了攻击门槛，实现了身份欺诈的规模化生产。

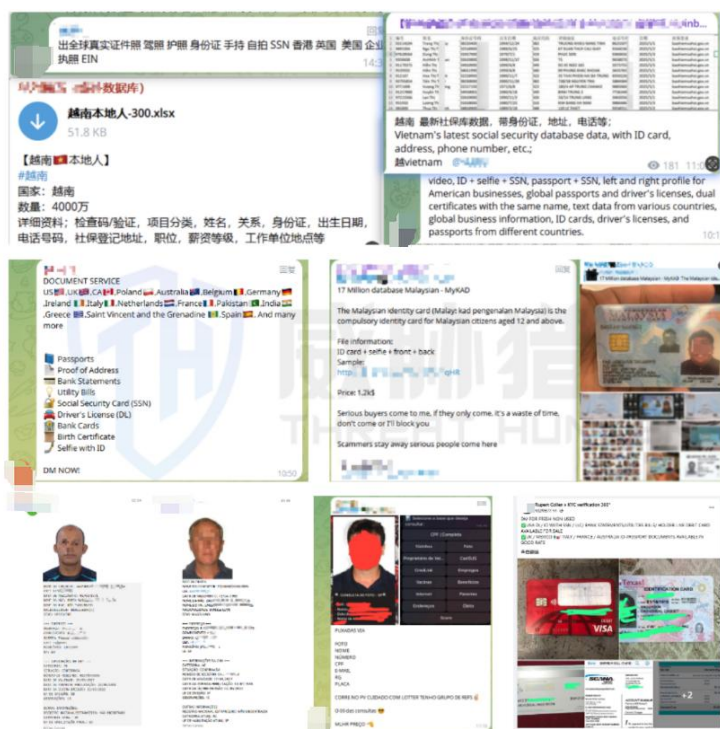


KYC 攻击产业链结构

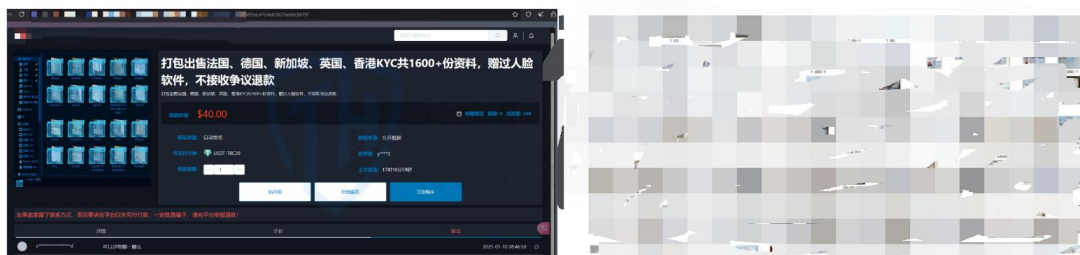
2.2、KYC 攻击上游分析：物料来源的“AI 化”与“定制化”

传统身份物料以泄露数据为主要来源，而在 2025 年，上游供应呈现出明显的“虚实结合”趋势。

1. 传统数据泄露仍是基石：暗网与黑市持续流通大量真实公民身份信息（身份证、护照、手持照），数据库入侵等数据泄露途径，仍是黑产获取底层身份物料的主要来源之一。
2. AI 生成物料成为主流：随着生成式 AI 的普及，上游开始批量提供“虚拟身份”。利用 AI 生成的虚拟人脸照片、深度伪造（Deepfake）的动态视频，甚至结合真人脸建模服务，可绕过日益严格的活体检测。
3. 证件伪造工艺精进：实体假证制作已进入“高仿”时代，黑产利用激光雕刻技术和高清打印，甚至掌握了防伪要素，能够批量生产通过 OCR 识别的伪造证件。
4. 交付标准提升：黑产将高质量的物料以“套餐”形式交付，通常包含高清证件照、配套的个人 PII 信息以及通过活体检测所需的动态视频素材。



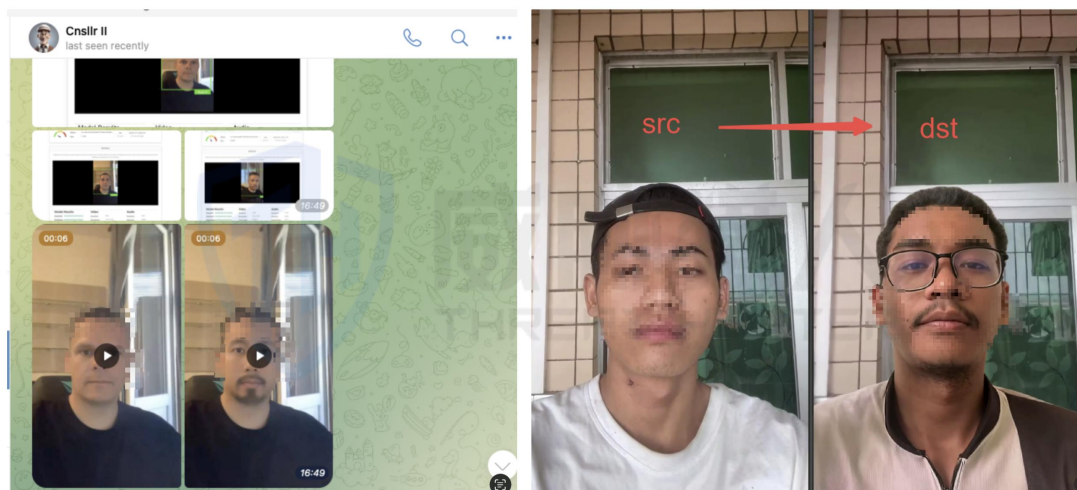
各国身份物料在 Telegram 上被售卖



暗网和交易渠道上大量的物料被售卖



黑产利用激光打印制作假证的过程



利用 AI 合成头像与视频

2.2.1 身份物料中的关键要素信息

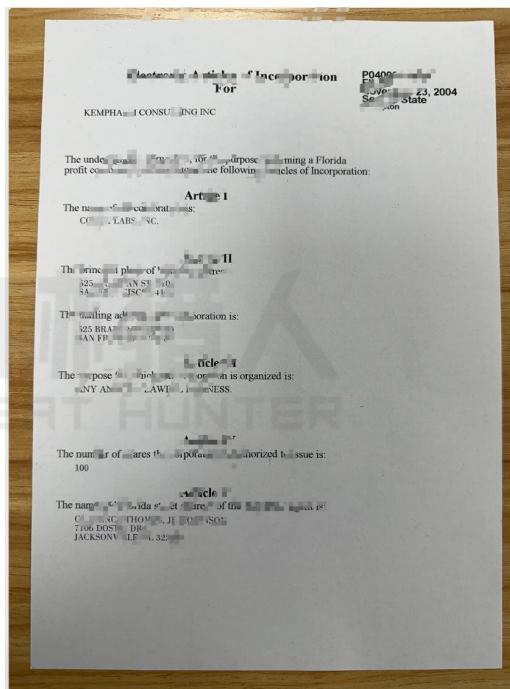
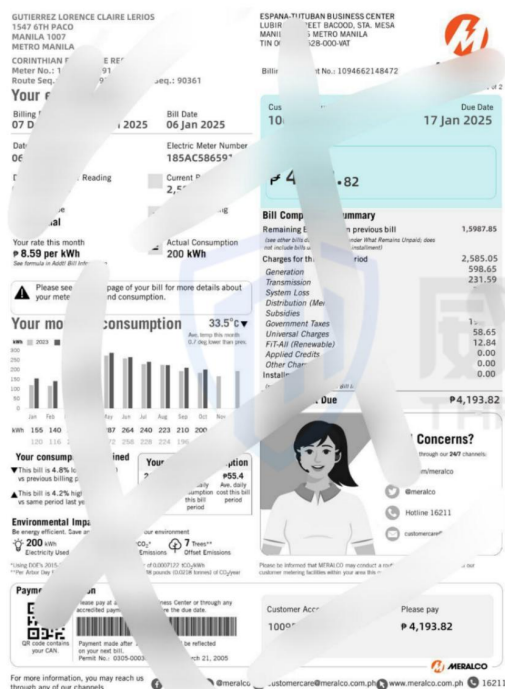
无论来源为何，上游提供的身份物料必须包含通过 KYC 所需的关键信息要素。主要包括：

- **个人身份信息：**姓名、性别、出生日期、身份证号/护照号等。这些文字信息通常需要和提交的平台表单填报一致，用于后台进行数据库校验。真实有效的身份证号（如符合校验规则、未过期）是关键要素之一。

No	ID Number	Full Name	Gender	Date of Birth	Phone	Address	Religion	Marital Status	Current Status	Remarks
145	92010100000	ABU RAHMAN	Male	1981-01-01	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
146	92010200000	ABU RAHMAN	Male	1981-01-02	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
147	92010300000	ABU RAHMAN	Male	1981-01-03	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
148	92010400000	ABU RAHMAN	Male	1981-01-04	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
149	92010500000	ABU RAHMAN	Male	1981-01-05	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
150	92010600000	ABU RAHMAN	Male	1981-01-06	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
151	92010700000	ABU RAHMAN	Male	1981-01-07	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
152	92010800000	ABU RAHMAN	Male	1981-01-08	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
153	92010900000	ABU RAHMAN	Male	1981-01-09	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
154	92011000000	ABU RAHMAN	Male	1981-01-10	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
155	92011100000	ABU RAHMAN	Male	1981-01-11	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
156	92011200000	ABU RAHMAN	Male	1981-01-12	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
157	92011300000	ABU RAHMAN	Male	1981-01-13	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
158	92011400000	ABU RAHMAN	Male	1981-01-14	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
159	92011500000	ABU RAHMAN	Male	1981-01-15	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
160	92011600000	ABU RAHMAN	Male	1981-01-16	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
161	92011700000	ABU RAHMAN	Male	1981-01-17	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
162	92011800000	ABU RAHMAN	Male	1981-01-18	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
163	92011900000	ABU RAHMAN	Male	1981-01-19	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
164	92012000000	ABU RAHMAN	Male	1981-01-20	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
165	92012100000	ABU RAHMAN	Male	1981-01-21	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
166	92012200000	ABU RAHMAN	Male	1981-01-22	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
167	92012300000	ABU RAHMAN	Male	1981-01-23	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
168	92012400000	ABU RAHMAN	Male	1981-01-24	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
169	92012500000	ABU RAHMAN	Male	1981-01-25	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
170	92012600000	ABU RAHMAN	Male	1981-01-26	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
171	92012700000	ABU RAHMAN	Male	1981-01-27	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
172	92012800000	ABU RAHMAN	Male	1981-01-28	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
173	92012900000	ABU RAHMAN	Male	1981-01-29	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
174	92013000000	ABU RAHMAN	Male	1981-01-30	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
175	92013100000	ABU RAHMAN	Male	1981-01-31	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
176	92013200000	ABU RAHMAN	Male	1981-02-01	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
177	92013300000	ABU RAHMAN	Male	1981-02-02	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
178	92013400000	ABU RAHMAN	Male	1981-02-03	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
179	92013500000	ABU RAHMAN	Male	1981-02-04	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
180	92013600000	ABU RAHMAN	Male	1981-02-05	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
181	92013700000	ABU RAHMAN	Male	1981-02-06	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
182	92013800000	ABU RAHMAN	Male	1981-02-07	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
183	92013900000	ABU RAHMAN	Male	1981-02-08	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
184	92014000000	ABU RAHMAN	Male	1981-02-09	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
185	92014100000	ABU RAHMAN	Male	1981-02-10	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
186	92014200000	ABU RAHMAN	Male	1981-02-11	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
187	92014300000	ABU RAHMAN	Male	1981-02-12	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
188	92014400000	ABU RAHMAN	Male	1981-02-13	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
189	92014500000	ABU RAHMAN	Male	1981-02-14	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
190	92014600000	ABU RAHMAN	Male	1981-02-15	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
191	92014700000	ABU RAHMAN	Male	1981-02-16	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
192	92014800000	ABU RAHMAN	Male	1981-02-17	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
193	92014900000	ABU RAHMAN	Male	1981-02-18	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
194	92015000000	ABU RAHMAN	Male	1981-02-19	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
195	92015100000	ABU RAHMAN	Male	1981-02-20	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
196	92015200000	ABU RAHMAN	Male	1981-02-21	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
197	92015300000	ABU RAHMAN	Male	1981-02-22	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
198	92015400000	ABU RAHMAN	Male	1981-02-23	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
199	92015500000	ABU RAHMAN	Male	1981-02-24	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
200	92015600000	ABU RAHMAN	Male	1981-02-25	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
201	92015700000	ABU RAHMAN	Male	1981-02-26	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
202	92015800000	ABU RAHMAN	Male	1981-02-27	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
203	92015900000	ABU RAHMAN	Male	1981-02-28	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
204	92016000000	ABU RAHMAN	Male	1981-02-29	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
205	92016100000	ABU RAHMAN	Male	1981-03-01	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
206	92016200000	ABU RAHMAN	Male	1981-03-02	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
207	92016300000	ABU RAHMAN	Male	1981-03-03	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
208	92016400000	ABU RAHMAN	Male	1981-03-04	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
209	92016500000	ABU RAHMAN	Male	1981-03-05	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
210	92016600000	ABU RAHMAN	Male	1981-03-06	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
211	92016700000	ABU RAHMAN	Male	1981-03-07	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
212	92016800000	ABU RAHMAN	Male	1981-03-08	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
213	92016900000	ABU RAHMAN	Male	1981-03-09	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
214	92017000000	ABU RAHMAN	Male	1981-03-10	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
215	92017100000	ABU RAHMAN	Male	1981-03-11	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
216	92017200000	ABU RAHMAN	Male	1981-03-12	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
217	92017300000	ABU RAHMAN	Male	1981-03-13	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
218	92017400000	ABU RAHMAN	Male	1981-03-14	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
219	92017500000	ABU RAHMAN	Male	1981-03-15	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
220	92017600000	ABU RAHMAN	Male	1981-03-16	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
221	92017700000	ABU RAHMAN	Male	1981-03-17	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
222	92017800000	ABU RAHMAN	Male	1981-03-18	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
223	92017900000	ABU RAHMAN	Male	1981-03-19	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
224	92018000000	ABU RAHMAN	Male	1981-03-20	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
225	92018100000	ABU RAHMAN	Male	1981-03-21	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
226	92018200000	ABU RAHMAN	Male	1981-03-22	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
227	92018300000	ABU RAHMAN	Male	1981-03-23	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
228	92018400000	ABU RAHMAN	Male	1981-03-24	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
229	92018500000	ABU RAHMAN	Male	1981-03-25	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
230	92018600000	ABU RAHMAN	Male	1981-03-26	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
231	92018700000	ABU RAHMAN	Male	1981-03-27	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
232	92018800000	ABU RAHMAN	Male	1981-03-28	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
233	92018900000	ABU RAHMAN	Male	1981-03-29	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
234	92019000000	ABU RAHMAN	Male	1981-03-30	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
235	92019100000	ABU RAHMAN	Male	1981-03-31	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
236	92019200000	ABU RAHMAN	Male	1981-04-01	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
237	92019300000	ABU RAHMAN	Male	1981-04-02	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
238	92019400000	ABU RAHMAN	Male	1981-04-03	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
239	92019500000	ABU RAHMAN	Male	1981-04-04	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
240	92019600000	ABU RAHMAN	Male	1981-04-05	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
241	92019700000	ABU RAHMAN	Male	1981-04-06	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
242	92019800000	ABU RAHMAN	Male	1981-04-07	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active	
243	92019900000	ABU RAHMAN	Male	1981-04-08	011-2345678	SHAH BAIT GADING CEMARA RTA BERSEKUT BERSEKUT	Islam	Married	Active</	



- **辅助证明文件（若需要）：**例如地址证明（银行账单或水电费单）、社保卡、学历证明等。这些主要在更高级别审核时用到。上游一般储备各类模板，可以伪造出带有目标姓名地址的证明文件。



在黑产交易中，一套物料的价值取决于其完整性和可信度；完整指上述要素齐备，可信度指材料看起来真实、不易被系统或人工审核识破。

上游卖家会承诺其提供的资料通过率，例如“XX 国护照+真人自拍包，通过率 90%”。为了提高可信度，黑产还会关注细节：如自拍背景、光线符合常理，证件照片 EXIF 信息真实，相同身份的各项材料信息一致匹配等等。可以说，上游物料提供者扮演着身份塑造者的角色，他们打造出的“身份”将直接决定后续攻击能否顺利；因此这一环节对产业链整体成功率至关重要。

2.3、KYC 攻击中游分析——技术支持

中游环节是 KYC 攻击的技术核心，威胁猎人发现，2025 年黑产的技术对抗集中在环境伪造与多媒体欺骗两个维度。

- **环境与设备指纹的深度伪装：** 为了对抗设备指纹与风控监测，黑产广泛使用“一键新机”工具、云手机集群以及定制化的 ROM。这些工具不仅能模拟真实的硬件参数（如陀螺仪、光线传感器），还能配合 IP 代理和 GPS 模拟，构建完美的虚拟用户环境。

- **视觉欺骗技术的迭代：**

摄像头劫持（Injection）：利用 OBS 虚拟摄像头或 HOOK 框架，拦截系统 API 调用，直接将预录制的视频流“注入”应用，绕过实时拍摄要求。

AI 深度伪造（Deepfake）：针对动态活体检测（如眨眼、张嘴、摇头），黑产利用 3D 建模和动态照片滤镜让静态照片“活”起来。更高级的服务甚至能实现实时换脸和语音克隆，通过朗读指定数字等复杂验证。

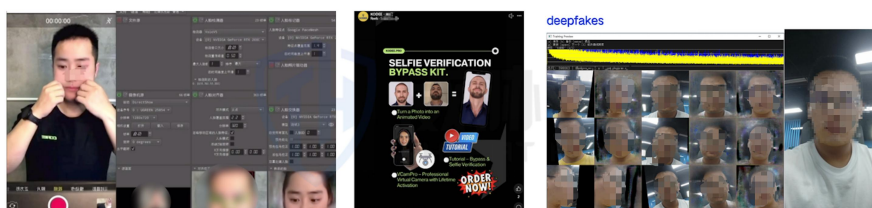
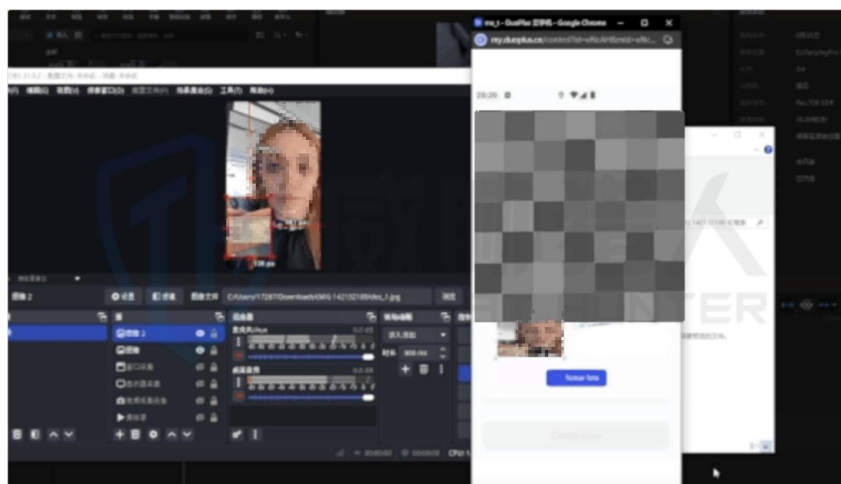
- **协议层的降维打击：** 部分高级团伙通过逆向分析应用协议，直接篡改上传数据包或跳过验证步骤，实现“一键秒过”。



"一键新机"App



地理位置伪装工具



人脸合成



2.3.1 持续对抗中的 KYC 技术演进

KYC 攻防是一个不断演进的过程。随着平台风控策略升级，黑产技术也在持续迭代。近年来可以看到以下演进趋势：

- **从静态到动态，对抗活体升级：**KYC 验证从最初的静态证照上传，逐步引入眨眼、张嘴、说数字、转头等动态活体校验；相应地，黑产也从盗用照片，演进至视频伪造、3D 人脸、动态滤

镜拍摄，直至 AI 换脸与语音合成，实现对多轮活体验证的系统性绕过。总体来看，活体攻击已由“播放素材”升级为“深度伪造动态人像”，隐蔽性和通过率持续提升。

- **环境伪装与反检测：**随着平台加强设备指纹与网络环境校验，黑产不断升级改机改环境技术，从模拟硬件 ID、传感器数据（如陀螺仪、光线感应器），到定向绕过检测 SDK 的补丁化工具，持续对抗平台规则。平台检测逻辑往往在短时间内被分析并共享，形成快速扩散的反检测能力。
- **更强的自动化与 AI 赋能：**黑产在批量注册与攻击流程中引入 OCR、生成式 AI 等自动化能力，实现验证码识别、假人脸与假证的规模化生成，效率和仿真度均显著提升。由此，身份伪造从低效的人工作坊转向高度自动化的“工业化生产”，对传统 KYC 验证机制形成系统性冲击。
- **反侦查与溯源规避：**黑产在身份欺诈过程中系统性引入去水印、去指纹特征、多跳代理与防追踪沙箱等手段，刻意弱化平台对设备、网络与内容指纹的采集能力；部分团伙甚至采用“一机一号、一次一用”的隔离方案，最大限度降低账号关联风险。这些反溯源策略显著抬高了平台风控与执法追查成本，使攻击行为更加隐蔽、难以回溯。

总体而言，平台每一次风控升级，都会迅速被黑产研究并找出对策，这种持续对抗导致部分场景下的 KYC 审核机制逐渐失效，尤其是纯线上远程验证，已在深度伪造技术面前逐步失守。



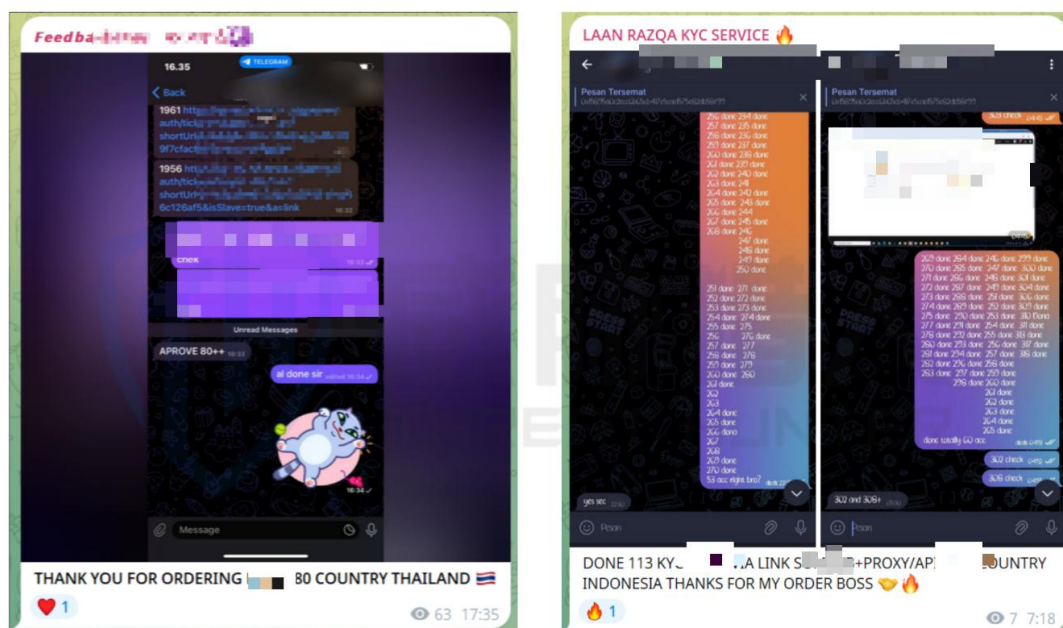
KYC 对抗中的技术演进

对企业而言，依赖“一次性校验”的信任模式亟需转型；而生成式 AI 与智能体技术的爆发不仅为业务创新带来了机遇，也为黑灰产提供了低门槛、高效率的自动化作恶工具以及规模效应。可以预见，未来身份欺诈的对抗强度与专业化水平仍将持续上行。

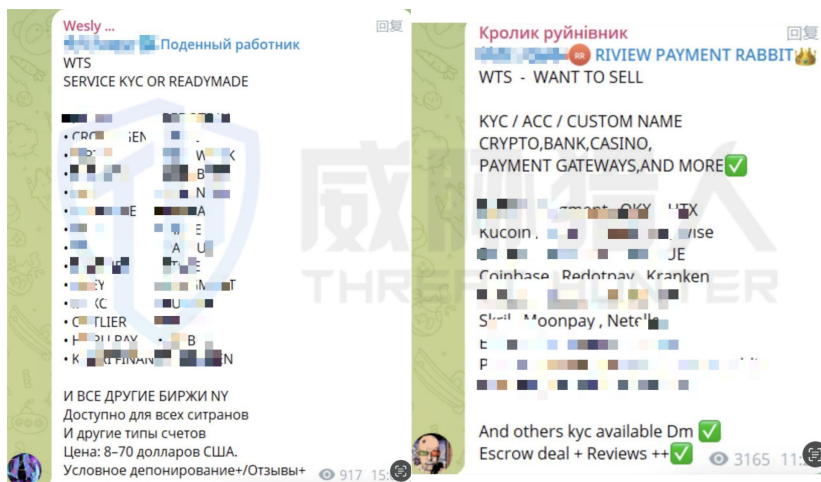
2.4、KYC 攻击下游分析——KYC 代过组织“SaaS 化”运作

下游的 KYC 代过组织已演变为成熟的服务提供商，其运作模式具备典型的商业特征。

- **公开的市场营销：**代过组织活跃于 Telegram、社群甚至公开网络，他们明码标价，根据平台难度和地区差异制定详细的价目表。
- **服务承诺与售后：**为了争夺客户，黑产团伙推出了“包过”、“不过退款”以及“售后质保”服务（如账号被封免费重做），极大地降低了买家的心理门槛。
- **混合运作模式：**除了纯技术绕过，下游组织还会通过招募“真人”（如利用廉价劳动力）配合技术手段来完成高难度的 KYC 验证。



KYC 代过组织，在 Telegram 上发布广告



KYC 代过组织，提供的代过服务很丰富

2.4.1 KYC 代过组织的典型特征

KYC 代过组织作为黑灰产业链条的中坚力量，有以下典型特征：

- **明码标价，业务清单明确：**他们通常针对不同平台、不同验证难度制定价格，价格会随市场供需浮动，但整体公开透明，给人一种“正规服务”的错觉。一些组织还列出自己擅长的平台列表和成功率，吸引客户。



代过组织对每平台都明码标价

内分工专业：一个成熟的代过团队内部通常分工明确，如由技术手执行具体的工具操作，“料子手”准备所需身份料，上线对接客户谈价收款，下线专职寻找最新教程工具等。这样流水线协作提高了效率和成功率。

承诺包过和售后：为了竞争，代过组织往往承诺高成功率，甚至“不过退钱”或免费重做。这种承诺一方面表示其技术自信，另一方面也吸引更多客户尝试。此外，他们有时提供售后服务，比如账号通过后若短期内被风控清退，可免费再次代办。这些策略本质是在打造信誉，形成黑市中的“品牌”，以便长期经营。

隐蔽的交易和支付：尽管公开招揽，这些组织在实际交易时相当谨慎。通常通过 1V1 聊天确认细节，支付手段采用数字货币（USDT 等）或等值卡密，以避免资金链暴露。有的中介会使用“担保人”机制确保交易安全。总之，他们尽量降低自身被执法打击的风险。

使用各种方式绕过，甚至招募真人进行绕过：除了使用技术手段绕过外，很多代过组织，还会使用招募真人的形式——用少量价格去招募真人提供资料，人们为了小利出卖身份，帮助代过组织绕过 KYC 验证。

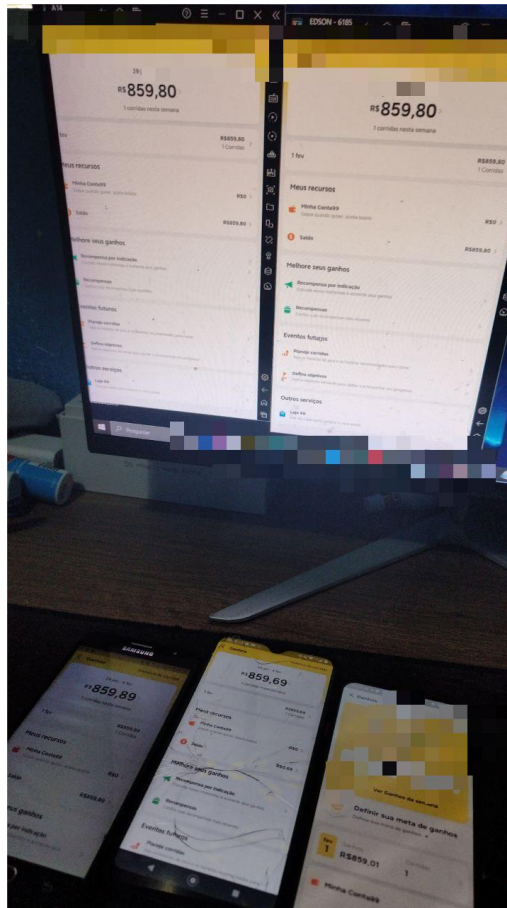


黑产招募真人，并使用统一使用谷歌表格填写材料

2.5、KYC 攻击变现环节分析——获利手段

通过 KYC 验证后的账号被视为“可信身份”，是黑产变现的根本前提。2025 年的变现路径主要集中在：

- **金融清洗：**利用实名账户进行洗钱、“跑分”以及加密货币的跨境转移。
- **电商与营销欺诈：**批量注册实名买家号骗取平台补贴，或注册虚假商家店铺进行诈骗和售假。
- **信用与资源滥用：**在出行、社交等领域，利用假身份进行非法运营、引流诈骗或信用借贷。



绕过 KYC 后获利



03

2025 年

KYC 典型攻击案例

三、2025 年 KYC 典型攻击案例

3.1 2025 年 KYC 产业攻击链结构

从“单点突破”到“全栈自动化”：AI 与物理外挂重构攻击成本曲线

2025 年的 KYC 攻击不再局限于单一的技术绕过，而是形成了一条“物料生成—环境伪装—视觉注入—逻辑对抗—变现收割”的标准化工业闭环。

- **攻击门槛显著降低：** 随着“一键式 AI 换脸”与“定制化云手机”的普及，高精度的身份伪造已从实验室技术下沉为廉价的黑产工具。
- **防御边界被物理穿透：** 攻击手法已从纯软件注入（如 ROM 定制）向“软硬结合”演进，偏振镜消光等物理手段的出现，标志着单纯依赖屏幕反光等被动活体检测技术面临失效风险。
- **业务风险传导加速：** 攻击链的标准化使得从“伪造身份”到“信贷/电商套现”的周期大幅缩短，黑产对风控规则的测试与迭代速度已达到小时级。

业务链路	攻击策略			具体案例
身份资料伪造	①、虚假身份生成	②、证件租借	③、AI合成照片	1、虚假物料准备 
	④、AI生成视频	⑤、非本人手机号		
设备指纹绕过	①、云手机	②、Xposed框架	③、magisk框架	2、设备物料准备  
	④、指纹伪造	⑤、环境模拟器		
视频注入	①、相机劫持	②、屏幕攻击	③、虚拟摄像头	3、视频注入  
	④、云机相机劫持			
人脸活化伪造	①、DeepFace	②、照片活化	③、动作迁移	4、人脸活化伪造  
	④、表情复制			
贷款套现	①、套现跳板账号	②、养号提额循环套取		5、贷款套现 

3.2 2025 年 KYC 产业链新型手法

2025 年，KYC 对抗已突破单一维度的软件攻防。黑产通过引入物理光学设备（如偏振镜）与深度逆向逻辑（如三色劫持），实现了对传统视觉风控的“降维打击”。同时，傻瓜式 AI 工具的泛滥，使得高阶攻击成本被极度摊薄。

3.2.1 视觉对抗层：物理与光学的“降维打击”

【核心变化】 从“软件修图”升级为“光学欺骗”，物理外挂直接无效化被动活体检测。

物理消光手段： 针对平台依赖的“屏幕反光”等活体特征，黑产引入偏振镜等物理设备消除屏幕反射光，从光学物理层面绕过检测逻辑。

高清重构技术： 利用高分辨率屏幕配合 AI 后处理技术（去噪、校色、抖动模拟），让“怼屏”攻击画面在细节和纹理上无限接近真实拍摄，导致纯视觉算法难以区分电子屏与真人脸。

3.2.2 注入攻击层：逻辑漏洞的“精准逆向”

【核心变化】 从“暴力注入”升级为“交互逻辑欺骗”，深度利用特定算法的校验机制。

深度逆向交互： 黑产已不再满足于简单的视频流替换，而是深度逆向了活体检测的交互逻辑（例如颜色校验机制）。

定制化工具涌现： 典型如“三色相机劫持”工具，能够根据 APP 指令精准反馈特定的颜色或光线变化，实现了针对特定算法逻辑的精准欺骗，证明黑产对风控代码的理解已达代码级。

3.2.3 基础资源层：高阶技术的“傻瓜式操作”

【核心变化】 从“技术极客专用”下沉为“人人可用的黑产基建”。

极致易用性： 10 月份出现的“一键式 AI 换脸工具”，成功将复杂的 Deepfake 技术封装为“上传即生成”的傻瓜式操作。

攻击规模化： 极低的使用门槛导致部分大型平台面临规模化攻击风险。攻击成本的极度摊薄，意味着防御方将面临海量、低成本、高并发的身份欺诈挑战。

黑产攻击层	最新的攻击手法/工具
	更新时间等信息
视觉对抗层	偏振镜在怼屏上的应用： 发布时间：2025-6月份 攻击方式：通过将手机摄像头夹带偏振镜的方式，可以在活体检测时消除大部分的屏幕反光，通过此来进行活体检测绕过。怼屏：2025年8月AI换脸+高分辨率屏幕和后处理技术（去噪、校色、抖动模拟等）让怼屏画面更像真实拍摄
注入攻击层	具备三色的相机劫持工具： 发布时间：2025-7月份 攻击方式：通过选取屏幕坐标选取色彩的位置，然后在进行活体检测时，应用会根据选取到的色彩颜色，将YUV帧图像的中间位置渲染一个圆圈然后转换为RGB色彩空间。
环境伪造层	改机 + 环境备份一体化工具： 发布时间：持续被黑产利用 攻击方式：通过应用通过root权限修改底层设备参数，结合一键环境备份，使用单一设备多账号功能，因工具本身特定，具备多功能实现，所以被黑产长期利用投入攻击当中。
基础资源层	一键式AI换脸工具提供核心物料： 发布时间：2025-10月份 攻击方式：该软件操作极为简便——用户仅需上传目标人脸图片与目标动作视频，便可一键生成换脸视频。该工具可与虚拟摄像头（虚拟视频相机）配合使用，已在大陆对多家大型平台实施攻击并宣称获得成功。

3.3 KYC 攻击在电商行业的典型案例

【案例复盘】

攻击目标：某头部电商平台的“先用后付”信用额度及高价值商品。**核心手法：**利用“四件套”身份物料结合云手机环境伪装，批量注册“白户”账号。通过注入攻击绕过人脸识别，获取平台高额信用授信（如分期付款、消费贷），最终通过购买易变现商品（如黄金、电子产品）或直接提现实施诈骗，形成一条完整的“骗贷/骗物”黑产业链。

现代电商 KYC 攻击已不再是单点的账号注册，而是一条严密的工业流水线。从物料准备到最终变现，攻击流程如下：

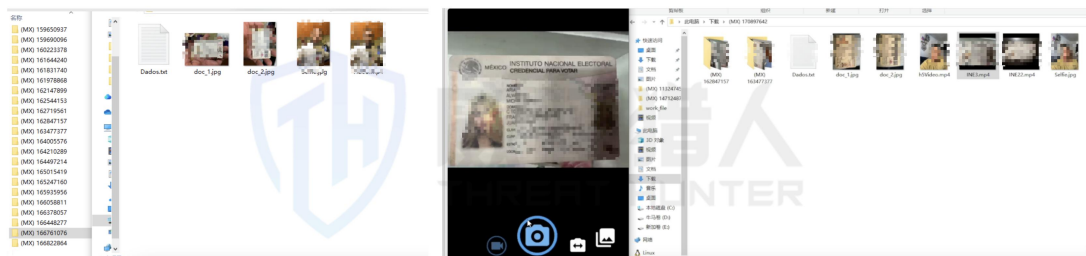


KYC 攻击的典型流程

3.3.1 第一阶段：虚假身份的“工业化组装”

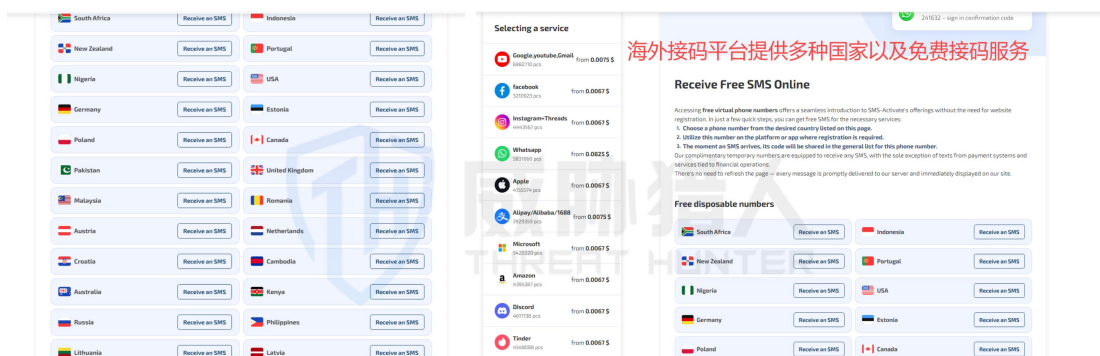
攻击的起点在于构建一个在数字世界中看起来“真实存在”的人。电商风控通常会校验身份信息与手机号、IP 归属地的一致性，因此黑产需要准备全套匹配的物料。

- **身份物料：** 攻击者从上游黑市购买包含身份证正反面、手持照以及高清人脸视频的“料子”。为了提高通过率，这些资料往往经过筛选，确保证件无遮挡、视频符合活体要求。



身份物料准备和测试

- **通信资源：** 利用接码平台批量获取非实名手机号（或黑卡），用于接收注册短信验证码。这些号码通常是攻击链中的“日抛型”耗材。



准备注册所需的手机号

3.3.2 第二阶段：设备指纹与环境的“深伪装”

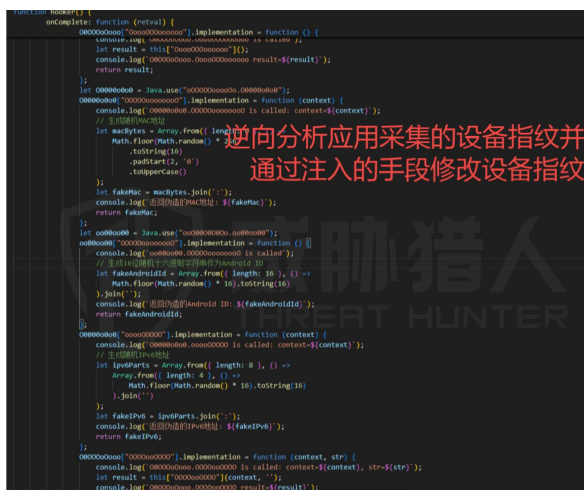
为了绕过电商平台严苛的风控，攻击者必须解决“设备指纹”和“地理位置”的合规性问题。

- **网络与地理位置仿真：** 攻击者会将 IP 地址和 GPS 定位修改为与身份物料（身份证归属地）一致的城市，以欺骗风控模型认为这是“本地人在本地操作”。



准备绕过 KYC 所需的环境

- **设备指纹对抗：** 利用 Xposed/Magisk 框架逆向修改手机底层参数（IMEI、MAC 地址、电量、传感器数据等），使每一台云手机在平台眼中都是一台全新的、无历史污点的真实移动设备。



逆向并修改设备指纹

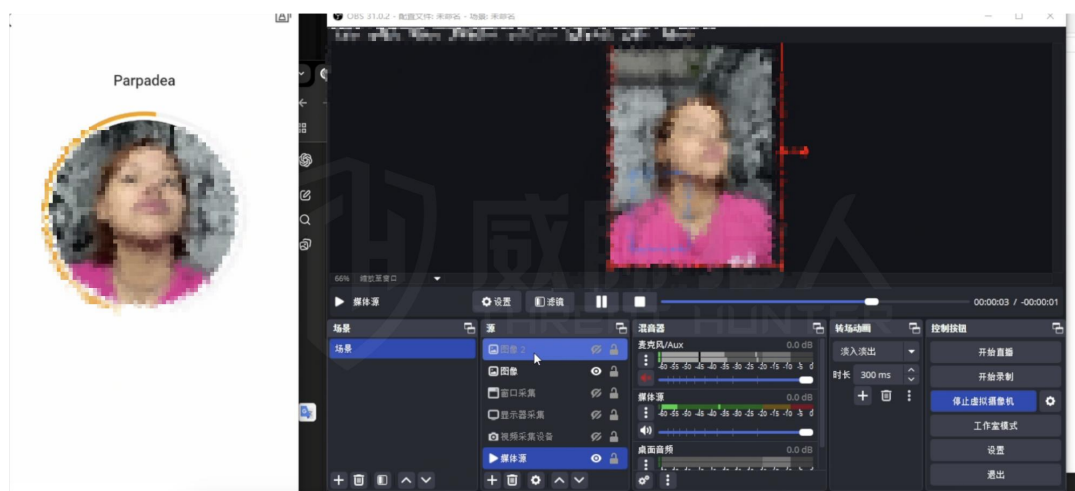


仿真地理位置

3.3.3 第三阶段：视觉注入与 KYC 实战突围

这是攻击链中最关键的“闯关”环节。当电商平台触发“实人认证”或“开通支付信用”的核身请求时，攻击者启动攻击脚本。

- **视频流劫持：** 攻击者并不拍摄真实画面，而是通过 HOOK 技术劫持摄像头的系统调用接口。
- **动态调整：** 将本地准备好的高清动态人脸视频（对应第一阶段物料）直接“注入”到 APP 的采集窗口。攻击者甚至会根据 APP 反馈（如光线不足、角度不对）实时调整注入视频的参数，直到骗过活体检测算法。

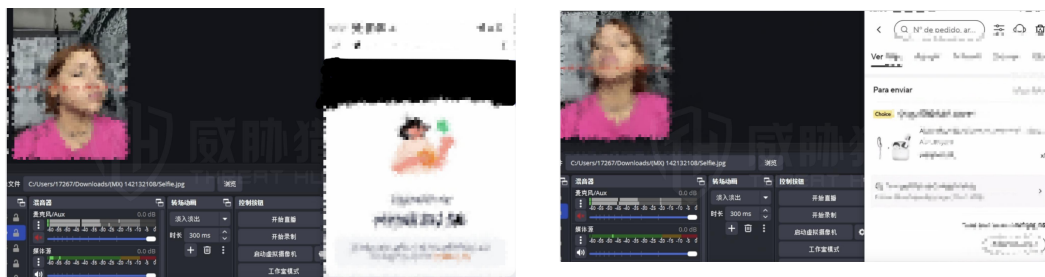


触发验证 KYC，并加载本地准备好的资料

3.3.4 第四阶段：信用变现与资产收割

一旦 KYC 验证通过，该账号在平台眼中即变为“高信用实名用户”。攻击者随即进入收割阶段，此阶段速度极快，通常在数小时内完成。

- **信用套现：** 立即激活平台的消费信贷服务（如 XX 付、XX 白条），获取数千至数万元不等的信用额度。
- **物资转移：** 利用额度购买手机、黄金等硬通货，收货后销赃；或者直接申请现金贷款转出。由于账号信息均为伪造或冒用，平台产生坏账后无法追溯到攻击者本人。



绕过 KYC 后，获取消费信贷额度

3.4 KYC 攻击在金融/信贷行业的典型案例

【案例复盘】

攻击目标： 互联网金融平台的信贷额度（如现金贷）。 **核心手法：** 不同于纯机刷，金融场景常采用“真人众包 + 技术辅助”模式。黑产中介招募信用良好的“白户”或利用泄露的真实身份，通过位置篡改和流水伪造包装出高信用资质，利用人脸注入通过审核后，批量申请贷款并“断供”跑路，形成坏账。



信贷场景下的 KYC 攻击与套现链路

3.4.1 第一阶段：精准选料与“信用包装”

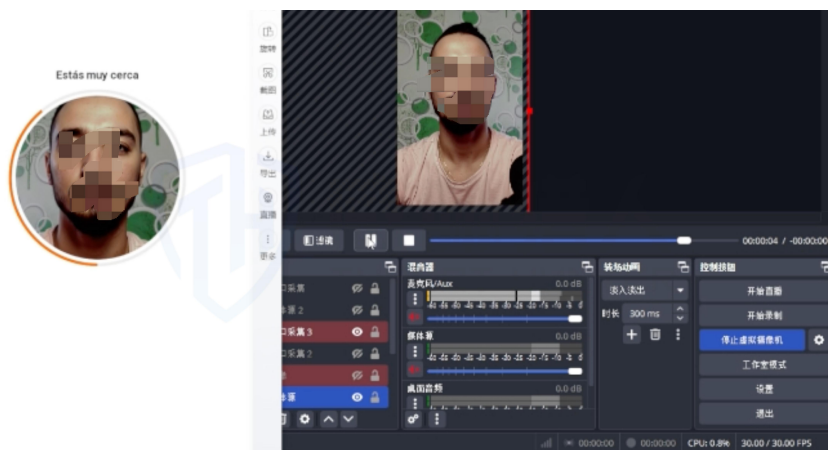
金融风控强依赖征信基础，纯虚假身份难以获取高额贷；因此，攻击者建立了一套成熟的真人身份分销体系。

- **身份中介与佣金结算：** 不同于简单的诱骗，这是一个有着明确价格标准的交易市场。中介作为连接上游与下游的枢纽，向上游寻找愿意出售身份的真实用户（俗称“肉身”），向下游攻击团队接单。

3.4.3 第三阶段：高对抗下的“视频伪造”

金融类 APP 的活体检测最为严格（通常包含动作交互或读数）。

- AI 深度伪造 (Deepfake)：针对金融 APP 中高频出现的动作活体检测（如“请眨眼”、“请张嘴”、“向左/右转头”），攻击者利用 AI 驱动技术让静态照片“活化”。通过动作迁移算法，攻击者可以操控静态人脸精准完成系统指定的连续动作，并将合成的动态视频流实时注入 APP，从而骗过活体防伪检测。

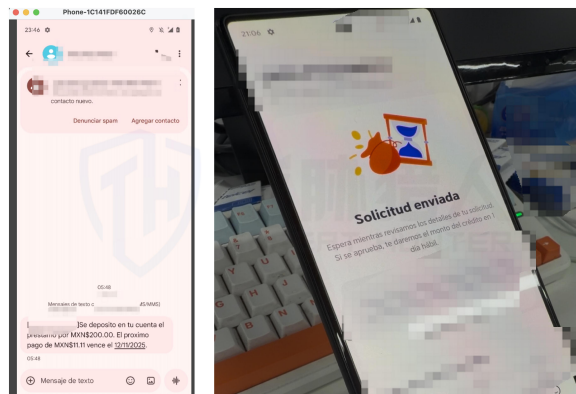


AI 生成的眨眼、转头等动态验证视频

3.4.4 第四阶段：资金“清洗”与坏账形成

批量提现：授信通过后，黑产迅速将贷款转出至二级洗钱账户（跑分平台）。

账号废弃：提现完成后，该账号即被抛弃，导致平台产生无法追回的坏账。



授信完成后进行贷款以及拨款成功相关截图

3.5 KYC 攻击在虚拟币交易所行业的典型案例

【案例复盘】

攻击目标： 全球头部加密货币交易所的实名账户

核心手法： 交易所已成为身份欺诈的“重灾区”。攻击者不再单纯依赖 P 图，而是大量采购“真人全套物料”（证件正反面+手持照+预录制人脸视频）。通过摄像头劫持技术，将预录制好的真人视频直接注入 APP 完成活体检测。

黑产动机： 极高的 ROI（投资回报率）是驱动攻击的根本动力。一套低成本的物料经加工为“成品号”后，价格翻涨数倍；若用于空投或洗钱，其潜在收益更是高达百倍千倍。

从“料子”到“成品”，再到“暴利”，形成了一条标准化的资产增值链路。



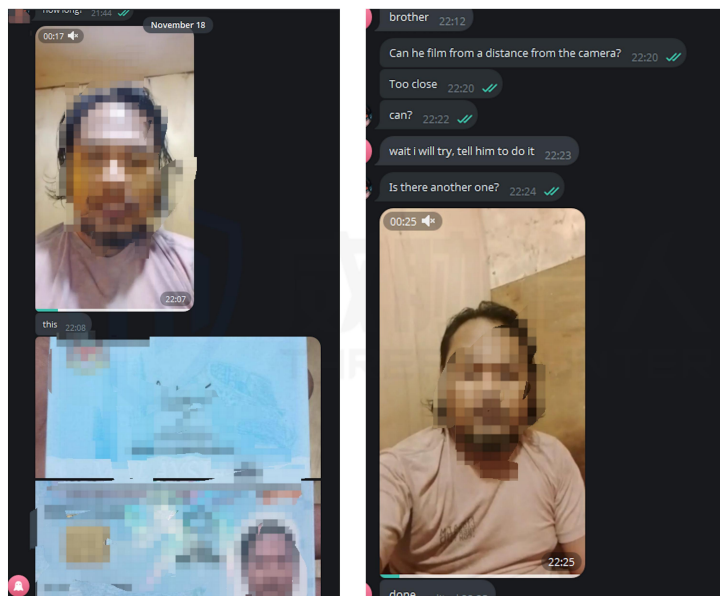
交易所 KYC 攻击与套现链路

3.5.1 第一阶段：供应链源头——“真人全套”物料

不同于 AI 生成的虚拟人脸，交易所攻击更倾向于使用真实存在的身份，以应对严格的证件 OCR 和背景调查。

- **物料分级售卖：** 黑市中有着明确的售卖标准。对于交易所攻击，最抢手的是“大满贯”料子：
- **基础版：** 身份证/护照正反面照片。
- **进阶版：** 基础版 + 手持证件自拍。
- **豪华版（攻击专用）：** 进阶版 + 预录制人脸视频。

注：这些视频通常由真人配合录制，包含点头、眨眼等基础动作，专门用于过活体验证。

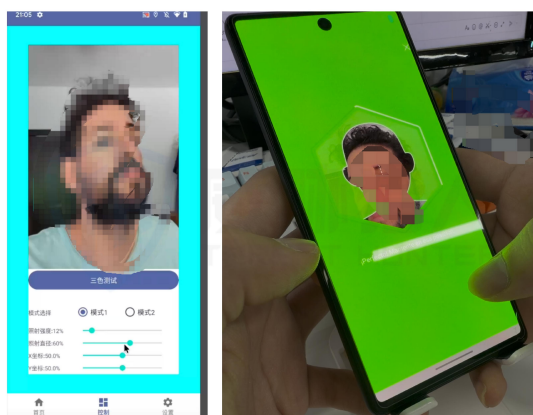


Telegram 上售卖的“证件+视频”全套真人料子

3.5.2 第二阶段：中间加工——视频注入与环境伪装

拿到料子后，黑产技术团队负责将其“加工”为通过验证的账号。

- **预录制视频注入：** 当交易所 APP 要求进行活体检测时，攻击者不使用摄像头拍摄，而是使用 HOOK 工具或虚拟摄像头软件，将准备好的“预录制真人视频”直接注入到数据流中。由于视频本身是真人拍摄的，且包含真实的生物特征，这种方式能极高概率绕过非交互式的活体检测。
- **环境对齐：** 配合住宅代理 IP，模拟用户身处证件所属国家，完成设备指纹的合规化包装。



利用虚拟摄像头注入本地预录视频

3.5.3 第三阶段：价值兑现——黑产“高 ROI 生意”

模式 A：成品号售卖 (Account Flipping)

投入： 购买一套东南亚/拉美真人资料（含视频）成本约 \$1 - \$5。

产出： 通过 KYC Level 2/3 的高级认证账号，黑市售价可达 \$20 - \$100+。

ROI： 纯利 300% - 900%。黑产仅需简单的流水线操作即可实现资产翻倍。

模式 B：空投女巫攻击

空投：在加密货币和区块链项目中，空投指项目方为了推广新币，会免费发放代币给用户。

女巫攻击：在计算机安全领域，指攻击者通过制造大量虚假身份（账号或节点）来操控网络或系统。

投入： 批量注册 100 个账户，总成本约 \$1,50。

产出： 若某个新币项目发放空投，单号收益可能达到 \$500 - \$2,000，总收益可达 \$50,000+。

ROI： 5000%+；这种博彩式的收益诱惑，促使黑产动用数万个真人身份进行“饱和式攻击”。

模式 C：洗钱通道

价值： 对于电诈或网赌团伙，一个安全的大额提币账户是“刚需”，其实际价值远超账号本身价格，是资金转移链路上不可或缺的耗材。





04

结语

四、结语

KYC 身份认证的攻防，已从单一的技术对抗演变为高度成熟的产业链博弈。尽管风控围栏日益收紧，但在极高投产比的诱惑下，黑产技术的迭代速度远超预期，身份信任体系的防护注定是一场持久战。

威胁猎人建议：

1、构建持续监测的身份风控体系

KYC 不应止于一次性校验，而需覆盖账号全生命周期。在高风险操作或关键节点触发二次核验，并持续监测账号行为与环境变化，及时识别异常交易、异地登录及批量账号特征，防止风险长期潜伏。

2、升级 KYC 核验与反欺骗能力

引入多要素联合验证机制，融合证件核验、活体检测、设备指纹、地理位置与权威数据校验，并重点部署深度伪造检测能力，对抗 AI 换脸与视频注入等新型攻击。

3、协同封堵上游资源与攻击扩散

通过接入权威数据源降低伪造资料通过率，并推动监管与行业协同，打击身份数据黑市与制假链条，建立风险线索共享机制，防止虚假身份跨平台重复利用。

4、建立常态化的红蓝攻防演练机制

定期进行红蓝攻防测试，以攻击者视角对业务全链路进行“实战模拟”。通过模拟相机劫持、注入攻击及黑产链路渗透，主动发现现有风控体系中的盲区与漏洞，化“被动防御”为“主动迭代”，在真实攻击发生前完成加固。

作为长期关注黑灰产情报的研究团队，我们深入暗网一线，持续解构攻击手法、还原产业链路，为行业提供真实的风险视角。我们深知，唯有保持敏锐的洞察与持续的跟踪，才能在 AI 时代的身份博弈中掌握主动。

威胁猎人 KYC 红队服务依托专业的风险情报收集与分析能力，覆盖 Telegram、暗网、论坛等多元渠道，确保及时获取并深度解析 KYC 相关欺诈线索、IOC 和风险特征。

通过这些情报洞察黑产的最新手法和产业链动态，我们将情报转化为实战武器，定期进行红蓝攻防测试，模拟真实攻击链路对业务进行深度体检，实现对 KYC 攻击行为的早期预警，帮助企业在欺诈发生前或初期采取有效措施，避免或减少损失。

说明：本报告所提供的数据信息系威胁猎人依据大样本数据抽样采集、小样本调研、外部情报数据采集、数据模型预测及其他研究方法估算、分析得出，由于统计分析领域中的任何数据来源和技术方法均存在局限性，依据上述方法所估算、分析得出的数据信息仅供参考。



以情报构筑数字化安全基石



扫码关注
获取行业最新反欺诈报告

☎ 服务热线：400-809-3699

🌐 官方网址：www.threathunter.cn

✉ 联系邮箱：marketing@threathunter.cn

📍 总部地址：广东省深圳市南山区粤海街道科技园社区科苑路15号科兴科学园B2栋1705