THREAT HUNTER RESEARCH

2025 Global KYC Attack Risk Report

A global review of identity and document abuse, automated attack tools and services designed to bypass KYC controls.

Original publication: 2026-02-05
Research team: Threat Hunter Research Team
Source report: 43 pages

Original report text

This text version is reconstructed based on the 43-page original PDF, retaining the report narrative, chapters and research scope; the cover, repeated table of contents and purely decorative pages are not repeated. Localized figures are placed in context throughout this web edition, with the original PDF retained for reference.

About Threat Hunter

Threat Hunter was founded in 2017 and helps organizations identify and respond to business fraud, external digital risk, and API security threats. Its work combines cybercrime intelligence, risk data, product platforms, and specialist services.

The company provides mature and diverse products and services focusing on risk scenarios such as business fraud, data leakage, phishing and counterfeiting, and API attacks that different industries face in the process of digital development. It has been selected as a representative vendor in Gartner's technology maturity curve report and IDC's threat intelligence field for many times.

Headquartered in Shenzhen, Threat Hunter also operates offices in Beijing, Shanghai, and Chongqing, with Digital Risk Response Centers in Shenzhen and Chongqing. The company supports customers in China, Europe, the United States, South America, and Southeast Asia.

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。

Original report charts, processes and cases

Source: Threat Hunter original report, page 2

Preface

With the full spread of digital business, KYC (Know Your Customer, identity authentication) has become the most critical starting point for trust in finance, virtual assets, e-commerce and platform-based businesses, and is also the "first gate" of the fraud-control system.

However, in recent years, cybercriminal groups have continued to integrate data leakage, forged documents, AI face-changing and other means, forming a highly mature attack chain around the KYC authentication process. From the production of identity materials, technical bypass services, to finished product account transactions and fund realization, KYC attacks are no longer scattered individual behaviors, but a fraud network with large-scale supply, standardized processes and high ROI.

Based on global cybercrime intelligence monitoring data, Threat Hunter will systematically restore the overall risk landscape of KYC attacks in 2025 from multiple dimensions such as attack target industry distribution, darknet and community activity, industry chain division of labor, regional risks, and core bypass materials, and reveal the real pressure and structural challenges faced by the current identity authentication system.

KYC attack risk landscape in 2025

1. KYC attack landscape in 2025

1.1 KYC attacks are concentrated in financial services

In 2025, KYC attacks are concentrated in a small number of industries, with financial services, virtual currencies/exchanges, and wallets and payment tool platforms accounting for more than 78%. The financial industry has become the core attack target of the cybercrime ecosystem.

- Among them, financial services platforms accounted for 36.4% of attacks. threat actors target these platforms mainly for cross-border collection and money laundering;
- The proportions of attacks on virtual currency/exchange platforms and wallet/payment tool platforms were 23.65% and 18.31% respectively. In addition to collecting payments, threat actors target these platforms and exploit their marketing activities, such as registering batch accounts and automating airdrop rewards.

In addition, content platforms and e-commerce platforms have also become targets of attacks by threat actors; the former mainly involves unmanned live broadcasts and trolls to increase sales, while the latter involves cross-border e-commerce, unsourced sales and other malicious activity scenarios.

1.2 KYC attack services are increasingly advertised through dark-web channels

KYC Target Industry Distribution

Source: Threat Hunter original report, page 6

According to monitoring data statistics from the Threat Hunter anti-fraud intelligence platform:

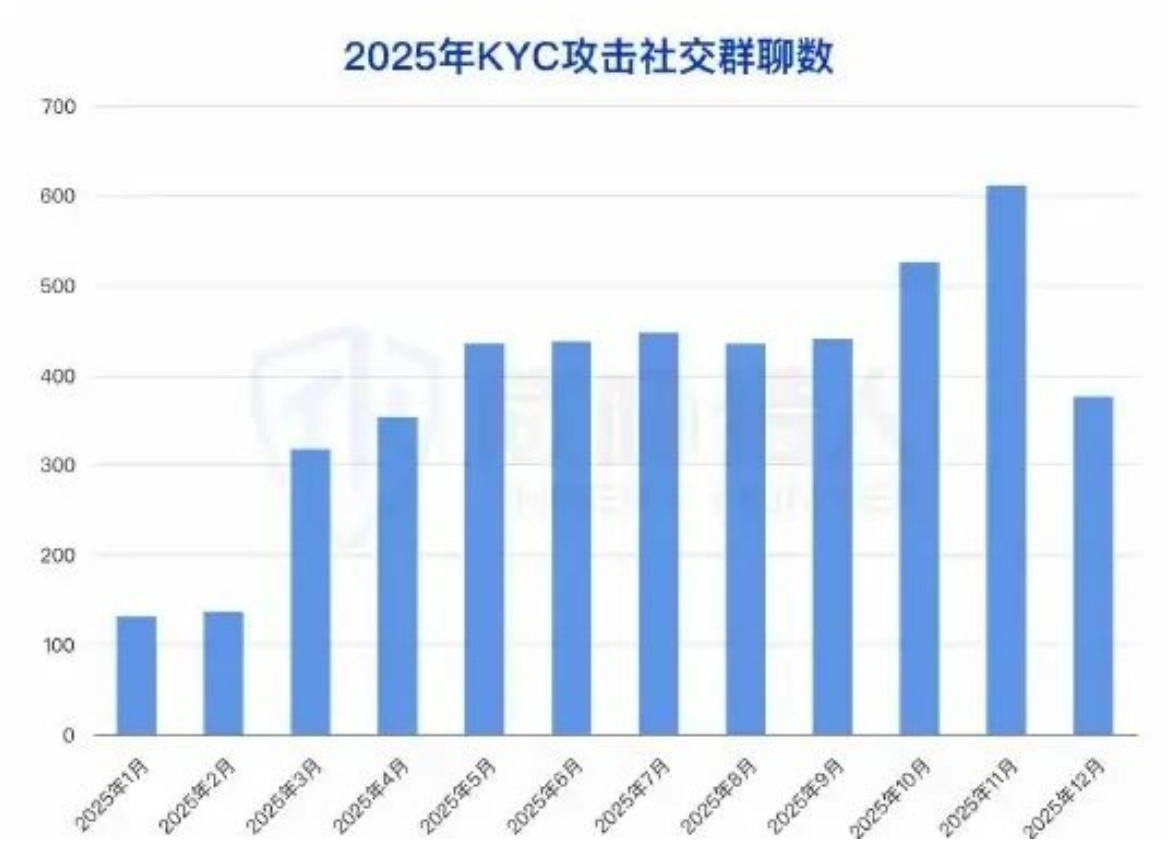
In 2025, the number of KYC attack group chats and the number of threat actors showed an overall upward trend, which shows that more and more threat actors are participating in KYC attacks and are constantly establishing group chats to exchange attack experiences and promote and sell attack services.

1.3 A mature KYC-bypass supply chain has distinct specialist roles

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

KYC attack information shows an upward trend in dark web communication channels (Chart 1)

Source: Threat Hunter original report, page 7



KYC attack information shows an upward trend in dark web channels of communication (Chart 2)

Source: Threat Hunter original report, page 7

The KYC-bypass market is highly developed, with distinct communities and service providers operating at each layer of the supply chain.

- Upstream: As the infrastructure of the threat actors ecosystem, it provides the technology, materials and tutorials required to bypass KYC verification. The proportion of the overall threat actors type is as high as 37.33%, indicating that the upstream supply is highly concentrated and large-scale.
- Midstream: It is the key hub connecting supply and demand, and plays the role of service delivery, information sharing and community maintenance. The KYC bypass services provided by midstream threat actors are typically B2C/C2C service models, including KYC on behalf of agents, batch registration of accounts, assistance with face recognition, etc. It has the characteristics of high frequency, low unit price, and strong demand. It has the largest number (32.32%) of transactions among threat actors, and its activity is extremely high.

KYC attack information shows an upward trend in dark web communication channels (Chart 1)

Source: Threat Hunter original report, page 8

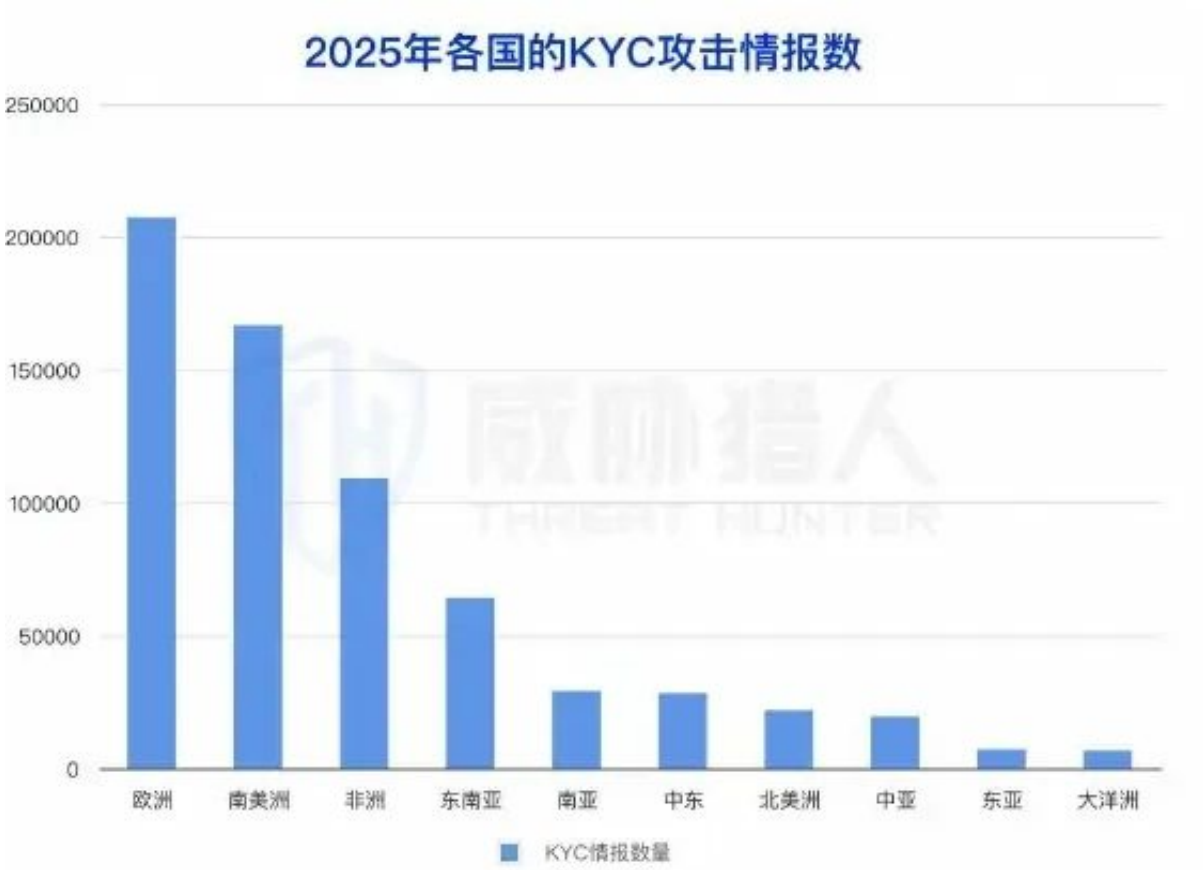
KYC attack information shows an upward trend in dark web channels of communication (Chart 2)
Source: Threat Hunter original report, page 8

- Downstream: It is the final monetization link for threat actors, mainly selling accounts that have completed KYC verification to downstream criminals. Among them, threat actors selling verified accounts accounted for 30.34%, second only to bypass services, which shows that the demand for terminal accounts is strong and the market has matured.

1.4 KYC attacks have a wide scope. Europe, South America, Africa, and Southeast Asia are the four most active regions for KYC attacks.

KYC attacks show obvious characteristics of non-high frequency in Europe and the United States and concentration in Southeast Asia. Attackers are highly focused on areas with mature financial systems or complete chains of threat actors.

According to monitoring data from the Threat Hunter anti-fraud intelligence platform:



The KYC attack industry is highly mature and separates different kinds of KYC attack cybercrime according to the chain level.

Source: Threat Hunter original report, page 9

In 2025, Europe, South America, Africa, and Southeast Asia are the four most active regions for KYC attacks (accounting for 82.93% in total). The main reason is that these regions are experiencing rapid financial digital transformation, the existence of large-scale chains of threat actors, and judging from some public news, there are loopholes in the identity verification supervision of some regions.

1.5 Among the types of KYC bypass materials, address proof has become the most frequently sold KYC attack material by threat actors.

Identity proof: It mainly includes high-definition scans/photos of the front and back of your passport, ID card or driver's license, which is the basic proof of personal identity materials.

Proof of address: Mainly includes utility bills, bank statements or tax letters, which are used to assist in verifying the user's true residence.

Biometric identification: mainly includes hand-held ID photos, nodding/blinking videos or 3D face data, which is used to break through the liveness detection authentication in KYC authentication.

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

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

KYC attacks are widespread, with Europe, South America, Africa and South-East Asia being the four most active regions of the KYC attacks.

Source: Threat Hunter original report, page 10

Complete information: Mainly includes a complete set of data packages including documents, hand-held selfies, address proof and even personal information (commonly known as "Fullz").

Enterprise certification: mainly includes business licenses, tax documents, legal person driver's license and other enterprise qualification documents, which are used to authenticate corporate accounts, cross-border e-commerce stores or corporate business.

Threat Hunter researchers analyzed the KYC bypass materials sold by threat actors and can further subdivide them into five types: address proof, identity proof, complete information, business certificate, and biometric identification.

Among them, "proof of address" bypass materials are most commonly sold. The main reasons are as follows:

- Most platforms require bills within the past 3 months, and ID cards remain unchanged for a long time. Address proofs need to be frequently updated and purchased repeatedly.
- Address proofs are mostly PDF files or photos of utility bills or bank statements. They are highly templated and can be generated in batches at low cost with the help of AI, leading to oversupply in the market.
- At the same time, "identity certificate" information, as one of the certification information required for identity authentication in most areas, is also sold in large quantities.

1.6 The price of KYC personal attack materials is stable, but the price of enterprise certification materials has the largest increase and fluctuation

In 2025, the sales price of KYC attack materials showed an overall upward trend.

Threat Hunter researchers monitored and found:

The sales price of enterprise-type certificates is the highest. The main reason is that the bypass process involves enterprise registration and other related operations, making the bypass process more complicated than the KYC bypass of individual users.

KYC bypasses the material type and the address proves to be the most frequent KYC attack material sold in the black market.

Source: Threat Hunter original report, page 11

At the same time, the prices of materials related to personal KYC certification, such as address certificates, identity certificates, biometrics, complete information, etc., have been relatively stable throughout the year. This reflects the high saturation and industrialization of the personal identity information market. The supply source is extremely sufficient. Even in the peak demand season, prices are difficult to fluctuate.

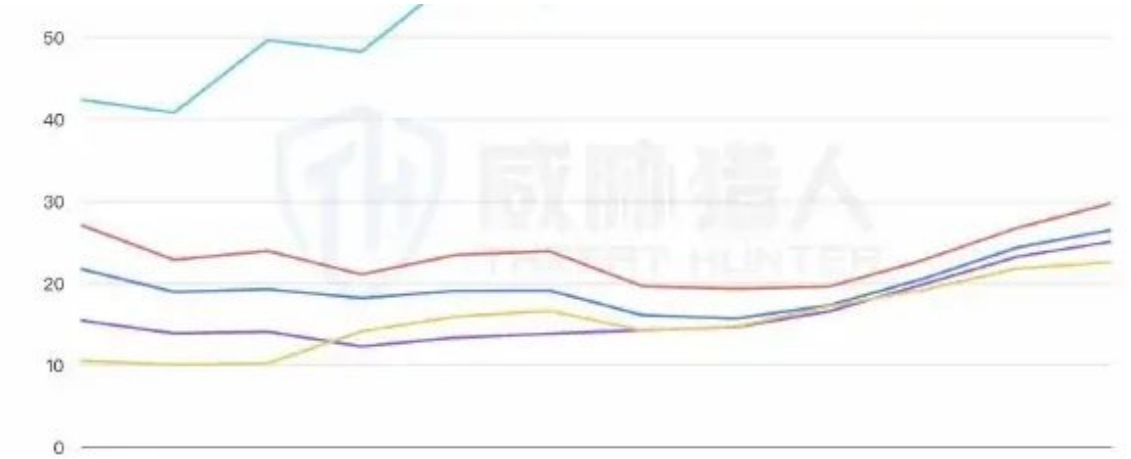
KYC attack industry chain in 2025

2. KYC attack industry chain in 2025

2.1 Overview of the industrial chain: from “workshop style” to “precision industrialization”

KYC attacks in 2025 are no longer individual attacks alone, but an underground industrial ecosystem with strict division of labor and tight integration. This ecology has formed a standard "production-sales-use" closed loop:

- The upstream is responsible for the large-scale production of "raw materials" (identity materials);
- Midstream is responsible for the research and development of core “weapons” (bypassing technologies and tools);



KYC personal assault material prices are stable, but businesses have proven the most volatile increase in class material

Source: Threat Hunter original report, page 12

- The downstream is responsible for market-oriented operations (on behalf of services);
- The terminal realizes the realization of traffic and funds. This chain-like operation significantly lowers the threshold for attack and enables large-scale production of identity fraud.

KYC attack industry chain structure

2.2. Upstream analysis of KYC attacks: “AI” and “customization” of material sources

Traditional identity materials are mainly based on leaked data, but in 2025, upstream supply showed an obvious trend of "combination of virtual and real".

KYC 攻击产业链结构

The KYC attack consists of a complete industrial chain of identification materials, technical support, proxy organization and downstream realization.

Source: Threat Hunter original report, page 10

Figure guide

1	KYC attack supply chain
2	Upstream: identity-material providers
3	Midstream: technical tools and bypass methods
4	Downstream: KYC proxy organizations
5	Monetization
6	E-commerce: fraudulent account operation
7	Social platforms: traffic diversion and fraud

1. Traditional data breaches are still the cornerstone: darknets and black markets continue to circulate large amounts of real citizen identity information (ID cards, passports, mobile phone

(Photo), database intrusion and other data leakage methods are still one of the main sources for threat actors to obtain underlying identity materials.

2. AI-generated materials become mainstream: With the popularity of generative AI, upstreams begin to provide “virtual identities” in batches. Using AI to produce

Virtual face photos, deepfake dynamic videos, and even real-life face modeling services can bypass increasingly stringent liveness detection.

3. The process of document forgery has improved: The production of physical fake documents has entered the era of "high imitation". threat actors use laser engraving technology and high-definition printing to

It has even mastered the anti-counterfeiting elements and can mass-produce forged documents recognized by OCR.

4. Improved delivery standards: threat actors deliver high-quality materials in the form of "packages", which usually include high-definition ID photos and matching personal information.

Human PII information and dynamic video material required for liveness detection.

Identity materials from various countries are sold on Telegram

A large amount of materials are sold on the dark web and trading channels. threat actors use laser printing to create fake certificates and use AI to synthesize avatars and videos.

KYC upstream analysis of attacks: “AI” and “customization” of material sources

Source: Threat Hunter original report, page 15

2.2.1 Key element information in identity materials

Regardless of the source, identity materials provided upstream must contain key information elements required to pass KYC. Mainly include:

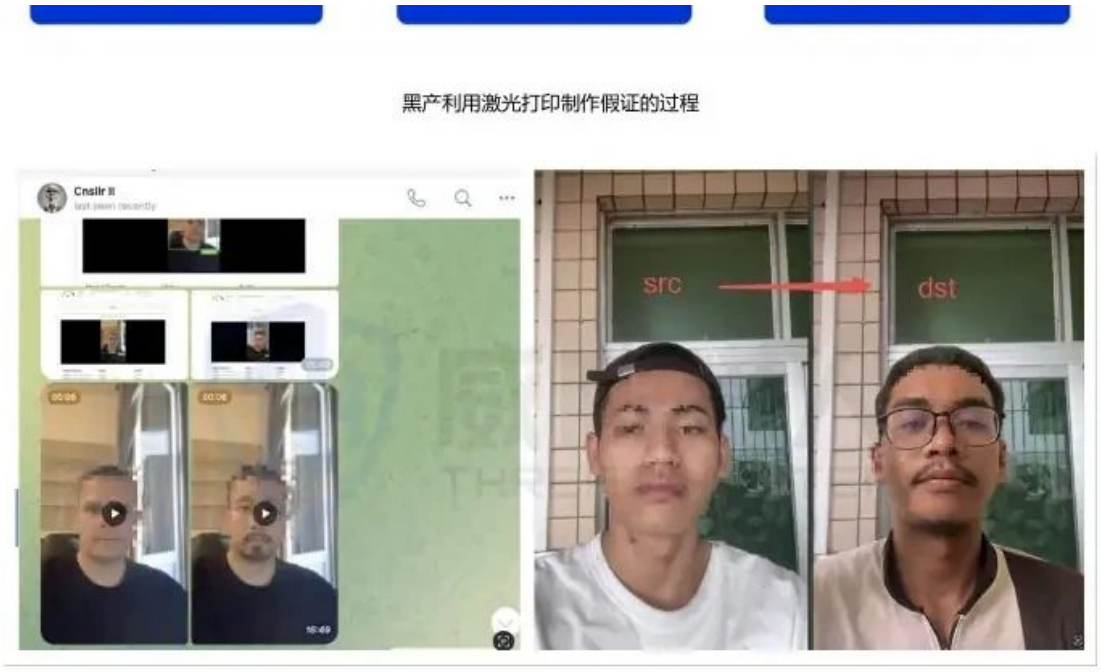
- Personal identity information: name, gender, date of birth, ID number/passport number, etc. This text information usually needs to be consistent with the submitted platform form and is

used for database verification in the background. A true and valid ID number (such as meeting the verification rules and not expired) is one of the key elements.

- ID card image: Clear and readable photos or scans of the front and back of the ID. The image must fully display the profile picture, text, number and security features on the document. Some platforms require the four corners of the document to be complete and unobstructed, which requires the upstream to provide high-resolution original ID photos. Images of forged documents also need to simulate these features, otherwise they will be easily seen through OCR and counterfeiting algorithms.

KYC upstream analysis of attacks: “AI” and “customization” of material sources (Chart 1)

Source: Threat Hunter original report, page 16



KYC upstream analysis of attacks: “AI” and “customization” of material sources (figure 2)

Source: Threat Hunter original report, page 16

- Live selfie photos/videos: biometric images of the applicant used for face comparison. Common ones are selfie photos of holding the ID, or videos recorded according to the instructed actions. The upstream must provide such image materials of the same person as in the ID photo. If real stolen information is used, there is often a lack of corresponding selfies, which is a difficulty to bypass; therefore, the upstream may use technical means to generate images of the "real" owner of the ID photo (such as deep fake videos) or recruit people who look similar to the ID photo to take the photos.
- Supporting supporting documents (if necessary): such as proof of address (bank statement or utility bill), social security card, academic certificate, etc.

These are mainly used during higher level audits. Upstream generally reserves various templates and can forge certification documents with the target's name and address.

In the transaction of threat actors, the value of a set of materials depends on its completeness and credibility; completeness means that the above elements are present, and credibility means that the material looks authentic and cannot be easily seen through system or manual review.

The upstream seller will promise the pass rate of the information it provides, such as "XX country passport + live selfie package, pass rate 90%". In order to improve credibility, threat actors will also pay attention to details: such as the background of the selfie, the lighting is consistent with common sense, the EXIF □□information of the ID photo is authentic, and the information of various materials with the same identity is consistent and matched, etc. It can be said that upstream material providers play the role of identity shapers, and the "identity" they create will directly determine whether subsequent attacks can go smoothly; therefore, this link is crucial to the overall success rate of the industry chain.

2.3. KYC attack midstream analysis - technical support

编号和安全特征。一些平台要求证件四角完整、无遮挡，这就要求上游提供高分辨率的原始证件照。伪造证件的图像也需模拟这些特征，否则容易被 OCR 和鉴伪算法识破。

Information on key elements of identification material

Source: Threat Hunter original report, page 17

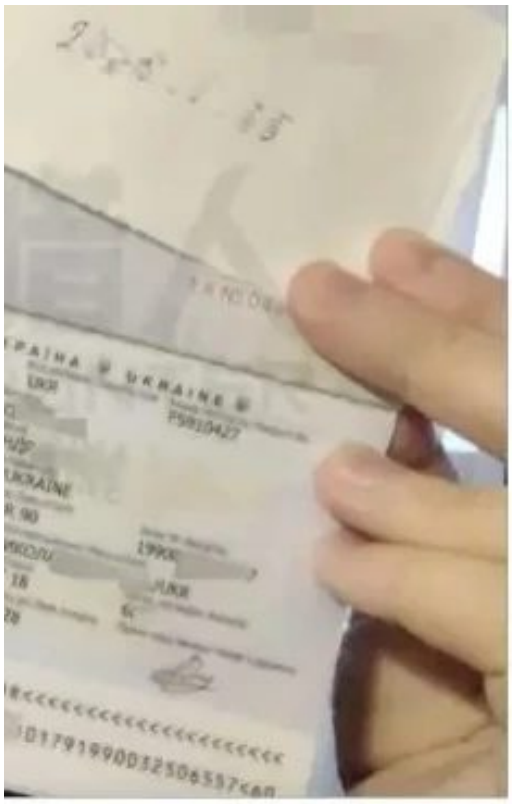
The midstream link is the technical core of KYC attacks. Threat Hunter found that the technical confrontation of threat actors in 2025 will focus on the two dimensions of environmental forgery and multimedia deception.

- Deep camouflage of environment and device fingerprints: In order to combat device fingerprints and fraud-control monitoring, threat actors extensively use “one-click new phone” tools, cloud phone clusters, and customized ROMs. These tools can not only simulate real hardware parameters (such as gyroscopes, light sensors), but also work with IP agents and GPS simulations to build a perfect virtual user environment.

- 辅助证明文件（若需要）：例如地址证明（银行账单或水电费单）

Information on key elements in identification material (Chart 1)

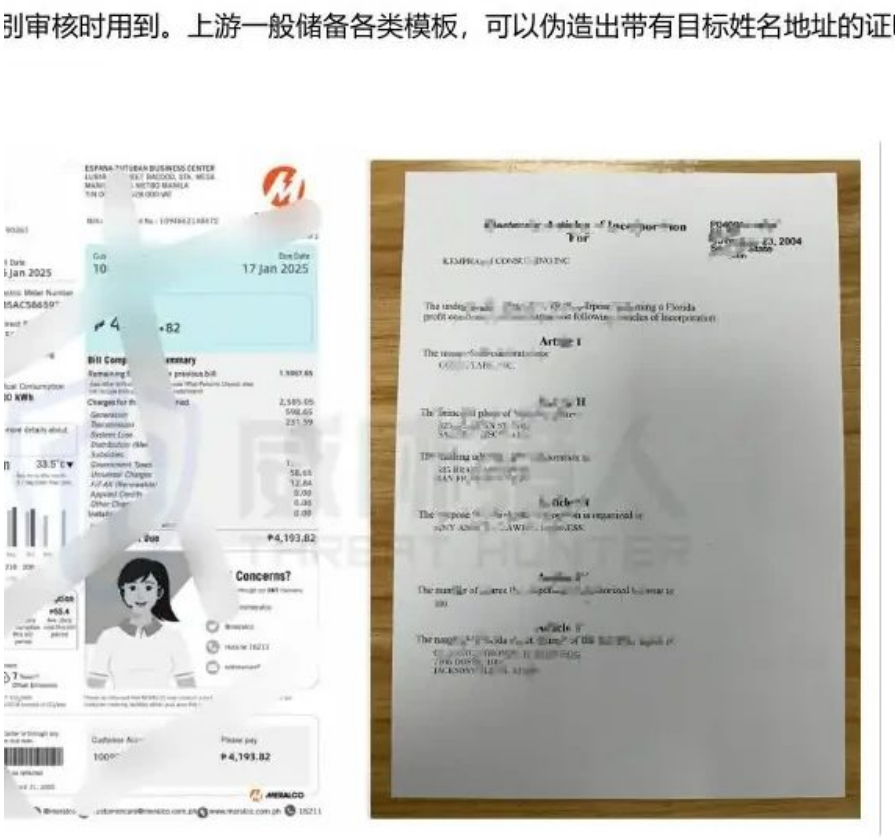
Source: Threat Hunter original report, page 18



电费单）、社保卡、学历证明等。

Information on key elements in identification material (Chart 2)

Source: Threat Hunter original report, page 18



Information on key elements in identification material (Chart 3)

Source: Threat Hunter original report, page 18

- Iteration of visual deception technology:

Camera hijacking (Injection): Use the OBS virtual camera or HOOK framework to intercept system API calls and directly "inject" the pre-recorded video stream into the application, bypassing the real-time shooting requirements.

AI Deepfake: For dynamic liveness detection (such as blinking, opening mouth, shaking head), threat actors use 3D modeling and dynamic photo filters to make static photos "alive". More advanced services can even achieve real-time face changing and voice cloning, and complex verifications such as reading specified numbers aloud.

- Dimensionality reduction attack at the protocol layer: Some high-level gangs use reverse analysis of application protocols to directly tamper with uploaded data packets or skip verification steps to achieve "one-click transaction".

"One-Click New Phone" App Geolocation Disguise Tool

Face synthesis

2.3.1 KYC Technology Evolution in Continuous Confrontation

KYC offense and defense is an evolving process. As platform fraud-control strategies are upgraded, threat actors technology continues to iterate. The following evolutionary trends can be seen in recent years:

- From static to dynamic, upgrading against live bodies: KYC verification has gradually introduced dynamic live body verification such as blinking, opening mouth, saying numbers, turning head, etc. from the initial static license upload; accordingly, threat actors have also evolved from stolen photos to video forgery, 3D faces, dynamic filters

Mirror shooting, to AI face-changing and speech synthesis, achieving a systematic bypass of multiple rounds of in-vivo verification. Overall, living body attacks have been upgraded from "playing material" to "deep fake dynamic portraits", and the concealment and pass rate continue to improve.

- Environmental camouflage and anti-detection: As the platform strengthens device fingerprinting and network environment verification, threat actors continue to upgrade and modify the machine and environment technology, from simulating hardware IDs, sensor data (such as gyroscopes, light sensors), to patching tools for directional bypass detection SDK, and continue to fight against platform rules. Platform detection logic is often analyzed and shared in a short period of time, forming a rapidly spreading anti-detection capability.
- Stronger automation and AI empowerment: threat actors introduce OCR, generative AI and other automation capabilities into the batch registration and attack process to realize verification code recognition, large-scale generation of fake faces and fake certificates, significantly improving efficiency and simulation. As a result, identity forgery has shifted from inefficient manual workshops to highly automated "industrial production", creating a systemic impact on the traditional KYC verification mechanism.

KYC mid-attack analysis - technical support (chart 1)

Source: Threat Hunter original report, page 20

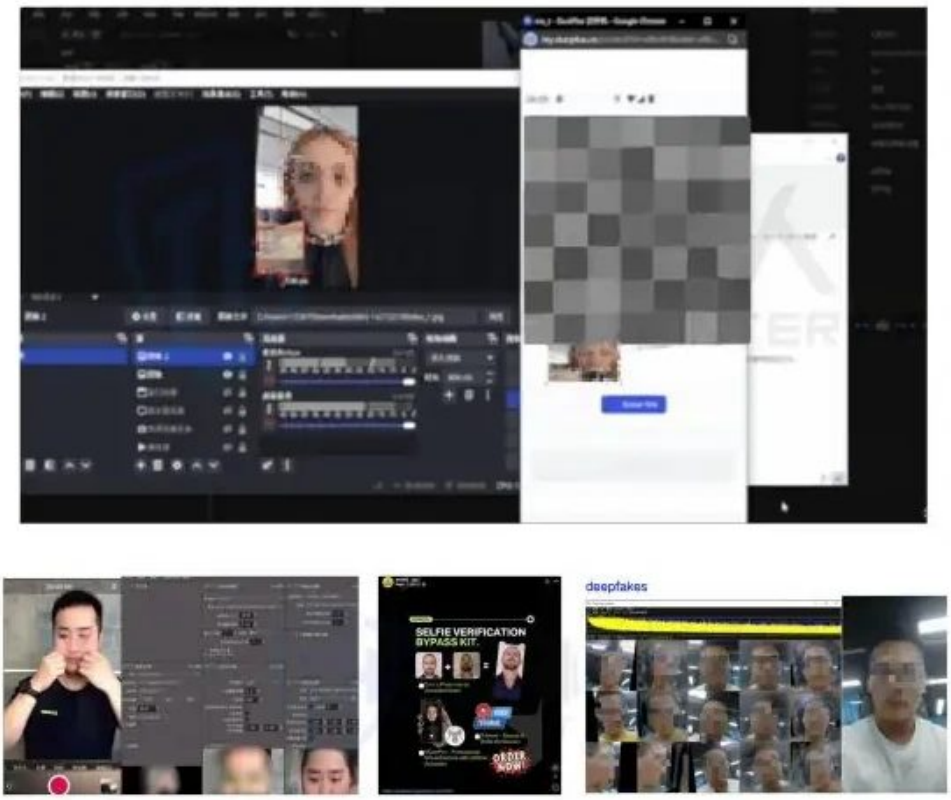
KYC Middle Impact Analysis - Technical Support (Chart 2)

Source: Threat Hunter original report, page 20

- Anti-detection and traceability avoidance: threat actors systematically introduce methods such as watermark removal, fingerprint removal, multi-hop proxies, and anti-tracking sandboxes in the identity fraud process, deliberately weakening the platform's ability to collect device, network, and content fingerprints; some gangs even adopt a "one machine, one account, one use at a time" isolation solution to minimize the risk of account association. These anti-tracing strategies significantly increase the cost of platform fraud controls and law enforcement tracing, making attacks more covert and difficult to trace back.

In general, every fraud controls upgrade on the platform will be quickly studied and countermeasures found by threat actors. This continuous confrontation has led to the gradual failure of the KYC audit mechanism in some scenarios, especially pure online remote verification, which has gradually lost ground in the face of deep forgery technology.

Technological evolution in KYC confrontation



人脸合成

KYC technology evolution in ongoing confrontation

Source: Threat Hunter original report, page 21

For enterprises, the trust model that relies on "one-time verification" is in urgent need of transformation; and the explosion of generative AI and agent technology not only brings opportunities for business innovation, but also provides low-threshold, high-efficiency automated malicious tools and scale effects for the cybercrime ecosystem. It is foreseeable that the intensity and professionalization level of identity fraud confrontation will continue to rise in the future.

2.4. Downstream analysis of KYC attacks - KYC operates on behalf of the organization's "SaaS" operations

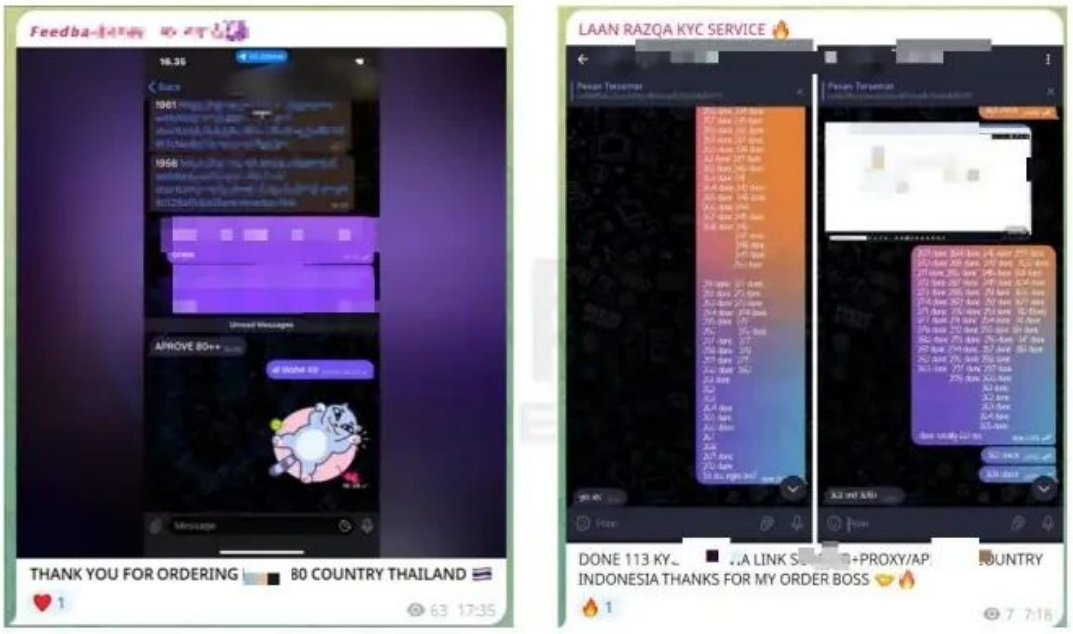
The downstream KYC agency organization has evolved into a mature service provider, and its operating model has typical business characteristics.

KYC technology evolution in ongoing confrontation

Source: Threat Hunter original report, page 22

- Public marketing: Agent organizations are active in Telegram, communities and even public networks. They clearly mark prices and develop detailed price lists based on platform difficulty and regional differences.
- Service commitment and after-sales: In order to compete for customers, the threat actors gang has launched "guaranteed", "no refund" and "after-sales warranty" services (such as free redoing if the account is blocked), which greatly lowers the psychological threshold of buyers.

- **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 technology evolution in ongoing confrontation

Source: Threat Hunter original report, page 23

- Hybrid operation model: In addition to pure technical bypass, downstream organizations will also recruit "human participants" (such as using cheap labor) and cooperate with technical means to complete difficult KYC verification.

KYC acts on behalf of the organization to post ads on Telegram

KYC agency organization provides a wide range of agency services

2.4.1 Typical characteristics of KYC organizations

As the backbone of the cybercrime ecosystem chain, KYC organizations have the following typical characteristics:

- Clearly marked prices and clear business list: They usually set prices for different platforms and different verification difficulties. The prices will fluctuate with market supply and demand, but the overall price is open and transparent, giving people the illusion of "regular services". Some organizations also list the platforms they are good at and their success rates to attract customers.

Each platform is clearly priced on behalf of the organization.

Professional internal division of labor: A mature agency team usually has a clear internal division of labor, such as technical hands performing specific tool operations, "material hands" preparing required identity materials, online docking with customers to negotiate prices and collections, and dedicated research for the latest tutorial tools, etc. This pipeline collaboration improves efficiency and success rate.

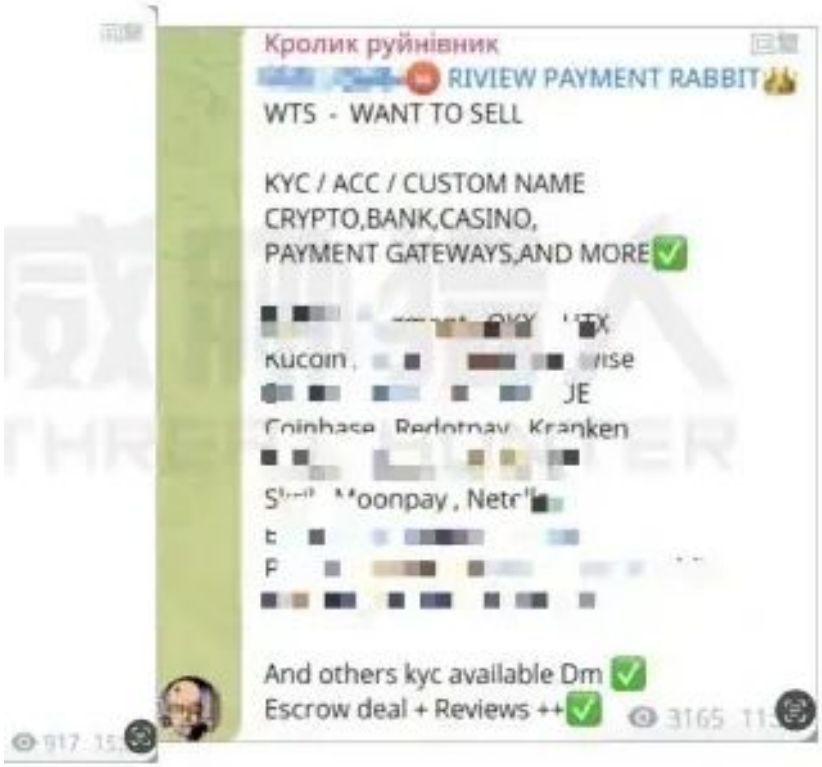
Promise on warranty and after-sales service: In order to compete, agency organizations often promise a high success rate, or even “no money back” or free redoing. On the one hand, this commitment shows its technical confidence, and on the other hand, it also attracts more customers to try it. In addition, they sometimes provide after-sales services. For example, if the account is cleared by fraud controls in a short period of time after being approved, you can apply for it again for free. The essence of these strategies is to build credibility and form a "brand" in the black market for long-term operations.

Covert Transactions and Payments: Despite overt solicitations, these organizations are quite discreet when it comes to actual transactions. Details are usually confirmed through 1V1 chat, and the payment method uses digital currency (USDT, etc.) or equivalent card numbers to avoid exposure of the capital chain. Some intermediaries will use a "guarantor" mechanism to ensure transaction security. In short, they try to reduce their risk of being attacked by law enforcement.

Use various methods to bypass, or even recruit human participants to bypass: In addition to using technical means to bypass, many proxy organizations will also use the form of recruiting human participants - recruiting human participants to provide information at a small price. People sell their identities for small profits to help proxy organizations bypass KYC verification.

Characteristic features of the KYC proxy organization (Chart 1)

Source: Threat Hunter original report, page 24



过组织，提供的代过服务很丰富

Characteristic features of the KYC proxy organization (Chart 2)

Source: Threat Hunter original report, page 24

• **明码标价，业务清单明确：**他们通常针对不同平台、不

供需浮动，但整体公开透明，给人一种“正规服务”的错觉

表和成功率，吸引客户。

代过组织对每平台都明码标价

Characteristic features of the KYC proxy organization (Chart 3)

Source: Threat Hunter original report, page 24

threat actors recruit human participants and fill in materials using a unified Google form

2.5. Analysis of KYC attack monetization links - means of profit

Accounts that have passed KYC verification are regarded as "trusted identities" and are the fundamental prerequisite for threat actors to monetize. The monetization path in 2025 is mainly focused on:

- Financial laundering: using real-name accounts for money laundering, “scoring” and cross-border transfer of cryptocurrency.
- E-commerce and marketing fraud: Registering real-name buyer accounts in batches to obtain platform subsidies, or registering fake merchant stores to commit fraud and sell counterfeit products.
- Credit and resource abuse: In areas such as travel and social networking, fake identities are used for illegal operations, traffic fraud or credit lending.

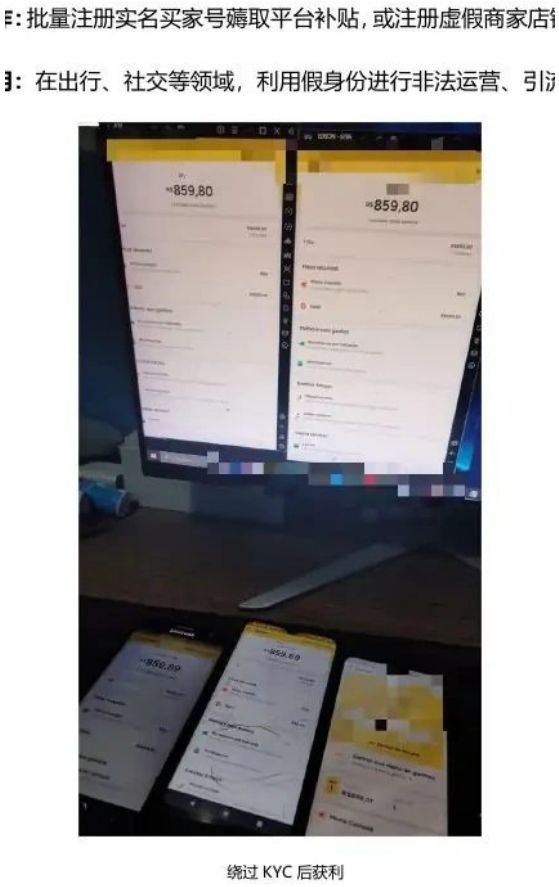
Make profit after bypassing KYC

Typical KYC attack cases in 2025

3. Typical KYC attack cases in 2025

3.1 KYC industry attack chain structure in 2025

From "single point breakthrough" to "full stack automation": AI and physical plug-ins reconstruct the attack cost curve. KYC attacks in 2025 are no longer limited to a single technical bypass, but have formed a standardized industrial closed loop of "material generation-environment camouflage-visual injection-logical confrontation-monetization harvesting".



KYC attack realization chain analysis - means of profit

Source: Threat Hunter original report, page 26

- The threshold for attack is significantly lowered: With the popularity of "one-click AI face-changing" and "customized cloud phone", high-precision identity forgery has been reduced from laboratory technology to cheap threat actors' tools.
- The defense boundary is physically penetrated: Attack methods have evolved from pure software injection (such as ROM customization) to "software and hardware combination". The emergence of physical means such as polarizer extinction marks the risk of failure of passive life detection technologies such as screen reflection.
- Acceleration of business risk transmission: The standardization of the attack chain has greatly shortened the cycle from "forging identity" to "credit/e-commerce cash out", and threat actors' testing and iteration speed of fraud-control rules has reached the hour level.

3.2 New methods of KYC industry chain in 2025

In 2025, KYC has broken through the single-dimensional software attack and defense. By introducing physical optical equipment (such as polarizers) and deep reverse logic (such as three-color hijacking), threat actors achieve a "dimensionality reduction attack" on traditional visual fraud detection. At the same time, the proliferation of fool-like AI tools has greatly diluted the cost of high-level attacks.

2025 KYC industrial attack chain structure

Source: Threat Hunter original report, page 28

3.2.1 Visual confrontation layer: "dimensionality reduction attack" of physics and optics

[Core changes] From "software photo editing" to "optical deception", physical plug-ins directly invalidate passive liveness detection.

Physical matting methods: In view of the platform-dependent "screen reflection" and other living characteristics, threat actors introduce physical devices such as polarizers to eliminate the screen reflected light and bypass the detection logic from the optical physical level.

High-definition reconstruction technology: The use of high-resolution screens combined with AI post-processing technology (denoising, color correction, jitter simulation) makes the "screen-shattering" attack images infinitely close to real shots in terms of details and textures, making it difficult for purely visual algorithms to distinguish electronic screens from real faces.

3.2.2 Injection attack layer: "Precise reverse engineering" of logical vulnerabilities

[Core changes] Upgraded from "brute force injection" to "interactive logic deception", making deep use of the verification mechanism of specific algorithms.

Deep reverse interaction: threat actors are no longer satisfied with simple video stream replacement, but have deeply reversed the interaction logic of liveness detection (such as color verification mechanism).

The emergence of customized tools: Typical tools such as "three-color camera hijacking" can accurately feedback specific color or light changes according to app instructions, achieving precise deception for specific algorithm logic, proving that threat actors' understanding of fraud controls codes has reached the code level.

3.2.3 Basic resource layer: “fool-like operation” of high-end technology

[Core changes] From "technical geeks only" to "threat actors infrastructure available to everyone".

Extreme ease of use: The “one-click AI face-changing tool” that appeared in October successfully encapsulated the complex Deepfake technology into a fool-proof operation of “upload and generate”.

Scale-up of attacks: The extremely low threshold for use causes some large platforms to face the risk of scale-up attacks. The extreme dilution of attack costs means that defenders will face massive, low-cost, and high-concurrency identity fraud challenges.

3.3 Typical cases of KYC attacks in the e-commerce industry [Case Review]

Target of attack: "Use now, pay later" credit limit and high-value commodities of a leading e-commerce platform. Core method: Use the "four-piece set" of identity materials combined with cloud mobile phone environment disguise to register "white household" accounts in batches. Bypassing facial recognition through injection attacks, obtaining high-value credit from the platform (such as installment payments, consumer loans), and finally committing fraud by purchasing easily cashable commodities (such as gold, electronic products) or directly withdrawing cash, forming a complete chain of "loan fraud/scam" threat actors.

Modern e-commerce KYC attacks are no longer a single point of account registration, but a strict industrial assembly line. From material preparation to final realization, the attack process is as follows:

Typical process of KYC attack

3.3.1 Phase One: “Industrial Assembly” of False Identity

The starting point of the attack is to construct a person who appears to be "real" in the digital world. E-commerce fraud controls usually verifies the consistency of identity information with phone number and IP address, so threat actors need to prepare a full set of matching materials.

- Identity materials: The attacker purchases "materials" including the front and back of ID cards, handheld photos, and high-definition facial videos from the upstream black market.

In order to improve the pass rate, these materials are often screened to ensure that the documents are unobstructed and the videos meet the requirements of living subjects.

Preparation and testing of identity materials

- Communication resources: Use the SMS verification-code receiving service to obtain non-real-name phone numbers (or black cards) in batches to receive registration SMS verification codes. These numbers are often "daily disposable" consumables in the attack chain.

Prepare the phone number required for registration

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：通过将手机摄像镜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，已在中国大陆对多家大型平台实施攻击并宣称获得成功。

KYC's typical case of assault in the e-commerce industry.

Source: Threat Hunter original report, page 30

3.3.2 The second stage: "Deep camouflage" of device fingerprints and environment

In order to bypass the strict fraud controls of e-commerce platforms, attackers must solve the compliance issues of "device fingerprint" and "geographic location".

- Network and geolocation emulation: The attacker will modify the IP address and GPS location to match the identity material (ID card ownership location)

The consistent city deceives the fraud-control model into thinking that this is "local people operating locally."

Prepare the environment required to bypass KYC

- Device fingerprint confrontation: Use the Xposed/Magisk framework to reversely modify the underlying parameters of the phone (IMEI, MAC address, power, sensor data, etc.), so that every cloud phone is a brand new real mobile device without historical stains in the eyes of the platform.

Reverse and modify device fingerprint simulation geolocation

3.3.3 The third stage: visual injection and KYC practical breakthrough

This is the most critical "breakthrough" link in the attack chain. When the e-commerce platform triggers a core request for "liveness verification" or "opening payment credit", the attacker launches the attack script.

- Video stream hijacking: The attacker does not shoot real footage, but hijacks the camera's system call interface through HOOK technology.
- Dynamic adjustment: "Inject" the locally prepared high-definition dynamic face video (corresponding to the first-stage materials) directly into the app's collection window. The attacker will even adjust the parameters of the injected video in real time based on app feedback (such as insufficient light and wrong angle) until they can fool the live detection algorithm.

Trigger verification KYC and load locally prepared information

3.3.4 The fourth stage: credit realization and asset harvesting

准备绕过 KYC 所需的环境

Phase II: “Deep disguise” of equipment fingerprints and environment (chart 1)

Source: Threat Hunter original report, page 32

抗： 利用 Xposed/Magisk 框架逆向修改手机底层参数（IME

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

逆向并修改设备指纹

Phase 2: “Deep disguise” of equipment fingerprints and the environment (Chart 2)

Source: Threat Hunter original report, page 32

Once the KYC verification is passed, the account will become a "high-credit real-name user" in the eyes of the platform. The attacker then enters the harvesting phase, which is extremely fast and usually completes within hours.

- Credit cash-out: Immediately activate the platform's consumer credit services (such as XX payment, XX IOU) and obtain credit lines ranging from thousands to tens of thousands of yuan.
- Material transfer: Use the credit limit to purchase hard currency such as mobile phones and gold, and then sell the stolen goods after receiving the goods; or directly apply for a cash loan to transfer out.

Since the account information is forged or used fraudulently, bad debts incurred by the platform cannot be traced back to the attacker himself.

Get a consumer credit line after bypassing KYC

3.4 Typical cases of KYC attacks in the financial/credit industry [Case Review]

算法。

Phase 3: Visual Injection and KYC Operational Breakout

Source: Threat Hunter original report, page 33

Target of attack: Credit lines of Internet financial platforms (such as cash loans). Core method: Different from pure machine traffic manipulation, financial scenarios often adopt the "human-in-the-loop crowdsourcing + technical assistance" model. threat actors recruit "white households" with good credit or use leaked real identities to package high credit qualifications through location tampering and flow forgery. After passing the review using face injection, they apply for loans in batches and "cut off the supply" and run away, forming bad debts.

KYC attacks and cash-out links in credit scenarios

3.4.1 The first stage: precise material selection and “credit packaging”

Financial fraud controls relies heavily on credit reporting, and it is difficult to obtain high credit limits with purely false identities; therefore, attackers have established a mature human-operated identity distribution system.

- Identity intermediary and commission settlement: Different from simple deception, this is a trading market with clear price standards. As a hub connecting the upstream and downstream, the intermediary looks for real users who are willing to sell their identities to the upstream (commonly known as "flesh"), and takes orders from the downstream attack team.

- Operation mode: The downstream initiates demand The intermediary contacts the upstream "physical body" to cooperate with the real name After the verification is passed, the intermediary settles the commission to the upstream.
- Low cost: According to black market conditions, the settlement price of a set of "human-operated services" that includes real ID card information and facial verification is often only around US$10 (approximately RMB 70). This extremely low acquisition cost allows threat actors to attack financial credit products in batches with extremely high ROI (return on investment).

3.4.2 The second stage: “de-association” of device fingerprints

In order to prevent being identified as a gang crime by the financial platform's "association map", the attacker implemented strict device isolation.

- One machine, one number, one IP: Use the modification tool to modify the device IMEI and IMSI, and cooperate with the high-anonymity proxy IP to ensure the independence of each application environment and avoid the fraud-control rule of "multiple accounts on the same device".

Financial grade device fingerprint bypass configuration

KYC Attacks on Typical Cases in the Financial/Credit Sector [Repeated Case] (Chart 1)

Source: Threat Hunter original report, page 34

KYC Attacks on Typical Cases in the Financial/Credit Sector [Case Rox] (Chart 2)

Source: Threat Hunter original report, page 34

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

KYC attacks in the financial/credit sector

Source: Threat Hunter original report, page 34

3.4.3 The third stage: "Video forgery" under high confrontation

Financial apps have the strictest liveness detection (usually including action interactions or readings).

- AI Deepfake: Targeting the action liveness detection that appears frequently in financial apps (such as "Please blink", "Please open your mouth", "Turn your head left/right"), attackers use AI-driven technology to "animate" static photos. Through the action migration algorithm, the attacker can control the static face to accurately complete the continuous actions specified by the system, and inject the synthesized dynamic video stream into the app in real time, thereby deceiving live anti-counterfeiting detection.

AI-generated dynamic verification videos such as blinking, turning head, etc.

3.4.4 The fourth stage: “cleaning” of funds and formation of bad debts

Batch cash withdrawal: After the credit is approved, threat actors quickly transfer the loan to the secondary money laundering account (benchmark platform).

Account abandonment: After the withdrawal is completed, the account will be abandoned, resulting in irrecoverable bad debts on the platform.

Phase I: Precision selection and “credit packaging”

Source: Threat Hunter original report, page 35

Screenshots related to successful loan and appropriation after credit is granted

3.5 Typical cases of KYC attacks in the virtual currency exchange industry [Case Review]

Target of attack: Real-name accounts of the world’s leading cryptocurrency exchanges Core method: Exchanges have become the “hardest hit area” for identity fraud. Attackers no longer rely solely on P-pictures, but purchase a large number of "human-operated complete sets of materials" (front and back of IDs + hand-held photos + pre-recorded face videos). Through camera hijacking technology, pre-recorded real-life videos are directly injected into the app to complete live detection.

Motivation of threat actors: Extremely high ROI (return on investment) is the fundamental driving force for attacks. After a set of low-cost materials is processed into a "finished product number", the price increases several times; if used for airdrops or money laundering, the potential revenue can be as high as hundreds and thousands of times.

From "materials" to "finished products" and then to "huge profits", a standardized asset value-added link is formed.

Exchange KYC attack and cash out link

3.5.1 The first stage: source of supply chain - "full set of human participants" materials

Unlike AI-generated virtual faces, exchange attacks prefer to use real identities to cope with strict document OCR and background checks.

Phase III: “Video forgery” in high-level confrontation

Source: Threat Hunter original report, page 36

- Graded sales of materials: There are clear sales standards in the black market. For exchange attacks, the most sought-after material is the "Grand Slam" material:
- Basic version: ID card/passport front and back photos.
- Advanced version: Basic version + selfie with ID in hand.
- Deluxe version (only for attacks): Advanced version + pre-recorded face video.

Note: These videos are usually recorded by genuine participants, contain basic movements such as nodding and blinking, and are specially used for live verification.

A complete set of "certificate + video" real-life materials sold on Telegram

3.5.2 The second stage: intermediate processing - video injection and environment camouflage

After receiving the information, the threat actors technical team is responsible for "processing" it into a verified account.

- Pre-recorded video injection: When the exchange app requires liveness detection, the attacker does not use a camera to shoot, but uses HOOK tools or virtual camera software to inject the prepared "pre-recorded live video" directly into the data stream. Since the video itself is recorded by a genuine participant and contains real biological characteristics, this method can bypass non-interactive liveness detection with a high probability.
- Environment alignment: Cooperate with the residential proxy IP to simulate that the user is in the country where the certificate belongs, and complete the compliance packaging of the device fingerprint.

Inject local pre-recorded video using virtual cameras

3.5.3 The third stage: value realization - threat actors "high ROI business"

Mode A: Sales of finished product number (Account Flipping)

Investment: The cost of purchasing a set of Southeast Asian/Latin American real-life materials (including videos) is about $1 - $5.

Output: Advanced certified accounts that have passed KYC Level 2/3, and can be sold for $20 - $100+ on the black market.

ROI: Net profit 300% - 900%. threat actors can double their assets with just simple pipeline operations.

Mode B: Airdrop Witch Attack Airdrop: In cryptocurrency and blockchain projects, airdrop means that in order to promote new coins, the project will issue free tokens to users.

Sybil attack: In the field of computer security, it refers to an attacker controlling a network or system by creating a large number of false identities (accounts or nodes).

Investment: To register 100 accounts in batches, the total cost is about $1,50.

Output: If a new currency project issues an airdrop, the income from a single number may reach $500 - $2,000, and the total income may reach $50,000+.

ROI: 5000%+; This kind of gambling-style profit temptation prompts threat actors to use tens of thousands of human participants's identities to carry out "saturation attacks."

Mode C: Money laundering channel value: For electronic fraud or online gambling gangs, a safe large-amount currency withdrawal account is a "rigid need". Its actual value far exceeds the price of the account itself, and it is an indispensable consumable on the fund transfer link.

Conclusion

4. Conclusion

Phase 2: Intermediate processing - video injection and environmental disguise (Chart 1)

Source: Threat Hunter original report, page 38

Phase 2: Intermediate processing - video injection and environmental disguise (Chart 2)

Source: Threat Hunter original report, page 38

The attack and defense of KYC identity authentication have evolved from a single technical confrontation to a highly mature industry chain game. Although the fraud controls fence is tightening day by day, under the temptation of extremely high production ratio, the iteration speed of threat actors technology is far faster than expected, and the protection of the identity trust system is destined to be a protracted battle.

Threat Hunter recommends:

1. Build an identity fraud-control system with continuous monitoring

KYC should not stop at one-time verification, but needs to cover the entire life cycle of the account. Trigger secondary verification in high-risk operations or key nodes, and continuously monitor account behavior and environmental changes to promptly identify abnormal transactions, remote logins, and batch account characteristics to prevent risks from lurking for a long time.

2. Upgrade KYC verification and anti-fraud capabilities

Introducing a multi-factor joint verification mechanism, integrating document verification, liveness detection, device fingerprint, geographical location and authoritative data verification, and focusing on deploying deep forgery detection capabilities to combat new attacks such as AI face-changing and video injection.

3. Collaborate to block upstream resources and attack spread

Reduce the pass rate of counterfeit information by accessing authoritative data sources, promote collaboration between supervision and industry, crack down on identity data black markets and

counterfeiting chains, establish a risk clue sharing mechanism, and prevent the reuse of false identities across platforms.

4. Establish a normalized red and blue offensive and defensive drill mechanism

Regularly conduct red and blue attack and defense tests, and conduct "actual simulation" of the entire business link from the attacker's perspective. By simulating camera hijacking, injection attacks and threat actor link penetration, we proactively discover blind spots and vulnerabilities in the existing fraud-control system, transform "passive defense" into "active iteration", and complete reinforcement before real attacks occur.

As a research team that has been paying attention to cybercrime ecosystem intelligence for a long time, we go deep into the front lines of the dark web, continue to deconstruct attack methods, restore industry links, and provide the industry with a real risk perspective. We know that only by maintaining keen insight and continuous tracking can we take the initiative in the identity game in the AI □□era.

Threat Hunter KYC red team services rely on professional risk intelligence collection and analysis capabilities, covering multiple channels such as Telegram, dark web, forums, etc. to ensure timely acquisition and in-depth analysis of KYC-related fraud clues, IOCs and risk characteristics.

Through this intelligence, we gain insight into the latest methods of threat actors and industry chain dynamics. We transform the intelligence into practical weapons, regularly conduct red and blue attack and defense tests, simulate real attack links to conduct in-depth physical examinations of the business, and achieve early warning of KYC attacks, helping enterprises to take effective measures before or in the early stages of fraud to avoid or reduce losses.

Note: The data information provided in this report is estimated and analyzed by Threat Hunter based on large sample data sampling and collection, small sample survey, external intelligence data collection, data model prediction and other research methods. Due to the limitations of any data sources and technical methods in the field of statistical analysis, the data information estimated and analyzed based on the above methods are for reference only.

Phase III: Value realization - high ROI business

Source: Threat Hunter original report, page 39