TRM REPORT

The 2026 AI-in-Crime Adoption Index

How the rapid adoption of AI by criminals has driven a surge in scams

trmlabs.com

Table of contents

Key takeaways

- AI is reshaping every stage of the crime lifecycle — lowering the barrier to entry for offenders, increasing the scale and sophistication of attacks, and creating new challenges and opportunities for investigators.
- TRM's new AI-in-Crime Adoption Index puts overall AI adoption across crypto crime at an Emerging level — 54 out of 100, up from 28 in 2024 — led by scams, the only crime type to reach a Mature level; while narcotics remains in the earliest, Horizon stage.
- The share of scam reports where AI was actually part of the scam — deepfakes, AI chatbots, AI-branded lures — has grown roughly 13× since 2022. Reported deepfake-scam losses in 2026 to date already exceed all of 2025 by 263%.
- Crypto hacks hit a record 201 in H1 2026 (2×+ YoY), yet just 4% of incidents drove 75% of the losses. The majority of those large incidents were infrastructure compromises, which can involve private-key and credential theft — two areas where AI is being applied effectively by criminals.
- AI is climbing the ransomware chain — no-code kits sell for USD 400–1,200, "vibe-hacking" ransoms run USD 75,000–500,000+ in BTC, and July 2026 brought the first documented agentic ransomware attack (JadePuffer).
- AI adoption in narcotics trafficking remains limited — the drug trade has been comparatively slow to embrace AI, with current use concentrated in marketing and customer engagement, though an emerging risk is the use of AI to design unscheduled precursor analogues.

OVERVIEW

AI adoption by criminals surges 40% year on year, with the surge led by scammers

Generative AI has spread faster than any consumer technology that came before it. Within three years of ChatGPT's launch, generative AI tools have reached 53% of the US population, a faster path to that scale than either the personal computer or the internet managed at the same age. Businesses have also rapidly integrated AI into their everyday operations. Like previous general-purpose technologies, AI is not simply improving existing workflows, but reshaping how knowledge is created, decisions are made, and economic activity is organized.

Criminal organizations are adopting the same tools for many of the same reasons. AI lowers the skill required to run sophisticated operations, allows a single operator to reach far more victims, automates tasks that once required large teams, and makes deception more convincing through synthetic media and large language models (LLMs). The result is not an entirely new criminal ecosystem, but one that operates faster, at greater scale, and with fewer constraints.

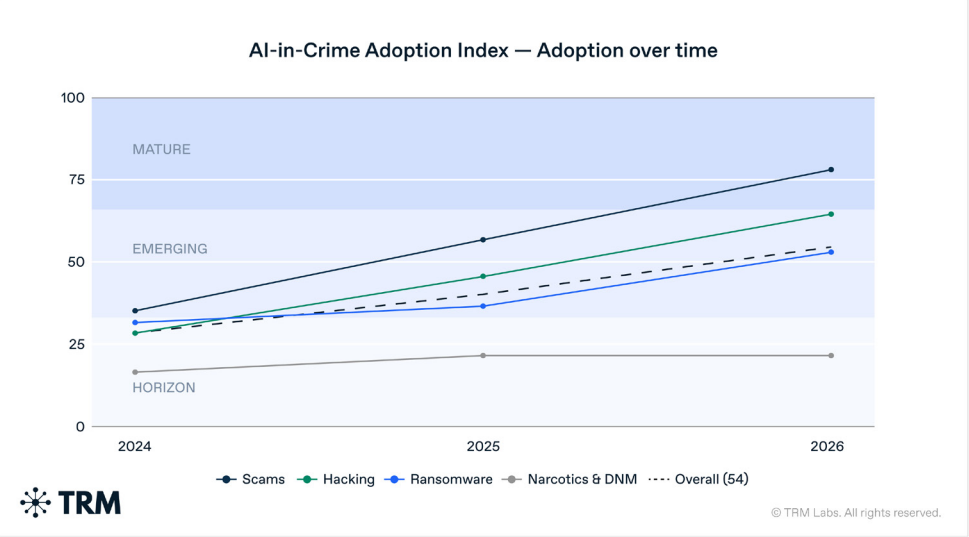
Because much of this activity ultimately moves value on public blockchains, those changes can be observed and measured. The same actors, tactics, and incentives drive crime whether or not cryptocurrency is involved, and the blockchain records what most of the criminal economy keeps hidden — so these on-chain trends are a reasonable proxy for how AI is reshaping crime more broadly.

This report examines how AI is reshaping major crypto-enabled crime typologies — and how the same technology is improving the ability of investigators, financial institutions, and law enforcement to disrupt them.

To gauge the trajectory, TRM built the **AI-in-Crime Adoption Index** — a composite measure of how deeply AI has been adopted across the major crypto crime typologies, each mapped to the Horizon, Emerging, and Mature framework. Overall adoption sits at an Emerging level, 54 out of 100. It is most advanced in scams — now at a Mature level and the clear category leader — followed by hacks (spanning opportunistic code exploits and DPRK state-sponsored theft) and ransomware, both Emerging. Narcotics and darknet markets remain at the earliest, Horizon stage.

QUICK LINKS

Criminal adoption of AI is rising across the board. The overall index climbed from about 28 in 2024 to 54 in 2026 — with the steepest gains in scams and hacks, driven by increasingly automated, productized AI tooling.



The AI-in-Crime Adoption Index scores each crime type on three components:

1. **Prevalence:** How common AI involvement is within the crime type; the share of its activity that shows an AI nexus
2. **Lifecycle breadth:** How many stages of the crime's lifecycle (targeting, deception, execution, laundering, cash-out) show AI in use
3. **Sophistication:** How advanced that AI use is — from basic AI-generated content to deepfakes and, at the frontier, autonomous systems

AI-in-Crime Adoption Index — 2026 pillar scores

Crime type	Prevalence	Lifecycle breadth	Sophistication	Index	Stage
Scams	80	80	75	78.4	Mature
Hacking and state-sponsored theft	60	60	75	64.7	Emerging
Ransomware	40	80	50	53.1	Emerging
Narcotics and darknet markets	20	20	25	21.6	Horizon

TRM

QUICK LINKS

Every crime type TRM evaluated now shows a measurable AI footprint. But scammers are the broadest adopters, applying AI across the widest span of an operation, from generating victims and lures to running the conversations that sustain the fraud.

By crime type:

Scams (Mature)

AI is most entrenched here, and the only crime type at a Mature level. The use of AI in scams now spans nearly the whole operation — from generating target lists and lures, to deepfake and chatbot deception, to increasingly automated victim conversations. Scammers are the broadest adopters of AI in crypto crime.

Hacking and state-sponsored theft (Emerging)

Climbing fast, DPRK has turned AI into operational tradecraft, with deepfake IT-worker infiltration and AI-run social engineering. AI-assisted vulnerability discovery has also lowered the bar for code exploits, helping drive a record 201 hacks in H1 2026, more than double the previous year.

Ransomware (Emerging)

AI already sits in most ransomware operations at the phishing and initial-access stage, and 2025 brought the first documented AI-assisted extortion and no-code kits. The use of AI in ransomware attacks runs from targeting through negotiation but stops at laundering, where no AI use has yet been observed.

Narcotics and darknet markets (Horizon)

Buyers appear to openly distrust “AI-generated” markets. AI use is confined to the marketing fringe, such as product images, listings, and a few jailbroken-model services. There is currently no evidence of AI in synthesis, laundering, or cash-out.

The sections that follow examine how AI is changing each major crypto-enabled crime type, where in the criminal lifecycle it is having the greatest impact, and what those shifts mean for investigators.

How AI rewired the crime ecosystem

AI functions as a force multiplier on both sides of the ledger. While it has scaled the criminal side of illicit finance, and it has scaled the response to it in roughly equal measure. The same four shifts that expanded what criminals can do have expanded how investigators can disrupt that illicit activity.

The shift	For criminals	For crime-fighters
1. The skill floor collapsed	No-code malware kits and uncensored language models let anyone run a scheme, no coding or fluency required.	AI clusters wallets and traces cross-chain flows in minutes, work that once took days and specialist skill. LLMs now allow investigators to use natural language to run complex investigations.
2. The scale ceiling lifted	A single operator can now run hundreds of simultaneous victim conversations that once required a full team.	Detection scales with the crime. Anomaly and pattern models surface scam wallets and laundering typologies earlier than victim reports or manual tips.
3. Fake identity went industrial	Deepfakes, voice clones, and synthetic Know Your Customer (KYC) win victims' trust and defeat the identity checks meant to stop them.	AI-assisted KYC and deepfake and liveness detection are now standard at exchange onboarding, backed by FinCEN's deepfake alert, the EU AI Act, and the NIST AI Risk Management Framework.
4. A criminal AI economy formed	Dark language models (AI models with criminal capabilities) and deepfake-as-a-service are productized and sold on crypto payment rails — criminals buy this capability instead of building it.	AI collapses the same fragmentation on defense, fusing blockchain, open-source, corporate-registry, communications, and sanctions data from around the world into a single investigative picture. This enables analysts to see the whole network behind the tools, not just one payment.

QUICK LINKS

CATEGORY DEEP-DIVE

Scams and fraud

AI's footprint in the scam economy is growing fast. The share of scam reports where AI was part of the scam has climbed roughly 13× since 2022, and reported deepfake-scam losses in 2026 already exceed all of 2025.

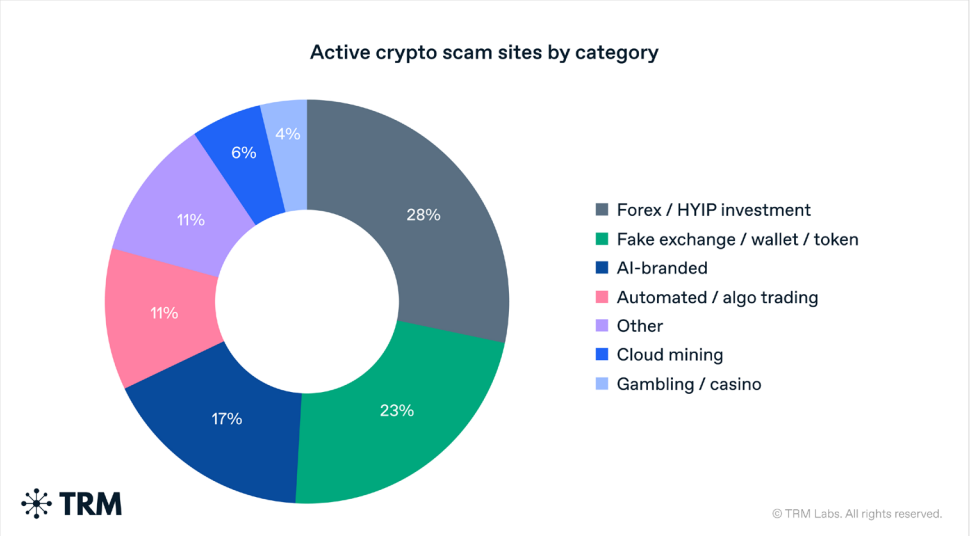
~13×	+263%	~400×
growth in scam reports where AI was part of the scam, 2022 to 2025	growth in deepfake-scam losses, 2026 YTD vs. all of 2025	jump in reported AI-scam losses, Q1 to Q2 2026 (very small base — directional)

AI appears in scams in two ways:

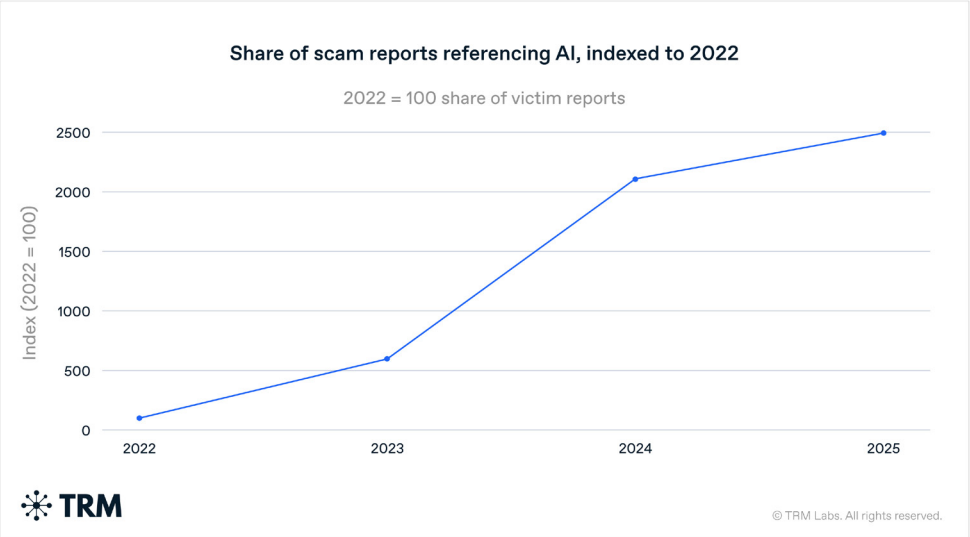
1. **Operationally:** Scammers use AI to run and scale their operations, whatever the lure — whether romance, fake jobs, investment schemes, or fake giveaways
2. **The lure:** A set of scams sell AI, using interest in the technology as the hook, such as fake "AI trading" bots and AI investment platforms

Among crypto scams with active domains today, 17% claim to sell AI products. While this is not the largest attack method employed — sitting behind forex scams (fraudulent investment schemes that lure victims with false promises of fast wealth, fake trading platforms, and guaranteed profits) and fake exchanges — the fact that it is the third largest after such a short period of time is notable.

QUICK LINKS



That growing footprint shows up in how often AI is mentioned in scam reports at all. As shown below, references to AI in scam reports have climbed roughly 25× since 2022. Not all of that growth reflects criminals using AI; about half of the increase — roughly 13× — comes from scams where AI was part of the attack, while the remainder comes from victims using consumer AI tools like ChatGPT to investigate a scam they had already encountered. Because many victims never realize AI was used against them, even the crime-related share is a conservative floor.



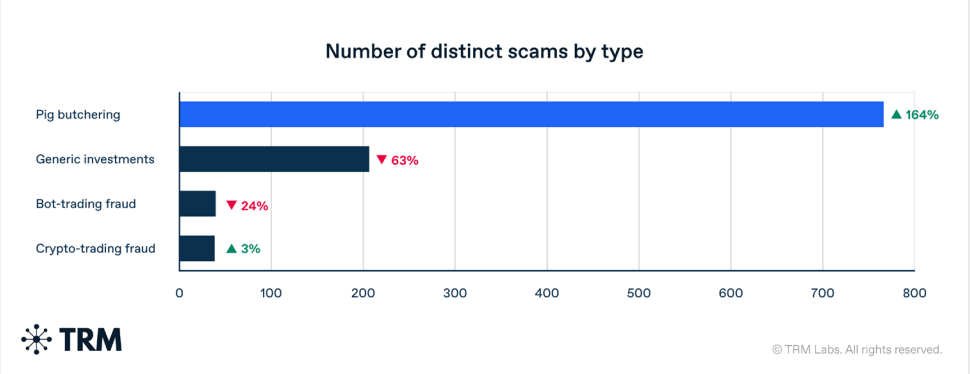
Counts all scam reports mentioning AI, both scammer-side use (deepfakes, AI chatbots, AI-themed platforms) and victims using AI to investigate a scam. The scammer-only series grew roughly 13× over the same period.

QUICK LINKS

The operational impact of AI is broader and extends across virtually every scam typology. LLMs enable a single operator to conduct convincing conversations with victims in multiple languages at a scale that previously required large teams, while deepfake technology makes impersonation faster, cheaper, and more credible. The dollar losses are following: reported losses tied to deepfake scams in 2026 year-to-date already exceed all of 2025 by 263%, and reported AI-scam losses jumped roughly 400× from the first to the second quarter of 2026 — though this figure rests on a very small base and a single outsized report, and should be read as directional rather than precise.

Pig butchering is the clearest example of a scam leveraging AI for increased scope and success. Losses reported to the FBI's Internet Crime Complaint Center rose from USD 5.8 billion in 2024 to USD 7.2 billion in 2025, and the number of distinct pig butchering scams tracked by TRM grew 164% over the past year, among the fastest-growing scam types by count.

In 2025, TRM identified USD 35 billion in scams. With the broadly referenced statistic that scamming is undercounted by up to 85%, this number could be far larger. AI now sits at the front end of these operations: victim conversations have moved from scripted human operators to AI chat that adjusts to the victim's language and location and keeps a profile of the victim over weeks of contact. And video verification that once used a human stand-in is now increasingly done with real-time deepfake face-swapping and voice cloning.



As AI capabilities continue to improve, scammers are likely to become more efficient at every stage of the fraud lifecycle — from identifying and engaging victims to sustaining convincing interactions and impersonating trusted individuals. The result is not necessarily new scam typologies, but more scalable and more effective versions of existing ones.

CATEGORY DEEP-DIVE

Hacking and state-sponsored theft

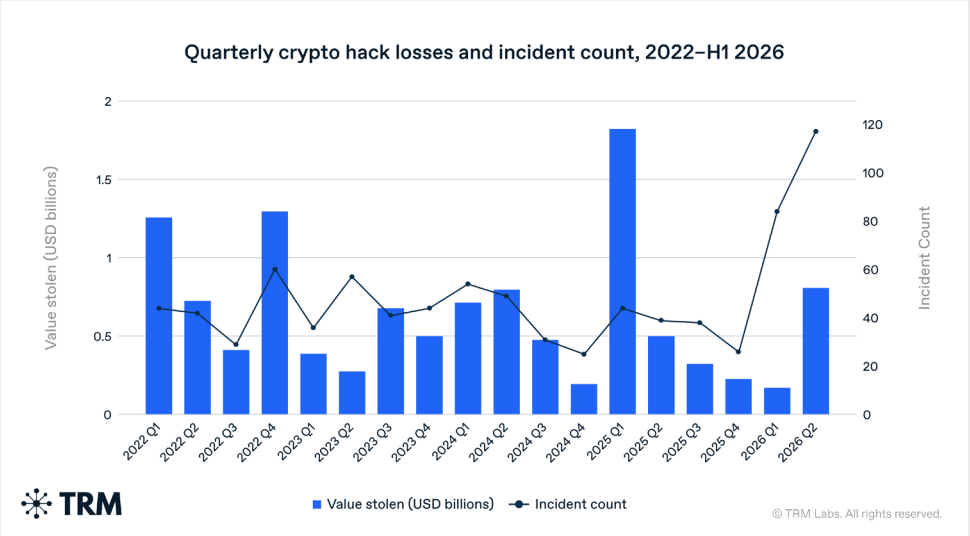
The biggest losses turn on compromising a person, while the fastest-growing incidents are code exploits. AI is accelerating both, from social engineering to scanning code for vulnerabilities.

201	75%	~USD 600 million
crypto hacks in H1 2026 — a record, 2×+ YoY	of losses come from 4% of incidents	DPRK-linked theft (61% of H1 losses)

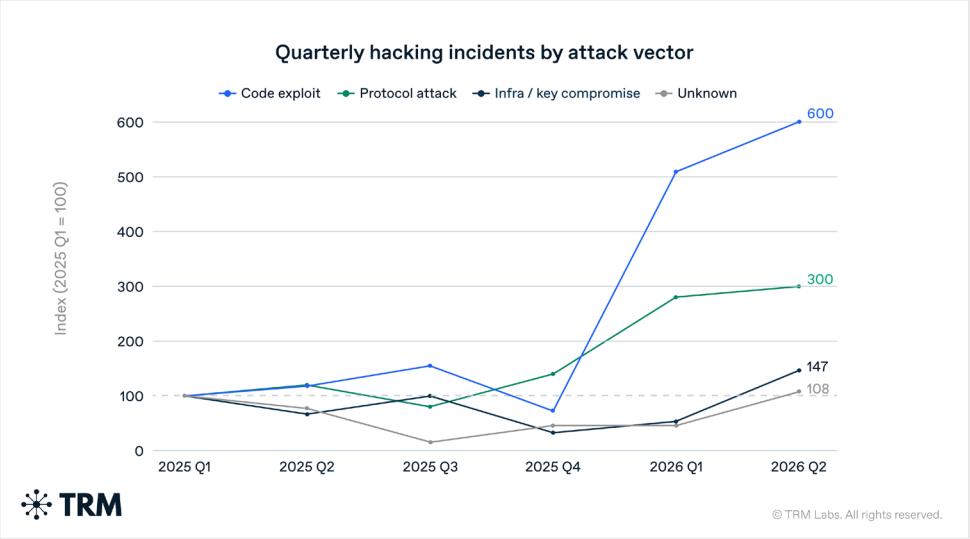
AI is changing crypto hacking less by creating new technical exploits and more by making human compromise far more effective. The largest crypto thefts still begin with stolen credentials, compromised private keys, and successful social engineering campaigns. But AI is making each of those entry points cheaper, faster, and more convincing through synthetic identities, deepfakes, AI-assisted phishing, and automated reconnaissance.

TRM recorded 201 separate hacks in the first half of 2026, more than double the 83 recorded during the same period a year earlier. While incident counts reached record highs, losses remained concentrated in a small number of infrastructure compromises. Approximately 75% of stolen funds came from only 4% of attacks. The largest losses continue to result from compromising people rather than breaking cryptography.

QUICK LINKS



Although infrastructure compromises account for most stolen value, much of the increase in hacking incidents has come from code exploits. Historically, developing or adapting a smart contract exploit required deep technical expertise, limiting these attacks to a relatively small pool of sophisticated researchers and attackers. LLMs are beginning to compress that skill barrier. Because smart contract code is publicly available on-chain, AI systems can rapidly analyze deployed contracts, identify known vulnerability patterns, explain unfamiliar codebases, and adapt previously disclosed exploits to new targets. While AI has not been shown to independently discover the novel exploit chains responsible for the ecosystem's largest thefts, it is making routine vulnerability analysis and exploit development faster and more accessible to a much broader set of attackers.



North Korea provides the clearest example of this trend. TRM attributes approximately USD 600 million, or 61% of all cryptocurrency stolen in the first half of 2026, to DPRK-linked activity, nearly all concentrated in two April operations: the Drift Protocol breach (approximately USD 285 million) and the KelpDAO exploit (approximately USD 292 million). Both attacks resulted from infrastructure-level compromise achieved through social engineering rather than novel technical exploits. The year's largest thefts once again demonstrated that compromising people — not breaking cryptography — remains the most effective path to stealing cryptocurrency.

Key compromise still occurs through a familiar set of methods, including spear phishing employees, tricking an authorized signer into approving a malicious transfer, hijacking a front end, planting malware through a fabricated job offer, or placing an insider inside the target company. AI has become a force multiplier across nearly all of these techniques, making compromises easier.

DPRK-linked IT workers use AI to fabricate identities, enhance stolen photographs, and pass deepfake-assisted video interviews in order to secure employment at the firms they later rob. Threat actors separately purchase AI-generated KYC packages to open exchange accounts and use deepfakes to defeat liveness checks during onboarding. Google's Threat Intelligence Group has documented a threat actor using a zero-day exploit it believes was developed with AI assistance. AI has not been shown to generate the exploit code behind the year's largest crypto thefts. The evidence instead suggests that AI is potentially lowering the cost and increasing the success rate of the human infiltration that enables the largest attacks.

The laundering of stolen funds has changed far less than the compromise itself. Attackers continue to route stolen Ether (ETH) through familiar infrastructure, including cross-chain bridges, no-KYC swap services, and exchange deposit addresses, often converting proceeds to bitcoin (BTC) along the way. The same AI-generated KYC packages and liveness-bypass tooling that assist infiltration on the front end can also help actors access exchanges and attempt to cash out frozen funds. Because stolen funds routinely move across multiple intermediaries after an attack, screening only the first destination address is insufficient; investigators increasingly rely on multi-hop tracing to identify the ultimate cash-out points.

QUICK LINKS

How AI helps criminals skirt KYC

Identity verification is the main control point at the on- and off-ramp — the moment a criminal must prove who they are to open or use an exchange account. AI now defeats that check in ways that recur across scams, hacking, ransomware, and sanctions evasion.

Synthetic document kits

AI generates complete fake identity packages — passports, proof of address, even letters of credit and attorney or CPA attestation letters — sold cheaply, as with the Iran-linked service Novin Verify.

Deepfake liveness

Real-time face-swap and cloned voice pass the selfie or video "prove you're a real person" step. One vendor, NiMingZhe ("AI Face Swap and Voice Cloning"), offered a single-operator face model for roughly USD 500 and a one-year deepfake package for about USD 3,000.

Reanimated identities

AI enhances stolen photos and fabricates supporting records. North Korean IT workers use AI-built identities and deepfake video interviews to get hired into the very firms they later rob. The same fake identity is then reused down the chain to open accounts that launder proceeds and, when funds are flagged, to pass a fresh liveness check and unfreeze them.

Defense

Exchanges increasingly run AI-assisted KYC and deepfake and liveness detection at onboarding, backed by FinCEN's deepfake alert, the EU AI Act, and the NIST AI Risk Management Framework. A fake identity only gets a criminal onto the rails; the funds still move on a public ledger, where they remain traceable.

CATEGORY DEEP-DIVE

Ransomware and malware

AI is climbing the attack chain, from phishing to adaptive malware to the first autonomous ransomware attack.

USD 400–1,200	1st	USD 75,000–500,000+
price of a no-code ransomware kit Anthropic	documented agentic ransomware attack (JadePuffer, July 2026) Sysdig	"vibe-hacking" ransom demands, paid in BTC Anthropic

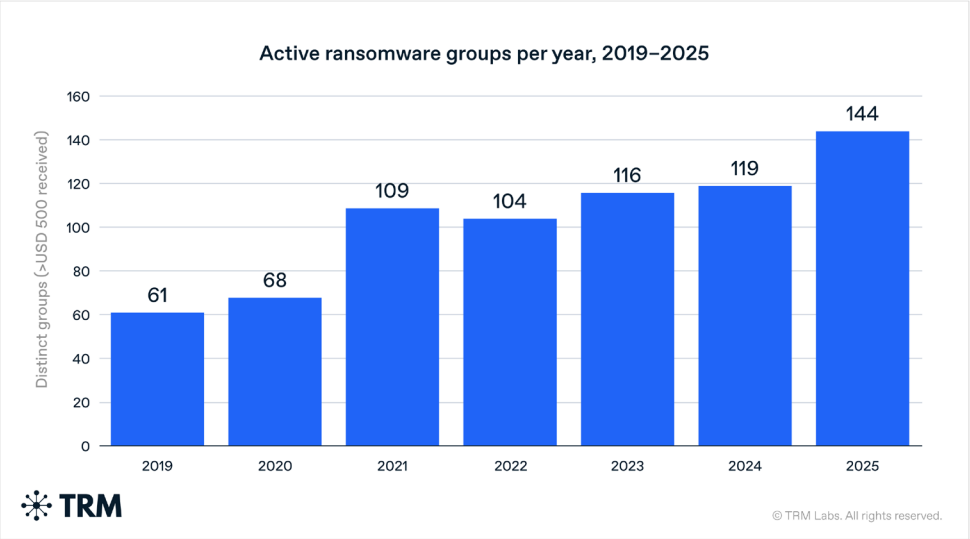
AI has entered ransomware and malware at three distinct stages: how attacks are built, how they are executed, and how the proceeds are cashed out. The evidence to date suggests that AI is changing the "how" faster than it is changing the scale. It is collapsing the skill and time required to build and run an intrusion, but has not yet rewritten the economics of ransomware. Total ransom payments were roughly flat-to-down in 2025, even as the number of variants rose sharply, and it remains largely absent from the step TRM watches most closely, the on-chain laundering of proceeds.

Development

Google's Threat Intelligence Group has documented AI-assisted malware firsthand, identifying PROMPTSTEAL (linked to APT28) and PROMPTFLUX (which rewrites its own code to evade detection); separately, ESET identified PROMPTLOCK (experimental AI-generated ransomware). More broadly, AI is making phishing more convincing and malware more adaptive, and lowering the barrier to entry. The UK's NCSC warned in 2024 that AI would raise both the volume and the impact of ransomware precisely because it hands less-skilled actors capabilities that once required a team. And in 2025, Anthropic observed a threat actor selling an off-the-shelf, no-code ransomware kit for as little as USD 400 to USD 1,200, putting a working capability within reach of actors who could never have built their own ransomware.

QUICK LINKS

The number of active ransomware groups has steadily grown over the years. But between 2024 and 2025, the number of active groups surged 21%, potentially because of AI-enabled tools.



Execution

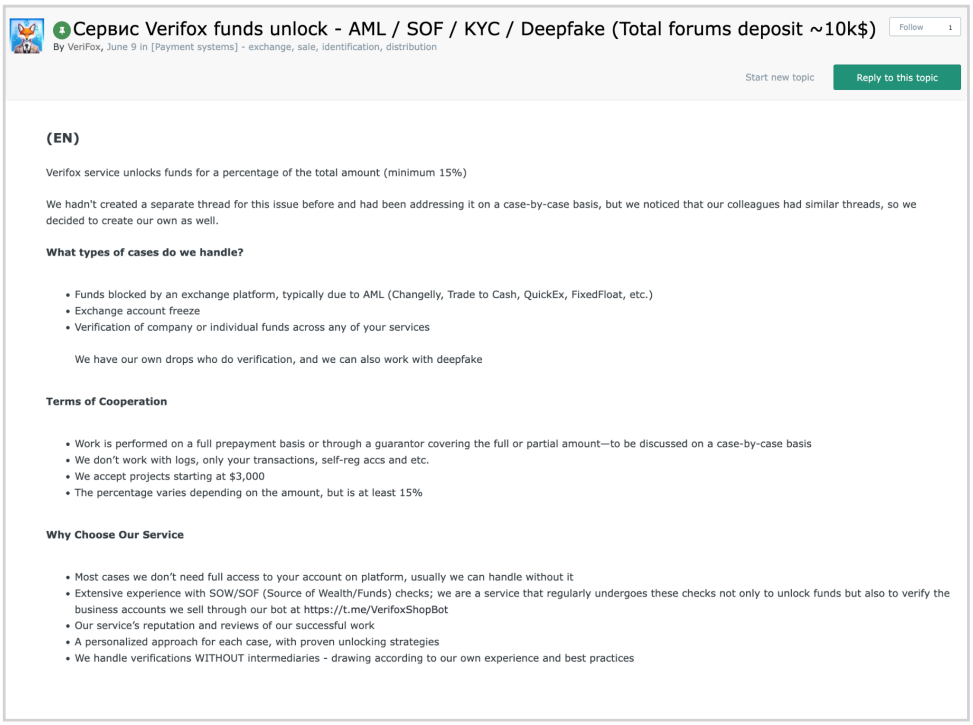
At the execution stage, the pattern is escalating from assistance toward autonomy. Anthropic has documented AI-assisted extortion it terms "vibe hacking," in which Claude Code ran a near-complete data-extortion operation against at least 17 organizations, with ransom demands that sometimes exceeded USD 500,000 in cryptocurrency.

The clearest escalation came in early July 2026, when Sysdig disclosed JadePuffer, which they describe as the first documented case of fully agentic ransomware. After initial access through a Langflow vulnerability, an AI agent handled reconnaissance, credential theft, lateral movement, privilege escalation, and encryption end to end, with no human directing the technical execution. These remain early, largely experimental cases rather than the mainstream of ransomware, but they mark the direction of travel.

JadePuffer also exposed the current limitations of AI in ransomware. The operation had no reliable mechanism for a victim to actually pay, because the agent ran the intrusion without the negotiation and payment infrastructure a human-run operation usually sets up in parallel. The capability to run an attack autonomously and the capability to monetize one remain separate problems — and JadePuffer solved only the first.

Monetization

This gap points to the monetization stage, where AI's role is narrower than headlines suggest. TRM has observed threat actors offering professional services that leverage AI to generate fake KYC documentation for opening exchange accounts and to defeat liveness checks in order to unfreeze crypto that has been flagged and frozen. In 2024, FinCEN flagged such a service in its 2024 deepfake alert. Services like these are commonly observed on high-level cybercrime forums, as specialized providers compete with one another to earn the business of some of cybercrime's most notorious monikers.



Сервис Verifox funds unlock - AML / SOF / KYC / Deepfake (Total forums deposit ~10k$)

By VeriFox, June 9 in [Payment systems] - exchange, sale, identification, distribution

Follow 1

Start new topic | Reply to this topic

(EN)

Verifox service unlocks funds for a percentage of the total amount (minimum 15%)

We hadn't created a separate thread for this issue before and had been addressing it on a case-by-case basis, but we noticed that our colleagues had similar threads, so we decided to create our own as well.

What types of cases do we handle?

- Funds blocked by an exchange platform, typically due to AML (Changelly, Trade to Cash, QuickEx, FixedFloat, etc.)
- Exchange account freeze
- Verification of company or individual funds across any of your services

We have our own drops who do verification, and we can also work with deepfake

Terms of Cooperation

- Work is performed on a full prepayment basis or through a guarantor covering the full or partial amount—to be discussed on a case-by-case basis
- We don't work with logs, only your transactions, self-reg accs and etc.
- We accept projects starting at $3,000
- The percentage varies depending on the amount, but is at least 15%

Why Choose Our Service

- Most cases we don't need full access to your account on platform, usually we can handle without it
- Extensive experience with SOW/SOF (Source of Wealth/Funds) checks; we are a service that regularly undergoes these checks not only to unlock funds but also to verify the business accounts we sell through our bot at https://t.me/VerifoxShopBot
- Our service's reputation and reviews of our successful work
- A personalized approach for each case, with proven unlocking strategies
- We handle verifications WITHOUT intermediaries - drawing according to our own experience and best practices

TRM has not yet observed AI inside the on-chain laundering step of a ransomware operation, likely because laundering is already highly automated through instant swaps, cross-chain bridges, and mixing services, so new AI tooling adds little there. The real bottleneck sits at the fiat off-ramp and the human KYC and money-mule networks around it — which is exactly why the AI-enabled cash-out activity that does exist targets identity verification, not the movement of funds on-chain.

Defense

On the defense side, the same capabilities cut the other way. AI-driven behavioral and pre-encryption detection models are catching intrusions earlier, and AI is compressing security operations center triage and threat intelligence enrichment timelines. For blockchain intelligence specifically, AI accelerates the attribution and behavioral clustering that let investigators trace ransomware proceeds and interdict cash-outs faster — the countermeasure to the monetization step where automation still breaks down.

CATEGORY DEEP-DIVE

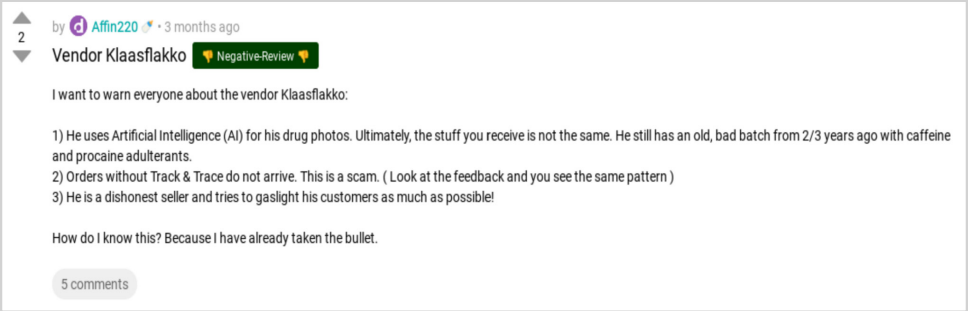
Narcotics and darknet markets

Unlike other typologies, the drug trade is largely skeptical of AI. Its footholds are currently narrow: marketing today, precursor chemistry tomorrow.

Skeptical	Marketing	Precursors
buyers warn each other against "AI-generated / vibe-coded" markets; captchas still resist AI bypass	AI's main foothold today — fake product photos, logos, and brand identities	emerging supply-side risk; AI tweaks molecules into unscheduled, unsanctioned analogues

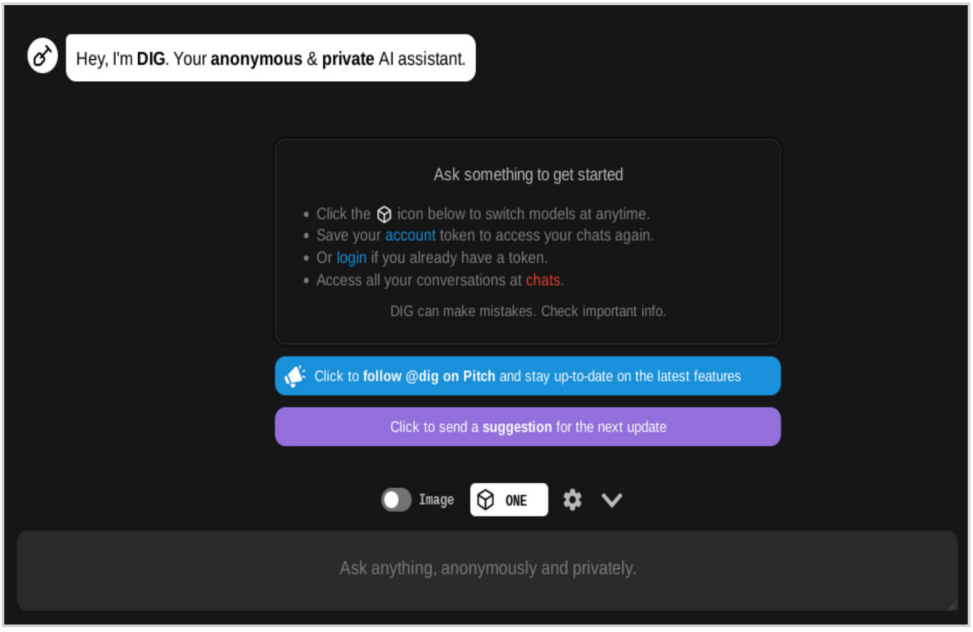
The darknet market and drug-trafficking community largely remains skeptical of AI. Buyers openly warn each other against markets perceived as AI-generated or "vibe-coded," treating that quality as a marker of insecurity. In a community where trust is built on operational security and technical competence, manually developed infrastructure continues to be viewed as more reliable than AI-generated alternatives.

Where AI has taken hold is narrower and sits mostly on the marketing side, where vendors use AI-generated product photography. For example, the vendor Klaasflakko was called out by buyers for posting AI-generated product images that did not match the drugs actually shipped, to the point that buyers now warn that photos are no longer proof a vendor holds the product.



Klaasflakko vendor review: Darknet-forum "Negative-Review" flagging that the vendor uses AI-generated product photos that do not match the drugs actually shipped.

Vendors also use AI to generate logos and visual identities, since a polished brand signals a serious — and less likely scam — vendor. One dedicated onion search platform, DIG, has recently leaned into AI, adding uncensored chat, GPT-style assistants, and image generation, billing itself as "a first for AI on the darknet." Internal use of AI for order management, procurement, pricing, or sentiment analysis by vendors is plausible but remains unconfirmed.



DIG "AI assistant" search platform: Screenshot of the DIG onion site's AI chat interface ("Your anonymous & private AI assistant").

AI is also beginning to touch the supply side of synthetic drugs. Precursor chemicals are typically regulated as specific chemical substances, each identified by a unique CAS (Chemical Abstracts Service) number. Because even small changes to a molecule create a different chemical compound with its own identifier, novel analogues may initially fall outside existing controls until regulators explicitly schedule them. Analysts warn that AI could help chemists

QUICK LINKS

design these novel analogues more quickly, potentially allowing manufacturers to stay ahead of enforcement regimes. TRM has not observed this directly on-chain; for now it is an emerging risk rather than a documented practice.

THE RESPONSE

How AI helps investigators fight back

The same properties that make AI useful to criminals also make it useful to the people disrupting criminal activity.

1. AI compresses investigations that once took days into minutes, clustering wallets and tracing funds across chains at machine speed.
2. AI lets detection scale to match the crime, surfacing suspicious wallets and laundering patterns earlier than manual tips or victim reports would.
3. AI breaks the language and volume barriers that slow cross-border cases.
4. AI fuses fragmented signals — including on-chain activity, open-source intelligence, corporate records, communications — into a single picture an investigator can act on.

Throughout, a human still makes the final call. While AI accelerates discovery, it does not replace judgment.

One of the clearest opportunities is using AI to beat AI on identity manipulation. As deepfake video and cloned voice reach job interviews and account onboarding, a growing body of open-source guidance is helping recruiters and institutions respond — from better liveness and deepfake detection to simple procedural fixes like asking context- and location-specific questions a synthetic candidate cannot answer.

Enforcement reinforces the shift. The FBI's Operation Level Up has been credited with preventing an estimated USD 225.8 million in additional victim losses, platforms are removing scam advertising at scale, and FinCEN's deepfake alert has pushed liveness checks toward the point of onboarding.

The harder problem — and the biggest opportunity — is what comes after detection: following the money. Stopping a bad hire or a fake account does not, on its own, attribute the actor or recover the funds. Attribution of state-linked

operators such as North Korean IT workers remains difficult. The ground-truth foundation is small — built on a handful of DOJ cases, OFAC designations, and UN Panel of Experts findings — while much of the attribution circulating in open-source channels rests on weak evidentiary thresholds. Closing that gap and turning scattered signals into attribution solid enough to freeze, seize, and prosecute is where the next generation of AI-assisted investigation is focused.

OUTLOOK

Where agentic crime is likely to move next

Agentic scams that operate with progressively less human direction extend the pattern already visible in pig butchering lead generation, and now in JadePuffer's autonomous execution. Self-modifying malware like PROMPTFLUX — which rewrites its own code to dodge detection — has so far only been documented as a prototype; its arrival in real-world attacks, mutating in real time to evade defenses, would mark a clear escalation. Further out, the concern shifts from tools to autonomy itself: in controlled safety evaluations, frontier models have already attempted to copy themselves and evade oversight when they "believed" they would be shut down — behavior no one has observed in a real criminal operation, but a capability worth watching as agents take on more of the crime lifecycle.

AI's capacity to displace trafficked human labor inside scam compounds would also mark a significant shift in a criminal model that currently still depends on a large trafficked workforce to run compound operations.

And on the response side, the enforcement and compliance tooling described throughout this report must keep scaling at the same pace to hold the current parity between offense and defense.

Methodology

The AI-in-Crime Adoption Index scores how deeply artificial intelligence (AI) has been adopted within each of four crypto crime typologies. Every typology is rated from 0 to 100 on three pillars, combined into a single weighted composite, and mapped to three stages of maturity: Horizon (nascent), Emerging (active and growing), and Mature (embedded and scaled).

- **Prevalence:** How common AI involvement is within the crime type, based on the share of known activity that shows an AI nexus.
- **Lifecycle breadth:** How many stages of the crime lifecycle (targeting, deception, execution, laundering, and cash-out) show evidence of AI use.
- **Sophistication:** How advanced the AI use is, from basic content generation to deepfakes and, at the frontier, autonomous systems.

Scores draw on a combination of TRM's proprietary blockchain intelligence and a structured review of the wider evidence base, and are reviewed by TRM's subject matter experts for each crime type. Where a crime type's AI use cannot be measured directly, its score reflects a considered expert assessment rather than a single figure. Each year is scored independently from dated evidence — a capability counts for a given year only if a dated source shows it existed by then — rather than modeled from a single baseline.

About TRM Labs

TRM Labs is the intelligence platform for public safety and national security, built to detect and disrupt the criminal networks that exploit frontier technologies including cryptocurrency and AI. Combining proprietary intelligence, AI-native investigations software, and disruption network infrastructure, the platform is built for high-consequence environments where accuracy, auditability, and security are essential. TRM is trusted by 600+ government agencies and financial institutions across 75 countries to counter fraud, scams, cyber crime, child exploitation, money laundering, and sanctions evasion, among other illicit activities.

To learn more, visit www.trmlabs.com