EDP ECOSYSTEM DEEP-DIVE

MODULE 13: MONEY LAUNDERERS AND EXCHANGES

Module Number	13
Module Name	Money Launderers and Exchanges
EDP Node Reference	Node 02 (primary): High-Risk/Non-Compliant Exchanges; cross-linkage Nodes 01, 08, 09
Ecosystem Layer	Crypto-to-Fiat Conversion / Exchange Off-Ramp
Upstream Connections	Crypto Mixers (Module 11 / Node 08); OTC Brokers (Module 12 / Node 01); Ransomware/RaaS Operations (Module 07)
Downstream Connections	Mule Networks (Module 14 / Node 09); Direct fiat withdrawal via bank wire, payment processors, local cash networks
Research Date	April 2026
Primary Researcher	Reno
Source Tools Used	Perplexity AI; Chainalysis; TRM Labs; CyberScoop/Wired; CryptoNews/Cointelegraph; Europol; academic literature (Tandfonline)
Handling	INTERAGENCY

CURRENCY NOTE (June 2026): The Garantex analysis in this module predates the Grinex collapse. OFAC designated Grinex, the Garantex successor exchange, in August 2025. In mid-April 2026, roughly 13.7 million USD was drained from approximately 70 Grinex addresses; the exchange halted operations and attributed the theft to Western special services without presenting evidence (CONFIRMED: Elliptic, TRM Labs, press reporting). Analytic read: the successor-exchange model survived designation but not sustained pressure, a live case exemplar for the Node 01/02 financial rails thesis. Re-baseline the cash-out landscape assessment at the next module revision.

SECTION 1: WHAT IT IS

Definition and Ecosystem Role

Cryptocurrency exchanges and their associated money launderers are the primary crypto-to-fiat conversion layer of the ransomware supply chain. They are the terminal interface between the illicit cryptocurrency world and the legitimate financial system — the point at which ransomware proceeds are converted to usable fiat currency, stablecoins, or alternative assets that can feed mule networks, OTC settlement, or direct banking. Node 02 is rated CRITICAL in the EDP Dependency Map alongside Node 01 (OTC Brokers): without a functional exchange-based off-ramp, ransomware proceeds remain stranded in cryptocurrency, subject to ongoing blockchain forensic tracing and OFAC pressure.

The exchange ecosystem for ransomware laundering encompasses three operationally distinct tiers: mainstream regulated centralized exchanges (CEXs) that receive criminal funds via straw-man accounts and nested OTC brokers despite active compliance programs; high-risk and sanctioned exchanges (Garantex/Cryptex-type) that provide permissive or fake KYC and operate under jurisdictional protection; and dedicated underground VASPs and nested exchanges whose core business is laundering for ransomware, fraud, and darknet markets.

[CONFIRMED] Chainalysis data for 2024 documents that centralized exchanges accounted for approximately 39% of all ransomware off-ramping — slightly above the 2020-2024 average of 37% — remaining the single

largest laundering category despite all enforcement activity against this tier. This persistence is the module's central analytical paradox: enforcement pressure on mixers and some exchanges increased ransomware actors' reliance on compliant CEXs (via intermediary layers) rather than eliminating it.

How It Functions: Canonical Ransom-to-Fiat Flow

The canonical 2024-2025 ransomware laundering flow, per Chainalysis and TRM Labs typologies:

- Step 1: Victim pays ransom to attacker-controlled wallet address, typically in Bitcoin or USDT. Payment addresses are generated by the ransomware implant or provided via negotiation interface.
- Step 2: Funds move through intermediary wallets using peel chains — small slices peeled off through a series of controlled addresses — combined with time delays and amount randomization to reduce simple heuristic attribution.
- Step 3: Optional obfuscation via mixers (declining share post-ChipMixer/Sinbad/Tornado enforcement) or increasingly via cross-chain bridges and DEX swaps (BTC to ETH, USDT, or TRX) to break chain-specific forensic heuristics.
- Step 4: Consolidated at CEX or high-risk exchange accounts controlled by money launderers or OTC broker nested desks. Accounts are opened using straw-man identities, forged KYC documents, or legitimate accounts purchased from mule account suppliers.
- Step 5: Final off-ramp — swap to fiat or local stablecoin, then withdraw via bank wire, payment processor, or local cash network. High-risk exchanges in permissive jurisdictions allow this step with minimal friction; at compliant CEXs it requires the mule/straw-man account layer.

[ANALYST INFERENCE] A documented behavioral adaptation: CyberScoop reporting notes that some ransomware operators let crypto "sit in wallets" for extended periods rather than moving funds to exchanges — indicating that tracing risk at exchange off-ramps is producing a behavioral deterrence effect consistent with the EDP Phase A mechanism. Funds parked in wallets are not yet converted to usable criminal proceeds, representing a partial enforcement win even before formal OFAC action.

Why Exchanges Remain the Dominant Off-Ramp

Three structural factors sustain exchange dominance in ransomware laundering despite sustained enforcement. First, liquidity: deep order books at major CEXs allow large ransom amounts (six to seven figures) to be converted with minimal slippage — a capability that mixers, OTC brokers, and DEXs cannot replicate at equivalent scale and speed. Second, jurisdictional coverage: the global distribution of exchange operators creates a persistent regulatory arbitrage gap where enforcement in one jurisdiction pushes activity to permissive alternatives rather than eliminating it. Third, the nested intermediary model: money launderers and OTC brokers insert themselves between ransomware operators and exchange accounts, absorbing KYC risk and allowing compliant CEXs to process illicit flows without directly implicating the exchange.

[CREDIBLE] Chainalysis notes a concentration risk pattern: for high-risk exchange categories, bridges, and sanctioned entities, a small number of services capture a disproportionately high share of ransomware flows. This concentration makes these services strategic chokepoints — OFAC designation of a single dominant high-risk exchange produces ecosystem-wide disruption disproportionate to the size of the designated entity.

SECTION 2: KEY ACTORS AND EXAMPLES

Exchange Tiers and Named Actors

Tier / Actor	Type	Ransomware Exposure / Key Facts	Enforcement Status	Confidence
Mainstream regulated CEXs (archetype)	Large compliant exchanges (Binance, Kraken,	39% of ransomware off-ramping in 2024 (Chainalysis); primary off-ramp despite	Active OFAC cooperation; blockchain	**[CONFIRMED]** High — Chainalysis

	Coinbase and equivalents) that receive ransomware flows via straw-man and mule accounts, nested OTC desks, and forged KYC	compliance programs; illicit flows exploited via intermediary account layers rather than direct attacker deposits	analytics integration; but structural vulnerability via nested OTC desk model and straw-man account supply	aggregate data; well-documented structural vulnerability
Garantex	Russian exchange with documented ransomware laundering role; ruble liquidity; permissive KYC; state-adjacent operation	Laundered >$2.3M in Ryuk proceeds; processed significant Conti and LockBit flows; "played a key role in laundering ransomware proceeds" (TRM Labs); high-volume illicit flow hub for Russian-speaking groups	OFAC designated April 2022; Europol-led physical shutdown April 2025; servers seized, domain redirected; operators charged	**[CONFIRMED]** High — US government designation; Europol enforcement documentation; TRM Labs case study
Cryptex (Cryptex.net)	Sanctioned high-risk exchange used by ransomware groups including Embargo; permissive compliance environment	Embargo ransomware moved >$1M through Cryptex from a tracked $34M in ransom-linked crypto (April 2024 to mid-2025); cited in Chainalysis as persistent high-risk node	OFAC sanctioned; enforcement action contributed to 2024 ransomware payment decline (Chainalysis attribution)	**[CONFIRMED]** High — OFAC designation documented; TRM/Cointelegraph case study
Nested / underground VASPs (archetype)	Smaller dedicated laundering exchanges and nested accounts; marketed to cybercriminals on underground forums; core business is illicit conversion	Run clusters of exchange accounts across multiple CEXs; use peel chains, micro-withdrawals, cross-chain services; market "no-KYC" and "sanctions-proof" services on forums and OTC networks	Rarely designated individually; disrupted via upstream exchange account suspension, OFAC action against parent exchange, or LE-coordinated account freeze operations	**[CREDIBLE]** Moderate-High — archetype well-documented; individual operator identification infrequent

Comparative Role Table: Exchanges vs. Mixers vs. OTC Brokers

Service	Primary Function	2024 Ransomware Share	Replace Difficulty	Primary Enforcement Tool
Centralized exchanges (compliant CEX)	Fiat conversion via straw-man / nested OTC accounts; deep liquidity; global reach	**~39%** of ransomware off-ramping (Chainalysis)	**HIGH** — liquidity and jurisdictional distribution create high redundancy	Nested account suspension; OFAC designation of complicit exchange operators; blockchain analytics compliance integration
High-risk / sanctioned	Permissive fiat conversion hub; ruble	Significant	**HIGH** —	OFAC designation followed by physical

exchanges (Garantex model)	liquidity; state-adjacent protection	share within the 39% CEX total; Garantex Ryuk exposure alone >$2.3M	jurisdictional protection; physical shutdown requires multi-agency coordination	enforcement (Europol model); operator prosecution
Crypto mixers (ChipMixer / Sinbad archetype)	Obfuscation layer; not a fiat conversion point; feeds exchanges/OTC	Historically 10-15%; dropped significantly in 2024 post-enforcement; flows shifted to bridges and CEXs	**MEDIUM** — replaced by bridge/DEX stacking but detection improving	OFAC designation; operator prosecution (2025 Blender/Sinbad indictments); BPH disruption
OTC brokers	Relationship-based fiat conversion; absorbs KYC risk for exchanges; consultative cash-out	Acts as intermediary to exchange deposits; not separately counted in Chainalysis 39% (flows attributed to exchange end-point)	**HIGH** — trust-dependent; see Module 12	OFAC designation; Tether/T3 Unit blacklisting; operator prosecution; local banking disruption
Cross-chain bridges and DEXs	Pre-exchange obfuscation; chain-hopping to break forensic heuristics	Increasing share as mixer alternative; feeds CEX deposits; APT and high-value ransomware preferred method	**HIGH** — decentralized; Tornado Cash precedent for OFAC action on smart contracts	OFAC designation of bridge smart contracts; voluntary compliance pressure on front-end providers; blockchain analytics monitoring

Embargo Ransomware Case Study: Exchange Flow Documentation

[CONFIRMED] TRM Labs and CryptoNews documented a detailed flow for Embargo ransomware activity from April 2024 through mid-2025. Total ransom-linked crypto tracked: approximately $34M. Approximately $13.5M moved through various VASPs at various stages of the laundering chain. More than $1M transited through Cryptex.net — a sanctioned high-risk exchange — before further distribution. The case illustrates how a mid-tier ransomware group (Embargo had a significantly smaller victim footprint than LockBit or RansomHub) still accessed sanctioned exchange infrastructure for a meaningful share of its laundering volume.

[CONFIRMED] Garantex documentation by TRM Labs establishes the exchange as a systemic node rather than an incidental participant: Ryuk ransomware alone laundered more than $2.3M through Garantex; the exchange also processed significant flows from Conti and LockBit, the two largest ransomware programs by revenue during their operational periods. Garantex's role as a ruble-liquidity hub for Russian-speaking cybercriminal groups — combined with its FSB-adjacent state protection — made it the clearest available proof of concept for the EDP Phase A exchange disruption model.

SECTION 3: INFRASTRUCTURE DEPENDENCIES

Upstream Dependencies

Mixing and obfuscation layer (Node 08 / Module 11): Mixer outputs feed exchange deposits after obfuscation. Post-enforcement (ChipMixer 2023, Sinbad 2023), the share of mixer-to-exchange flows declined; cross-chain bridge-to-exchange flows increased to compensate. Mixer disruption pushes flows toward exchanges with less obfuscation, increasing forensic traceability at the exchange deposit point.

OTC brokers and nested desks (Node 01 / Module 12): OTC desks operate nested accounts within CEXs, absorbing KYC compliance risk on behalf of ransomware operators. From the exchange's perspective, the deposit comes from a (sometimes legitimate-appearing) OTC account; from the forensic perspective, the chain traces back to ransomware wallets. OTC disruption forces ransomware operators to interact with exchange KYC directly or use lower-quality straw-man accounts.

Cross-chain bridges and DEXs: Increasingly used as pre-deposit layering between ransomware wallets and exchange accounts. Chainalysis notes that private-key compromise incidents (APT-linked heists and some ransomware) prefer bridges and mixers, while other ransomware attack vectors lean more on DEXs and direct exchange deposits. Bridge disruption (OFAC designation of smart contracts) reduces this layering option and increases forensic visibility of exchange deposits.

Underground forums (Node 07 / Module 10): Nested and underground VASP operators advertise services on Exploit, XSS, and RAMP. Forum disruption degrades the primary discovery channel for criminal-facing exchange services — reducing new criminal client acquisition for underground VASPs.

Downstream Dependencies

Mule networks (Node 09 / Module 14): Exchange-to-fiat conversion proceeds feed mule network accounts for layering and integration. The exchange is the bridge between the crypto and fiat worlds; mule networks handle the fiat-side layering after withdrawal. Exchange off-ramp disruption reduces the fiat volume entering mule pipelines.

Local banking relationships: High-risk exchanges depend on maintaining correspondent banking access for fiat withdrawal. Banking de-risking pressure — where correspondent banks terminate relationships with high-risk exchanges following OFAC designation — is a force multiplier for exchange enforcement that does not require direct seizure.

Stablecoin issuers (Tether/USDT, Circle/USDC): Stablecoin conversion at exchanges is an increasingly common intermediate step before fiat withdrawal. Tether blacklisting authority (demonstrated in the Khinkis/Module 12 context) and Circle's equivalent USDC freeze capability can intercept stablecoin holdings at exchange accounts before fiat withdrawal.

Critical Chokepoints

Chokepoint	Description	Primary Owner	Disruption Method
High-risk exchange OFAC designation	Designation of a dominant high-risk exchange creates secondary sanctions risk for any bank, exchange, or VASP transacting with the designated entity; forces criminal clients to find alternatives	Treasury / OFAC; FVEY financial partners	SDN designation; proactive sharing of designated wallet clusters with major exchange and banking compliance teams; secondary sanctions engagement for non-US entities
Physical exchange infrastructure seizure	Server seizure and domain takeover (Garantex model) produces more durable disruption than designation alone for RU-domiciled exchanges that continue operating post-designation	Europol; DOJ; partner jurisdiction LE; coordinated FVEY action	Multi-agency physical enforcement following OFAC designation; operator arrest where jurisdiction permits; server and domain seizure

Straw-man and mule account supply to CEXs	Ransomware operators' access to compliant CEX liquidity depends on a continuous supply of straw-man and mule accounts; disrupting this supply forces direct KYC exposure	FinCEN; FVEY LE; major CEX compliance teams; behavioral biometrics providers (BioCatch)	Behavioral biometrics account classification at exchange onboarding; enhanced KYC for high-risk account patterns; coordinated account suspension programs
Correspondent banking access for exchange fiat withdrawal	High-risk exchanges depend on correspondent banks for fiat withdrawal; banking de-risking following OFAC designation cuts the fiat pipeline without requiring exchange seizure	FVEY financial intelligence units; correspondent bank compliance teams; FinCEN	Correspondent bank de-risking pressure; FinCEN guidance; proactive sharing of designated exchange wallet clusters with banking compliance teams
Nested OTC desk account clusters within CEXs	OTC broker nested accounts at compliant CEXs are the primary mechanism for moving ransomware funds through exchanges without triggering direct compliance flags	FVEY LE; major CEX compliance teams; blockchain analytics vendors	Blockchain analytics-flagged nested-desk transaction pattern sharing with exchange compliance; subpoenas for identified nested-desk account operators; coordinated account suspension

Cross-Module Linkages

Module	Node	Linkage Type	Direction	Description
07 Ransomware / RaaS	Cross-cutting	Primary supply	Upstream	Ransomware payment receipts are the primary input; attacker cash-out demand drives the entire exchange off-ramp ecosystem
11 Crypto Mixers	08	Pre-exchange obfuscation	Upstream	Mixer outputs feed exchange deposits; mixer disruption shifts flows toward direct bridge-to-exchange paths with less obfuscation; improving detection at deposit point
12 OTC Brokers	01	Nested account intermediary	Upstream / Parallel	OTC nested desks operate inside exchanges and absorb KYC risk; OTC designation forces ransomware operators toward direct exchange KYC exposure or lower-quality straw-man accounts
10 Underground Forums	07	Criminal marketing	Upstream	Underground VASPs and nested exchanges advertise on top-tier RU forums; forum disruption degrades new criminal client acquisition for criminal-facing exchange services
14 Mule Networks	09	Downstream fiat layering	Downstream	Exchange fiat withdrawals feed mule network pipelines for layering and integration; exchange off-ramp disruption reduces fiat volume reaching mule networks
09 BPH	03	Infrastructure	Upstream (criminal-side)	BPH supports underground VASP web infrastructure and forum advertising; BPH disruption degrades the discovery and access layer for criminal-facing exchange services

SECTION 4: DISRUPTION LEVERAGE POINTS

Primary Leverage Points

Lever	Owner	Best Method	Backfire Risk	EDP Phase
OFAC designation of high-risk exchanges and exchange operators	Treasury / OFAC; FVEY financial partners	SDN designation of exchange entity and associated wallet clusters; proactive sharing with banking and exchange compliance teams; secondary sanctions engagement for non-US correspondent banks transacting with designated exchanges	**LOW** — validated: Garantex 2022, Cryptex 2024; each designation produced measurable flow disruption	Phase A — primary action; concentration risk makes each designation high-impact
Physical exchange infrastructure seizure (Europol model)	Europol; DOJ; partner jurisdiction LE; FVEY coordination	Server seizure and domain takeover following OFAC designation; operator arrest; coordinated multi-jurisdiction action for exchanges operating across multiple countries	**LOW** — Garantex April 2025 shutdown is the validated template; three-year gap between designation and seizure shows designation alone is insufficient for RU-domiciled exchanges	Phase A — high-impact, longer-cycle; requires physical jurisdiction
Blockchain analytics compliance integration at CEXs	Private sector (Chainalysis, TRM Labs, Elliptic); FinCEN; major CEX compliance teams	Real-time screening of deposit addresses against ransomware wallet clusters and mixer/bridge output patterns; automatic hold on high-risk deposits pending enhanced review; OFAC address screening mandates	**LOW** — systematic force multiplier for every OFAC designation; extends functional reach beyond formal SDN list	Phase A — ongoing; structural compliance mechanism
Correspondent bank de-risking for high-risk exchange fiat withdrawal	FVEY financial intelligence units; FinCEN; correspondent bank compliance teams	Proactive sharing of designated exchange wallet clusters with banking compliance; FinCEN guidance on high-risk exchange categories; correspondent bank de-risking pressure following designation	**LOW** — cuts fiat pipeline without requiring direct exchange seizure; force multiplier for OFAC designation	Phase A — compound action; follows OFAC designation
Straw-man account supply disruption at compliant CEXs	FinCEN; major CEX compliance teams; behavioral biometrics providers	Behavioral biometrics and account behavior modeling to identify straw-man and mule account patterns at CEX onboarding; coordinated account	**LOW** — degrades ransomware operators' access to compliant CEX	Phase A — continuous; structural compliance mechanism

		suspension programs; enhanced KYC for account patterns associated with nested OTC desk operations	liquidity without requiring direct LE action against the exchange	
Bridge and DEX protocol compliance pressure	OFAC; FVEY financial regulators; bridge and DEX front-end operators	OFAC designation of bridge smart contracts (Tornado Cash precedent); voluntary compliance pressure on front-end providers to block designated addresses; blockchain analytics integration for bridge deposit monitoring	**MEDIUM** — decentralized protocols are technically durable; front-end compliance is the practical chokepoint; legal challenges to smart contract designation ongoing	Phase A/B — compound; reduces pre-exchange obfuscation layer

Compounding Actions

- The concentration risk pattern documented by Chainalysis is the primary targeting argument: when a small number of high-risk exchanges capture a disproportionate share of ransomware flows, each designation produces ecosystem-wide disruption disproportionate to the size of the designated entity. OFAC should prioritize identification and designation of the current dominant high-risk exchange rather than distributing enforcement effort across many smaller services.
- Coordinate Node 02 (exchange) designation with simultaneous Node 01 (OTC broker) action. Designating an OTC broker while the exchange hosting its nested accounts remains operational creates displacement, not disruption. Simultaneous or closely sequenced pressure on both nodes closes both primary off-ramp channels at once — the mechanism consistent with the 2024 payment decline.
- The three-year gap between Garantex's OFAC designation (April 2022) and physical shutdown (April 2025) demonstrates that designation-only action is insufficient for RU-domiciled exchanges. Policy should institutionalize a physical enforcement follow-up track for designated RU-based exchanges with confirmed continued operation post-designation.
- Mixer enforcement compounds exchange targeting: ChipMixer and Sinbad enforcement reduced mixer obfuscation coverage, pushing ransomware flows toward bridges and direct exchange deposits with less obfuscation. Each additional mixer enforcement action slightly increases the forensic traceability of funds reaching exchange accounts.
- Extend the Garantex-successor identification task (established in Module 12) to include exchange-tier successors. The same ruble-liquidity gap created by Garantex's April 2025 shutdown applies at the exchange level; the successor exchange is the next Phase A designation priority.

SECTION 5: RESILIENCE AND REPLACE DIFFICULTY

Replace Difficulty Assessment

Node 02 carries a HIGH replace difficulty rating in the EDP Dependency Map — the highest tier alongside Nodes 01 (OTC Brokers) and 03 (BPH). This rating reflects the structural factors that make exchange-based fiat conversion difficult to replace: liquidity depth (large CEXs provide fiat conversion capacity that mixers, OTC desks, and DEXs cannot replicate), global jurisdictional distribution (enforcement in one jurisdiction pushes activity to alternatives rather than eliminating it), and the persistent demand for fiat currency (cryptocurrency proceeds that cannot be converted to fiat provide limited criminal utility).

The key distinction within the HIGH aggregate rating is between compliant CEXs (which are highly resilient because they cannot be designated without disrupting legitimate operations) and high-risk/sanctioned exchanges (which are medium-difficulty to replace, since they provide specialized permissive services that take time to rebuild in a new entity). The Garantex-to-successor gap is the empirical test: how long does it take the criminal ecosystem to identify and trust a new dominant high-risk exchange following a physical takedown?

Exchange Tier	Replace Difficulty	Key Durability Driver	Key Vulnerability	Recovery Timeline
Compliant CEXs (accessed via straw-man and nested OTC accounts)	**HIGH**	Deep liquidity; global availability; CEXs cannot be wholesale designated; jurisdictional redundancy means one CEX restriction shifts flows to another	Straw-man account supply disruption; nested OTC desk account suspension; behavioral biometrics improving detection of mule/straw-man patterns at onboarding	No recovery needed — CEX tier is essentially always available; enforcement must target the account supply mechanism, not the exchange itself
High-risk / sanctioned exchanges (Garantex model)	**MEDIUM-HIGH**	Jurisdictional protection (RU-based); ruble liquidity; established criminal client trust; state-adjacent operation creating de facto immunity from designation enforcement pre-physical-shutdown	Physical enforcement (Europol model); operator prosecution; correspondent bank de-risking following designation; ruble liquidity gap creates period of client displacement	Months to potentially over a year for a new dominant high-risk exchange to emerge and establish equivalent criminal client trust — the Garantex successor gap as test case
Nested / underground VASPs	**MEDIUM**	Low profile; no physical infrastructure to seize; accounts distributed across multiple CEXs; forum-based reputation enables client acquisition for new operators	Account cluster identification and suspension; parent exchange enforcement; forum reputation disruption removes primary advertising channel	Weeks to months for individual underground VASP operators; but replacement by equivalent operators is relatively rapid given low barrier to entry

Historical Reconstitution Record

Exchange	Disruption Event	Date	Reconstitution / Outcome	Notes
BTC-e	DOJ seizure; Alexander Vinnik indictment	2017	WEX.nz emerged as partial successor; collapsed 2018; no equivalent-scale replacement established	Operator prosecution produced more durable disruption than designation alone; criminal community fragmented across multiple alternatives
SUEX	OFAC designation — first crypto exchange designated	September 2021	Criminal clients migrated to Garantex, Cryptex, and alternatives within weeks to months	Established OFAC designation framework; displacement to Garantex confirmed migration pattern
Garantex	OFAC designation followed by Europol-led physical shutdown	April 2022 / April 2025	Post-designation continued operating within Russia for three years; 2025 physical shutdown created ruble-liquidity gap; Garantex successor identification is active intelligence priority	Critical lesson: designation-only insufficient for RU-domiciled exchanges; physical enforcement required; three-year operational continuation post-designation demonstrates limits of sanction-only approach
Cryptex	OFAC designation	2024	Cited as contributing factor in 2024 ransomware payment decline; Embargo case documents >$1M in tracked flows through Cryptex pre-designation	Part of coordinated Phase A action that produced measurable 35% payment decline; concentration risk means designation of even one significant exchange produces ecosystem-wide effect

The "Wallet Sitting" Behavioral Adaptation

[CREDIBLE] CyberScoop reporting documents a notable behavioral adaptation: some ransomware operators are allowing crypto proceeds to sit in wallets for extended periods — or refraining from moving funds entirely — rather than risking tracing when interacting with exchanges. This "wallet sitting" behavior represents a partial enforcement win: funds parked in cryptocurrency are not yet converted to usable criminal proceeds, and extended wallet dwell time increases the forensic window available for blockchain analytics attribution before cash-out.

[ANALYST INFERENCE] If "wallet sitting" becomes structurally prevalent, it suggests the Phase A exchange enforcement mechanism is producing a deterrence effect that extends beyond the specific designated entities — ransomware operators are modifying behavior in response to the perceived tracing risk at exchange off-ramps generally, not just at designated exchanges specifically. This would represent a positive behavioral externality from targeted enforcement that the EDP framework should track as an indicator of ecosystem-wide pressure effectiveness.

SECTION 6: INDICATORS AND KPIs

Ecosystem Health Indicators

Indicator	Normal State (2024-2025 Baseline)	Under Pressure / Degraded
CEX share of ransomware off-ramping (annual)	Approximately 39% in 2024; slightly above 37% 2020-2024 average (Chainalysis); persistent despite enforcement	Declining CEX share with corresponding increase in wallet dwell time (not in alternative channels) indicates effective pressure; increasing DEX/P2P share indicates adaptation rather than deterrence
Ransomware total revenue (annual, USD)	$813.55M in 2024 (down 35.82% from $1.25B in 2023); enforcement on exchanges and OTC cited as key driver	Continued year-over-year decline toward below $600M; directional decline sustained over two consecutive years
Mixer-to-exchange versus bridge-to-exchange flow ratio	Mixer share declined from 10-15% to lower level post-2023 enforcement; bridge/DEX share increasing as pre-exchange obfuscation layer	Increasing bridge-to-exchange ratio with declining obfuscation step count indicates forensic pressure driving attacker adaptation; monitor for bridge OFAC designation effectiveness
Active OFAC-designated exchange entities (cumulative)	SUEX (2021), Garantex (2022), Cryptex (2024) and others; designation pace accelerating	Enforcement tempo sustained at minimum 1-2 major exchange designations per year; no dominant high-risk exchange operating undesignated for more than 18 months
Ransomware wallet dwell time before exchange deposit (behavioral indicator)	Increasing dwell time documented in 2024 (CyberScoop); some operators "sitting on" funds; no precise baseline established in open sources	Increasing average dwell time signals effective deterrence at exchange off-ramps; decreasing dwell time signals new low-friction off-ramp discovered or enforcement pressure relaxed
Illicit volume proportion of total crypto volume	Dropped 51% in 2024 (TRM Labs) even as total crypto volume rose to $10.6T; $45B total illicit volume in 2024 (down 24% YoY)	Continued decline in illicit proportion signals sustained enforcement effectiveness across exchange and financial chain; plateau indicates criminal adaptation offsetting enforcement gains

Disruption KPIs

KPI	Baseline	Target Under Disruption	Collection Method
Annual ransomware payment volume (USD)	$813.55M in 2024 (Chainalysis; down 35.82% from 2023)	Below $600M sustained over two consecutive calendar years; not attributable to reduced attack volume (cross-reference DLS victim counts)	Chainalysis annual ransomware report; TRM Labs crypto crime report; cross-reference with Module 08 DLS victim volumes
CEX share of ransomware laundering flows (annual)	Approximately 39% in 2024; 37% 2020-2024 average (Chainalysis)	CEX share declining below 30% with corresponding increase in wallet dwell time (not DEX/P2P shift); sustained over two consecutive years	Chainalysis annual ransomware report; TRM Labs crypto crime flow analysis

OFAC-designated exchange entities (cumulative) and designation tempo	3+ major designations as of 2024; pace accelerating since 2021	Minimum 2 new major exchange designations per year; no identified dominant high-risk exchange operating undesignated for more than 18 months post-identification	Treasury/OFAC SDN list monitoring; blockchain analytics identification pipeline (Chainalysis, TRM Labs)
Garantex successor identification and designation timeline	Garantex shutdown April 2025; successor not confirmed as of April 2026; ruble-liquidity gap ongoing	Successor exchange identified within 6 months of Garantex shutdown; designated within 12 months of identification	FVEY blockchain analytics monitoring; underground forum surveillance for new exchange advertising; Rosfinmonitoring pipeline (conditional, per Module 14 limitations)
Time from high-risk exchange identification to OFAC designation (days)	Historically 6-18 months from blockchain analytics identification to designation; Garantex identification predated designation by approximately 12 months	Below 120 days from confirmed dominant high-risk exchange identification to OFAC action	Internal OFAC designation pipeline tracking; blockchain analytics partner identification tempo

Alert Thresholds

Threshold	Trigger Condition	Response
New high-risk exchange identified handling above $100M in attributable ransomware flows within 90 days	Blockchain analytics identifies new exchange processing above $100M in attributable ransomware proceeds within any 90-day window	Initiate OFAC designation process; alert FVEY financial partners; share wallet cluster with major exchange and banking compliance teams within 30 days; assess for Garantex-successor characteristics
Ransomware CEX off-ramp share increases above 45%	Chainalysis annual reporting documents year-over-year increase in CEX share above 45% of ransomware laundering flows	Assess whether increase reflects new nested VASP infrastructure, improved straw-man account supply, or reduced blockchain analytics detection at major CEXs; cross-reference with active OTC broker designation list
Garantex-successor exchange begins capturing displaced ruble-liquidity volume	Blockchain analytics identifies new RU-based exchange absorbing post-Garantex displaced volume above $50M in 90-day window	Immediate OFAC designation initiation; Europol coordination for physical enforcement groundwork; correspondent bank de-risking pressure; Dark Covenant screening for FSB protection relationship assessment
Ransomware payment volumes rebound above $1B annually	Chainalysis or TRM Labs documents year-over-year rebound above $1B after 2024 decline	Assess whether rebound reflects new exchange infrastructure, improved attacker off-ramp OPSEC, or enforcement gap; cross-reference with active designation list, exchange compliance coverage, and OTC broker disruption status

SECTION 7: SOURCES AND CONFIDENCE

Primary Sources

Blockchain Analytics and Financial Intelligence:

- Chainalysis — "Crypto Ransomware 2025: 35.82% YoY Decrease in Payments": 2024 revenue ($813.55M); 39% CEX share; mixer decline; bridge/DEX shift; concentration risk documentation; historical 37% average; primary quantitative source for exchange off-ramp data.
- Chainalysis — "Ransomware Hit $1 Billion in 2023" and 2024 Crypto Crime Trend reports: concentration on high-risk services; Garantex exposure; role of exchanges across multiple ransomware families.
- TRM Labs — "Ransomware in 2024: Latest Trends" and Garantex takedown analysis: peel chains; cross-chain laundering typologies; Garantex "key role in laundering ransomware proceeds" (Ryuk >$2.3M, Conti, LockBit); $2.2B stolen in 2024 crypto hacks.
- TRM Labs / Cointelegraph / CryptoNews — Embargo ransomware case: $34M tracked since April 2024; $13.5M through various VASPs; >$1M via Cryptex.net; cross-chain flow documentation.
- TRM Labs — "$2.2B Stolen in Crypto in 2024" and "Proportion of Illicit Volume Dropped 51%": macro context for illicit flow volumes and exchange role in post-heist laundering.

Media and Government Coverage:

- CyberScoop / Wired — coverage of Chainalysis 2024 ransomware findings: "wallet sitting" behavioral adaptation; 35% payment decline attribution.
- Europol — Garantex shutdown press release (April 2025): server seizure, domain takeover, operator charges; physical enforcement documentation.
- OFAC — SDN designation documentation: SUEX (September 2021), Garantex (April 2022), Cryptex (2024); designation rationale and criminal flow attribution.

Academic:

- Tandfonline academic article — "From prepaid cards to bitcoin: How did ransomware hackers adopt cryptocurrencies?": historical drivers for crypto adoption in extortion; structural role of centralized exchanges in ransomware monetization evolution.

Confidence Assessment by Topic

Topic	Confidence Level	Basis	Key Limitations
39% CEX share of ransomware off-ramping in 2024	**[CONFIRMED]** CONFIRMED	Chainalysis 2024 annual ransomware report; primary data source with disclosed methodology; consistent with prior year baselines	Methodology includes attribution assumptions; actual CEX share may vary if nested OTC broker flows are attributed differently; possible undercounting of obfuscated flows
Garantex laundering role (Ryuk >$2.3M; Conti; LockBit)	**[CONFIRMED]** CONFIRMED	TRM Labs documented case study; OFAC designation rationale; Europol enforcement documentation; multiple independent sources consistent	Dollar figures reflect attributed flows at time of investigation; actual total laundering volume through Garantex likely significantly higher given partial blockchain visibility
35% ransomware payment decline attribution to exchange enforcement	**[CONFIRMED]** CONFIRMED (figure); CREDIBLE	Chainalysis figure widely corroborated; enforcement attribution is Chainalysis analytical assessment consistent with TRM Labs and	Multiple confounding factors (victim resistance, backup improvement, negotiation quality); enforcement is one of several cited drivers;

	(enforcement attribution)	other blockchain analytics firms	precise attribution share not independently quantifiable
Embargo $34M tracked / $13.5M through VASPs / >$1M via Cryptex	**[CREDIBLE]** CREDIBLE	TRM Labs case study; secondary reporting (Cointelegraph, CryptoNews) consistent; Cryptex OFAC designation corroborates exchange identification	Tracking figures represent attributable flows; actual total may be higher; methodology for VASP attribution not fully disclosed in public reporting
"Wallet sitting" behavioral adaptation by ransomware operators	**[CREDIBLE]** CREDIBLE	CyberScoop reporting citing Chainalysis findings; consistent with behavioral deterrence theory and observable pattern of extended wallet dwell times in attributed transactions	Behavioral attribution is inference from on-chain patterns; operators may have other motivations for extended dwell (market timing, operational security practices independent of tracing risk)
Illicit volume proportion dropped 51% in 2024	**[CONFIRMED]** CONFIRMED	TRM Labs 2024 crypto crime report; $45B total illicit volume vs $10.6T total crypto volume; consistent with Chainalysis data	"Illicit" categorization methodology varies between analytics vendors; figure reflects known illicit flows rather than total illicit flows

Intelligence Gaps

- Garantex successor exchange: No confirmed dominant high-risk exchange absorbing Garantex's ruble-liquidity function has been publicly identified as of April 2026. This is the highest-priority gap for next Phase A designation action.
- Straw-man account supply chain for compliant CEXs: The specific criminal supply chains providing straw-man and mule accounts to compliant CEX KYC processes are not systematically documented. Understanding this supply chain would allow more precise disruption targeting at the account supply level rather than the exchange level.
- Wallet dwell time baseline: No quantified baseline for average ransomware wallet dwell time before exchange deposit exists in open sources. Establishing this baseline would allow measurement of the behavioral deterrence effect and its correlation with specific enforcement actions.
- Underground VASP operator identities: Nested and underground VASP operators advertising on top-tier Russian forums are not publicly identified in open sources. These operators are the primary mechanism for routing ransomware funds through compliant CEX accounts.

SECTION 8: ANALYST ASSESSMENT

Key Takeaway

Module 13 contains the central paradox of the EDP financial disruption framework: CEX share of ransomware off-ramping slightly increased in 2024 (to 39%, above the 37% historical average) even as the overall ransomware payment volume fell 35%. These two findings are not contradictory — they reflect the same enforcement mechanism operating correctly. Mixer and high-risk exchange enforcement pushed ransomware operators toward compliant CEXs via more complex intermediary chains (OTC nested desks, bridges, straw-man accounts), reducing total payment volume while increasing the CEX share of the remaining flows. The enforcement is working. The implication is not to target compliant CEXs but to tighten the intermediary account supply chains — nested OTC desks and straw-man account suppliers — that provide access to compliant CEX liquidity.

The Garantex enforcement sequence is the definitive proof of concept for Phase A exchange action. The three-year gap between OFAC designation (April 2022) and physical shutdown (April 2025) is the most important

operational lesson from the entire financial enforcement record: designation-only is insufficient for RU-domiciled exchanges. Physical enforcement, operator prosecution, and correspondent banking de-risking must follow designation within 12-18 months to produce durable disruption. The Garantex successor — whatever exchange is now absorbing displaced ruble-liquidity flows — is the immediate next Phase A priority, and it should be designated and physically targeted faster than the Garantex timeline.

Priority Recommendation

Immediate: Identify the Garantex successor exchange and initiate designation. The April 2025 Garantex shutdown created the largest ruble-liquidity gap in the RU criminal exchange ecosystem since the SUEX designation in 2021. Priority tasking to FVEY blockchain analytics partners (Chainalysis, TRM Labs) to identify RU-based exchange activity absorbing post-Garantex displaced volume. Target designation within 6 months of identification rather than the 12-month historical average — the criminal ecosystem reconstitutes faster with each successive disruption.

Near-term: Institutionalize the physical enforcement follow-up track for OFAC-designated RU-domiciled exchanges. The Garantex lesson — that designation alone allows three years of continued operation within Russia — should produce a policy commitment: any RU-based exchange designated by OFAC that continues operating within Russia should be escalated for Europol-model physical enforcement within 18 months of designation. This commitment would deter successors from establishing RU-domiciled operations assuming designation-only exposure.

Medium-term: Develop a straw-man account supply chain disruption program targeting the mechanism through which ransomware operators access compliant CEX liquidity. The 39% CEX share cannot be reduced by targeting exchanges directly — it requires targeting the intermediary account supply (nested OTC desks, straw-man account suppliers, mule account sourcing for CEX KYC). Coordinating behavioral biometrics vendors (BioCatch), exchange compliance teams, and FinCEN on account-pattern-based detection and suspension is the structural mechanism.

Sequencing note: Phase A Node 02 (exchange) and Node 01 (OTC broker) actions must remain closely coordinated. The 2024 35% payment decline reflects simultaneous pressure on both nodes — designated exchanges and OTC brokers, combined with improved exchange compliance integration. Allowing either node to remain without designation coverage for more than 18 months creates a displacement rather than disruption effect.

Connection to EDP Disruption Playbook

Node 02 (High-Risk/Non-Compliant Exchanges) is a Phase A node alongside Nodes 01 (OTC Brokers) and 03 (BPH). It forms the financial foundation of the EDP disruption framework: without functional exchange off-ramps, the entire ransomware supply chain — from stealer-log acquisition through RaaS deployment to extortion — produces cryptocurrency proceeds that cannot be converted to usable criminal wealth.

The 2024 payment decline is the empirical validation of the Phase A playbook. Coordinated OFAC action against Garantex and Cryptex (Node 02), combined with OTC broker enforcement (Node 01) and mixer actions (Node 08), produced a 35.82% year-over-year revenue reduction — the most significant ecosystem-level disruption metric in the EDP dataset. This compound effect is the core argument for Phase A coordinated action rather than sequential single-node targeting: each additional designation amplifies the effect of prior designations by closing alternative off-ramp channels.

Dependency Map Update Recommendations

Current Node 02 Field	Current Value	Proposed Change	Rationale
Primary Owner	Treasury/OFAC + FVEY financial regulators + blockchain forensics	Add Europol as co-primary owner for physical enforcement track; add major CEX compliance teams as co-primary for straw-man	Garantex enforcement demonstrates that Europol physical enforcement is an equal or greater action to OFAC designation for RU-domiciled

		account supply disruption	exchanges. CEX compliance teams are the structural mechanism for the straw-man account supply chokepoint — both require elevation to co-primary status.
No physical enforcement follow-up commitment	N/A	Add explicit policy recommendation: OFAC-designated RU-domiciled exchanges that continue operating post-designation should be escalated for Europol-model physical enforcement within 18 months of confirmed continued operation	The three-year Garantex designation-to-shutdown gap is the primary operational lesson from Module 13. Institutionalizing a shorter escalation timeline would deter successor exchanges from establishing RU-domiciled operations assuming designation-only exposure.
No tracking of "wallet sitting" behavioral indicator	N/A	Add ransomware wallet dwell time before exchange deposit as a standing behavioral indicator under Node 02; establish baseline and track correlation with specific enforcement actions	"Wallet sitting" represents a behavioral deterrence effect that the EDP framework does not currently model. If enforcement pressure is producing extended dwell times without payment cancellation, it represents partial success that warrants dedicated tracking.
No Garantex-successor tracking requirement	N/A	Add Garantex ruble-liquidity successor identification as a standing Phase A priority intelligence requirement under Node 02; flag with 6-month identification and 18-month designation targets	Consistent with Module 12 (OTC Brokers) Garantex-successor recommendation. The exchange-tier successor is a distinct target from the OTC-tier successor and requires separate tracking.

Follow-On Research

- Identify Garantex ruble-liquidity successor at exchange tier: separate tasking from Module 12 OTC-tier successor identification; blockchain analytics priority to identify RU-based exchange absorbing post-April 2025 displaced criminal volume.
- Establish ransomware wallet dwell time baseline: task Chainalysis and TRM Labs to quantify average dwell time between ransom payment receipt and first exchange deposit across attributed 2024-2025 ransomware flows; correlate with specific enforcement action dates.
- Map straw-man account supply chain for compliant CEX access: identify the criminal supply chains (mule account suppliers, identity document forgers, underground VASP operators) providing KYC-passing accounts to ransomware operators for compliant CEX deposits.
- Assess bridge and DEX OFAC designation pipeline: identify the specific cross-chain bridge protocols most heavily used in 2024-2025 ransomware pre-exchange obfuscation; assess each for OFAC designation viability under Tornado Cash precedent.
- Model Phase A compound action marginal effect: using 2024 data as baseline, model the marginal revenue reduction effect of each additional Node 01/02/08 designation — distinguishing compound action multiplier from single-node effect.