KPI DATA ACQUISITION AND SOURCING PLAN

Ransomware Ecosystem Disruption Framework | Interagency Working Group Reference | April 2026 | v1.0

PURPOSE

This document maps every KPI in the Ransomware Ecosystem Disruption Framework to a specific data source, responsible owner, update cadence, concrete data ask, and interagency framing strategy. It is the operational bridge between the KPI design (framework document) and the measurement program (tracker workbook). It is designed for use at interagency working group meetings to assign ownership, resolve gaps, and structure partner engagement asks.

Red-flagged rows indicate unassigned ownership gaps. These are not silent deficiencies. They are the interagency coordination agenda.

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
THEME A: Russian Domestic Enforcement							
A-1	Russian Domestic Actions Against Ecosystem Actors	MVD press releases; iStories, Meduza, OCCRP investigative journalism; open Russian court records; FinCEN cross-reference	Framework coordinator (open source); FBI Cyber (seeded referral attribution)	Quarterly	Provide count of Russian criminal, admin, or tax actions against ransomware-mapped actors per quarter. Three fields minimum: date, actor tier (elite/mid/support), charge type. Cyber-specific charges not required.	Framing: this metric measures whether Russia is treating cybercriminals as liabilities. LE partners benefit by demonstrating their operations generate observable downstream Russian responses, which supports resource arguments.	L1 AVAILABLE
A-2	Referral-to-Action Lag (days)	Internal operation logs (micro layer); open-source Russian enforcement reporting	*Owning operational team per referral. No current aggregator assigned.*	Per referral event; aggregated quarterly	De-identified log of Russia-directed referrals: three fields only. Date of referral, recipient channel (MVD/Rosfinmonitoring/FSB/CBR), and date of first observable Russian response or 'no response.' No full case files required.	Framing: this is the only metric that can show whether pressure on Russia produces observable domestic	L2 PENDING

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
						responses. Even a negative result (no response) is analytically significant and supports escalation arguments. Low ask, high analytic return.	
A-3	Protection Relationship Status Inventory	IC reporting feeds; underground forum monitoring (Flashpoint/Intel 471); blockchain anomaly detection; investigative journalism outputs	*IC analytic team (controlled annex). No current owner assigned.*	Quarterly snapshot	Snapshot count by status category (Active / Strained / Broken / Unknown) per quarter. Track transitions as separate trend line. Individual officer data maintained in Tier 3 controlled annex only. Leadership reports counts and categories, not names.	Framing: this is the protection-layer visibility gap. Even a partial inventory with INDICATIVE confidence is more defensible than a blank field. Engage IC partners by framing as a classified annex product, not a public-facing metric. Governance protections already built into framework.	L2 PENDING
THEME B: FSB/RIS Strife Indicators							
B-1	Weighted Arrest Impact Score (WAIS)	Owning agency debrief records; FBI/DOJ/NCA/Europol prosecution files; public indictments; Chainalysis/TRM for reconstitution tracking	Owning agency per arrest, aggregated by framework coordinator	Per arrest within 30 days of action	Score each arrest within 30 days using the four WAIS dimensions. Mark Cooperation Output as PENDING if debrief is incomplete rather than estimating. Aggregate into quarterly WAIS distribution (high/moderate/limited). Require this as part of standard after-action	Framing: WAIS gives LE partners a credible way to show their cases have ecosystem-level impact, not just headline arrests. It	L1 AVAILABLE

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
					process, not an optional analytic step.	differentiates meaningful operations from vanity arrests in leadership reporting. This serves their resource and credit interests.	
B-2a	Strife Proxy Metrics: Affiliate Defection, Exit Scam Frequency, New RaaS Brand Emergence, Recruitment Term Shifts	Intel 471; Flashpoint; Recorded Future; Ransomware.live; Ransomlook.io; GuidePoint GRIT; Check Point Research	Intel 471/Flashpoint primary. Framework coordinator aggregates quarterly.	Quarterly	Quarterly brand census reconciling new vs. rebranded groups. Affiliate migration tracking for 90 days post-disruption. Exit scam identification via wallet behavior (Chainalysis) vs. LE takedown confirmation. Recruitment term shifts tracked via underground forum monitoring.	Framing: vendor partners get feedback and cross-validation they cannot produce alone. Offer reciprocal data sharing where permissible. Underground monitoring vendors benefit from being cited in interagency framework products, supporting their commercial positioning.	L1 AVAILABLE
B-2b	Strife Event Log (IC-Level)	IC reporting; underground forum monitoring; Chainalysis wallet analysis; investigative journalism; debrief records (sanitized)	*Dedicated analytic owner required. Currently unassigned.*	Per event; reviewed quarterly	Structured log entry per strife event: type (leak/exit scam/defection/dispute), date, actors involved, ecosystem effect, confidence label. Conti leak and Black Basta leak are canonical reference entries. Debrief outputs fed back (sanitized) to enrich trust cascade and reconstitution WAIS dimensions.	Framing: this is the primary IC-value product for Theme B. Position it as the qualitative anchor that makes the proxy metrics credible. Ownership gap is an agenda item for the interagency	L2 PENDING

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
						working group, not a silent gap.	
THEME C: Ecosystem Economics							
C-1	Payment Volume vs. Victim Count Divergence	Chainalysis Crypto Crime Report (annual); TRM Labs (cross-validation); Elliptic (tertiary); public quarterly ransomware reports	Framework coordinator. Chainalysis/TRM primary sources.	Annual (public report cycle); Quarterly with subscription access	Negotiate standing quarterly data product: total ransomware-linked inflows by family, inferred payment rates where available, sector tagging where possible. Align Chainalysis/TRM reporting cadence to Macro KPI Dashboard quarters. Annual public reports sufficient for year-end baseline; subscription required for quarterly granularity.	Framing: vendors benefit from being the named data source in a high-visibility interagency measurement program. Offer analytic feedback and co-publication opportunities where permissible. This also supports their government contract positioning.	L1 AVAILABLE
C-2	Victim Payment Rate by Sector	Coveware quarterly reports; Kivu; Arete; cyber insurers (Corvus, Coalition, Beazley); national CERTs and ISACs with incident reporting	Framework coordinator. Coveware primary; insurer data supplementary.	Quarterly	Sector payment rate trends for healthcare, critical infrastructure, and general commercial segments. Absolute numbers not required if proprietary: relative rates and directional trends sufficient for C-2 KPIs. Pursue harmonization of incident reporting schemas across CERTs and ISACs to standardize ransom demanded/paid/refused fields.	Framing: insurers receive political cover and reputational benefit from participation. Propose anonymization plus aggregate findings that help them price risk and inform policy lobbying. A multi-insurer pooled dataset under research MOU is the strategic goal; bilateral data	L1 AVAILABLE

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
						sharing agreements are the interim step.	
C-3a	Leak Site Post Volume (Signal 1)	Ransomware.live (victims.json); Ransomlook.io (API); Ransomwatch (cross-validation); DarkFeed (supplementary)	Framework coordinator. Data files downloaded and processed. Monthly update cycle.	Monthly	POPULATED. Monthly victim post volume data loaded from Ransomware.live and Ransomlook.io source files (Jan 2022 through Apr 2026) into Leak Site Signals tab of KPI tracker. Update cycle: download fresh source files monthly and refresh tab. Both sources are public, no-cost, and no-auth required.	No additional partner engagement required for this signal at current fidelity. Automation via Claude Code or scheduled script recommended for scale. Validate against Ransomwatch quarterly for coverage gaps.	POPULATED
C-3b	Leak Site Time-to-Publish (Signal 2)	Coveware/Chainalysis negotiation timeline data; Ransomlook.io discovered vs. published date delta; private sector IR firms	Framework coordinator. Coveware/Chainalysis supplementary.	Quarterly	Track average days from confirmed compromise to leak site publication. Requires discovered date plus known compromise date per victim. Ransomlook.io provides discovered date; compromise date requires IR firm or CERT reporting. Trend direction is the primary signal; absolute precision not required.	Framing: compression in time-to-publish is a pressure signal indicating operators are accelerating due to fear of disruption. Engage IR firms by positioning this as a shared indicator that benefits their threat briefing products.	L1 AVAILABLE
C-3c	Takedown/Relaunch Cycle (Signal 3)	Public LE announcements (FBI, NCA, Europol, DOJ); Ransomware.live/Ransomlook.io site status monitoring; Chainalysis wallet analysis for exit scam vs. LE takedown distinction	Framework coordinator. FVEY LE partners for takedown date confirmation.	Per event	Log each site takedown and relaunch event: brand name, takedown date, relaunch date, relaunch type (same brand/rebrand/absorbed), and days to relaunch. Reference entries (LockBit, BlackCat, RansomHub, QakBot) already populated. Ongoing entries require	Framing: this is the most concrete measure of infrastructure resilience. LE partners benefit from a structured record that	L1/L2 PARTIAL

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
					real-time LE disclosure coordination.	shows whether their takedowns produce durable effects. Supports both internal accountability and public attribution narratives.	
MESO LAYER: Node Pressure Metrics							
M-01	OTC Broker Designation Coverage (Node 01)	Chainalysis/TRM (top-20 OTC broker identification); OFAC SDN list; Treasury designation pipeline; Intel 471/Flashpoint (underground OTC advertising)	OFAC/Treasury primary. Chainalysis/TRM for broker identification.	Monthly/per designation	Commission specific Intermediary Cash-Out Mapping deliverable: top-20 OTC broker nodes, key mule network linkages, and 3-5 fully mapped laundering chains from ransom demand to fiat. This is the highest-ROI data investment for Node 01 KPIs. Designation pipeline coordination with OFAC required for real-time tracking.	Framing: Chainalysis/TRM benefit from demonstrated operational impact of their analysis feeding into designation packages. Position as a feedback loop: their analysis produces designations, which produce observable behavioral change, which they can then track and publish.	L1/L2 PARTIAL
M-02	Exchange VASP Friction Metrics (Node 02)	VASP/Exchange LE Cooperation Reference (internal); OFAC SDN; FinCEN SARs (aggregate); Chainalysis/TRM blockchain flow data; correspondent banking friction events	Treasury/FinCEN primary. FVEY financial partners supplementary.	Quarterly	Count of VASP enhanced-due-diligence referrals acted on per quarter. Proportion of ransomware-attributed withdrawal addresses flagged at exchange level. Correspondent banking friction events (de-risking actions against exchanges). Cross-reference against VASP cooperation tier ratings in existing	Framing: FinCEN and FVEY financial partners benefit from a shared metric that demonstrates the operational value of their VASP	L1 AVAILABLE

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
					internal exchange reference document.	engagement programs. Position exchange friction metrics as proof that FATF correspondent banking pressure produces measurable crypto ecosystem effects.	
M-03	BPH Reconstitution Speed (Node 03)	Shadowserver; Censys; FBI/NCA post-action monitoring; public LE disclosures; Aeza Group/Zservers tracking post-designation	*FBI/NCA/Shadowserver. Post-action follow-up protocol currently ad hoc.*	Per action; 30/90/180-day follow-up	Partner with Shadowserver/Censys to produce quarterly BPH report scoped to Russia/CIS-linked ransomware: active provider counts, ASN concentration, average time from takedown to reappearance, infrastructure overlap across families. Post-action follow-up protocol must be formalized. Currently ad hoc.	Framing: Shadowserver and infrastructure mapping partners benefit from having their data cited in interagency products. Formalized post-action reporting also supports LE public attribution and helps justify future operational resources.	L1 AVAILABLE
M-04	IAB Market Volume and Pricing (Node 04)	Intel 471; Flashpoint; Recorded Future; CISA victim notification data; underground forum monitoring (Exploit, XSS)	Intel 471/Flashpoint primary. CISA for victim notification closure rate.	Monthly (listing volume); Quarterly (pricing trends)	Monthly IAB listing volume on Exploit and XSS forums. Average asking price by access type (RDP, VPN, domain admin). Top-10 operator churn rate quarterly. Victim notification success rate via CISA ISAC coordination. Systematic pricing data requires active vendor subscription.	Framing: underground intel vendors benefit from demonstrating that their forum monitoring data feeds operational outcomes. CISA benefits from a	L1 AVAILABLE

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
						formal feedback loop between their notification program and ecosystem-level impact metrics.	
M-07	Underground Trust Health (Node 07)	Intel 471; Flashpoint; Chainalysis (wallet behavior anomalies indicating exit scam vs. LE action); public forum dispute threads	Intel 471/Flashpoint primary. No current gap in ownership.	Quarterly	Arbitration request volume and accusation threads against specific actors on Exploit and XSS. Track by target actor and time proximity to pressure actions. Escrow operator count serving major RaaS brands. Time to re-establish escrow post-takedown. Forum health score requires subscription access.	Framing: trust degradation metrics are the leading indicator that financial disruption is translating into ecosystem friction. Position this as the early warning layer that predicts macro Theme B movements before they appear in arrest or payment data.	L1 AVAILABLE
M-08	Mixer/Obfuscation Service Coverage (Node 08)	Chainalysis/TRM (mixer usage volume, bridge migration patterns); OFAC SDN (designation status); public Chainalysis reporting on obfuscation trends	Chainalysis/TRM primary. OFAC for designation pipeline.	Quarterly	Mixer usage volume as percentage of total ransomware cash-out flows. Post-designation fund migration patterns (to bridges, personal wallets, or substitute mixers). Active mixer and bridge inventory vs. pre-designation baseline. Tornado Cash delisting impact tracking. Requires OFAC designation pipeline access for real-time tracking.	Framing: mixer disruption metrics provide some of the clearest causal evidence in the framework. Each designation produces an observable behavioral shift trackable on-chain. Position Chainalysis/TRM as the measurement partner that makes that causal chain	L1 AVAILABLE

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
						visible to leadership.	
M-09A	Domestic Mule Network Visibility (Node 09A)	Rosfinmonitoring/FNS/CBR channel access; Egmont FIU network (Belarus as viable backdoor channel); internal referral logs	*Rosfinmonitoring channel. Highest-priority unassigned gap. Belarus FIU as interim channel for non-FSB-protected targets.*	Quarterly (if channel established)	This is the highest-priority L2 gap. No open-source visibility into domestic Russian mule network activity. Requires formal back-channel FIU relationship. Belarus is the only credible Egmont backdoor with meaningful probability of forwarding referrals Rosfinmonitoring will act on, and only for non-FSB-protected targets. Must be an explicit interagency agenda item.	Framing: do not frame as a Russia cooperation request. Frame as a financial crime referral through the Belarus FIU using 115-FZ fraud framing (Articles 159-159.6) to avoid political protection triggers. This is the three-track referral architecture already developed in companion AML work.	L2 PENDING
M-09B	Third-Country Mule Prosecution Packages (Node 09B)	FVEY LE partners; Europol; MLAT referral tracking; public Chainalysis crypto-fiat nexus data	FVEY LE/Europol. MLAT referral count and action rate require formal partner reporting.	Quarterly	MLAT referral count and action rate per quarter. Third-country prosecution packages initiated vs. completed. Crypto-fiat nexus linkages from public Chainalysis data. Specific mule network mapping requires FVEY LE and Europol partner reporting. Partially visible through existing MLAT actions.	Framing: FVEY partners benefit from a shared ledger that demonstrates the operational value of their MLAT cooperation. This metric also supports diplomatic arguments for expanding third-country LE cooperation agreements.	L1/L2 PARTIAL
MICRO LAYER: Per-Operation Log							

KPI ID	KPI Name	Data Source(s)	Responsible Owner	Cadence	Specific Data Ask	Framing / Acquisition Strategy	Status
MICRO	Per-Operation Log (all nodes)	Owning agency operational records; WAIS scoring outputs; meso-layer node metrics at 30/90/180-day intervals	CRITICAL GAP: No designated log aggregator assigned. Must be resolved before any coordinated pressure campaign is measurable.	Per action; 30/90/180-day updates	Every disruption action requires a log entry pre-action. Minimum fields: operation ID, date, target node, action type, expected primary effect (30 days), backfire risk. Update at 30, 90, and 180 days. Undocumented operations do not count toward ecosystem metrics.	Without a populated micro log, macro KPI movements cannot be attributed to specific actions. Ownership of log aggregation is the agenda item.	L2 PENDING

RED TEXT: Unassigned ownership gap. These are interagency agenda items, not silent deficiencies. The framework is designed to make gaps visible, not hide them.

Vendor Concentration Risk: Multiple KPIs depend on a small set of commercial vendors (Chainalysis, Coveware, Intel 471/Flashpoint, Ransomware.live). Loss of any single vendor degrades a confidence tier. Maintain at least one cross-validation source per node.

Time-Window Coordination: WAIS is per-arrest, Group Pressure is per-group, macro KPIs are quarterly, leak site signals are monthly. Quarterly narrative synthesis must explicitly bridge these cadences to avoid apples-to-oranges comparisons in leadership reporting.