RANSOMWARE ECOSYSTEM DISRUPTION MEASUREMENT FRAMEWORK

KPI Architecture

Version 0.3 | June 2026 | Working Document

Developed by Reno

SECTION 1 | PURPOSE AND DESIGN PRINCIPLES

1.1 What This Document Is

This framework provides a structured, operationally defensible system for measuring the sustained degradation of the Russia/CIS-linked ransomware ecosystem. It is designed for IC/LE interagency use, feeding strategic-level matrix development and operational accountability.

It is not a scorecard for leadership optics. Every metric in this framework traces to concrete underlying data, carries an explicit confidence label, and has a stated limitation. Unless otherwise specified, all KPIs are scoped to Russia/CIS-linked ransomware and associated enabling infrastructure. Do not apply this framework to global ransomware without revisiting the design assumptions.

> **CORE MEASUREMENT PHILOSOPHY**
>
> Ecosystem-wide indicators are lagging. They tell you something already happened. Node-level indicators are leading. They tell you pressure is working before it shows up in aggregate data. This framework requires both, explicitly linked. A macro number without a traceable causal chain is not a KPI. It is a narrative.
>
> Any operation claiming ecosystem-level impact must be logged at the micro layer with at minimum: WAIS score (if arrest), time-to-reconstitution, and any protection-relationship observations. Undocumented operations do not count toward ecosystem metrics.

1.2 Framework Architecture

The framework operates at three levels. They are explicitly linked. Micro feeds meso, meso feeds macro. A change at the macro level must be explainable by movement at the meso and micro levels, or the confidence label on that macro metric drops.

Layer	What It Measures	Cadence	Primary Audience
MACRO: Ecosystem Outcomes	Ransom volume trends, domestic enforcement incidents, FSB/RIS strife indicators, payment rates	Quarterly	Senior leadership, STRAT offices
MESO: Node Pressure	Per-node cluster metrics: OTC brokers, IAB markets, BPH, leak sites, mixers, mule networks, stealers, marketplaces. Maps directly to Nodes 01-10 in the companion disruption playbooks, plus a Node 07 supplemental marketplace cluster.	Monthly or per action	Interagency working groups, operational leads
MICRO: Operation Logging	Per-action: expected effect vs. observed effect, time-to-reconstitution, cooperation output, protection-layer observations	Per operation	Owning agency or team

1.3 Confidence Labeling System

Every metric carries one of three confidence labels. Confidence reflects source reliability and measurement precision, not the importance of the indicator.

Label	Definition	Typical Sources
CONFIRMED	Hard data, traceable source, reproducible	Chainalysis/TRM blockchain forensics,

Label	Definition	Typical Sources
	methodology	official arrest and designation records, verified leak site tracking
CREDIBLE	Corroborated reporting, reasonable inference, multiple source types	Intel 471/Flashpoint underground monitoring, cross-validated financial intelligence, observed reconstitution tracking
ANALYST INFERENCE	Single-source or proxy measure, directional only. Not sufficient for operational targeting.	Forum monitoring, social signals, strife proxy metrics, stealer and marketplace indicators

1.4 Maturity Levels

Metrics are designated at one of two maturity levels. This is an honest assessment, not a limitation to hide.

Level	Definition	Implication
LEVEL 1: Operational Now	Populatable with existing available data sources and current partner contacts	Build and maintain immediately
LEVEL 2: Requires Buy-In	Requires formal interagency ownership assignment or classified collection feeds	Design is complete. Awaiting ownership assignment and authority confirmation.

SECTION 2 | MACRO KPIs - THREE THEMES

The framework is organized under three strategic success themes. These are the outcomes that define ecosystem degradation at the senior-reportable level. Each theme carries 3-4 macro KPIs with explicit formula, data source, confidence label, and known limitation.

THEME A

More Russian Domestic Enforcement. Russia's own institutions treat cybercriminals as liabilities, not assets.

KPI A-1 | Russian Domestic Actions Against Ecosystem Actors

Reliability: ● **CREDIBLE**

Definition: Count of Russian criminal, administrative, or tax enforcement actions against actors previously mapped as protected or linked to ransomware ecosystem operations. Includes tax fraud charges, AML actions, currency violations, and organized crime charges. Cyber-specific charges are not required.

- **Formula:** Count of actions per quarter, broken out by actor tier (elite, mid-tier, support). Primary analytic focus is on elite and mid-tier actions. Support-tier counts are reported but not emphasized in leadership summaries. A count inflated by low-tier symbolic busts does not represent progress toward this framework's objectives.
- **Tier weighting:** Each quarter, report the breakdown as elite-tier actions / mid-tier actions / support-tier actions. A ratio shifting toward elite and mid-tier is the signal. Raw count increases driven by support-tier arrests are not.
- **Data Sources:** Open-source Russian court records, MVD press releases, investigative journalism (iStories, Meduza, OCCRP), FinCEN and Rosfinmonitoring cross-referencing
- **Known Limitation:** Russian domestic actions are frequently unreported or reported with significant lag. Non-public charges may be invisible. Count is almost certainly an undercount.
- **Maturity:** LEVEL 1 for open-source visible actions. LEVEL 2 for seeded-referral attribution.

KPI A-2 | Time Lag: Referral to Observable Russian Action

Reliability: ● **CREDIBLE**

Definition: For operations where a financial exposure or referral package was seeded through domestic Russian channels (FNS, Rosfinmonitoring, CBR), the elapsed time between the seeding action and a visible Russian enforcement response.

- **Formula:** Days from documented referral or seeding action to confirmed Russian enforcement event, per case
- **Data Sources:** Internal operation logs (micro layer), open-source Russian enforcement reporting
- **Known Limitation:** Attribution of Russian action to a specific seeding operation is inferred, not confirmed. Correlation is the operative standard. Causation cannot be proven.
- **Maturity:** LEVEL 2. Requires internal operation log population by owning teams.

KPI A-3 | Protection Relationship Status Inventory

Reliability: ● **ANALYST INFERENCE**

Definition: Count and status classification of known or assessed protection relationships between Russian state officers or units and ecosystem actors. Status categories: Active, Strained, Broken, Unknown.

- **Formula:** Snapshot count per quarter by status category. Track transitions (Active to Strained, Strained to Broken) as a separate trend line.
- **Data Sources:** Underground forum monitoring, blockchain anomaly detection (sudden wallet behavior changes), IC reporting, investigative journalism outputs
- **Known Limitation:** Status assessment is analytic inference. A relationship assessed as Broken may be suspended rather than permanently severed. Current confidence is ANALYST INFERENCE: the primary data foundation (underground forum monitoring, blockchain anomaly detection) does not meet the CREDIBLE threshold. The CREDIBLE label applies only after L2 IC reporting feeds are formally assigned and operational. Do not brief protection relationship status counts at leadership level without noting this data limitation explicitly.
- **Governance Note:** At the leadership level, report counts and status categories only. Individual officer-level data is maintained in a controlled analytic annex, not the leadership dashboard.
- **Maturity:** LEVEL 2. Requires IC reporting feeds and protected analytic annex structure.

THEME B

Visible FSB/RIS Strife. Create and exploit contradictions inside the protection apparatus.

KPI B-1 | Weighted Arrest Impact Score (WAIS)

Reliability: ● CONFIRMED

Definition: A composite score for arrest and prosecution events that captures effect quality, not just occurrence. Raw arrest counts treat a single affiliate arrest and a coordinated RaaS core team takedown as equivalent events. WAIS does not.

Scoring principle: it is better to score coarsely but consistently than perfectly but rarely. Where debrief data is unavailable for the Cooperation Output dimension, mark the field PENDING rather than assigning a default value. A pending field is honest. A defaulted score is not.

- **Known Limitation:** The CONFIRMED reliability label applies to the underlying source data — arrest events, attribution assessments, prosecution outcomes — not to the scoring model itself. WAIS is an analyst-constructed composite framework. The four-dimension structure and point weighting reflect analytical judgment; they have not been independently validated against historical ecosystem-disruption outcomes. Treat WAIS scores as defensible structured estimates, not empirically calibrated measurements. The framework should be reviewed and recalibrated if a sustained data series (10+ scored events) becomes available.

Dimension	Score 1 - Limited	Score 2 - Moderate	Score 3 - High
NODE CRITICALITY Who was arrested?	Replaceable affiliate or low-tier support actor. Substitutable within 30 days.	Mid-tier operator or specialist such as an IAB operator, mule coordinator, or BPH contact. Substitutable with friction.	Non-substitutable node: RaaS core team member, key OTC broker, or protection-layer officer. Loss creates a sustained gap.
COOPERATION OUTPUT What did the arrest yield? Mark PENDING if debrief data is unavailable.	No cooperation. Or cooperation produced no actionable intelligence beyond the arrested actor's own operations.	Partial cooperation. Yielded some identity, infrastructure, or financial data enabling follow-on investigation.	Full cooperation. Enabled follow-on arrests, exposed financial records at scale, or produced protection-layer intelligence.
TRUST CASCADE	No observable disruption.	Localized disruption.	Broad cascade. Multiple

Dimension	Score 1 - Limited	Score 2 - Moderate	Score 3 - High
EFFECT What happened in the ecosystem?	Underground ecosystem continued without visible behavioral change.	Target's immediate network went dark, changed communications infrastructure, or showed elevated OPSEC behavior.	actors burned infrastructure, forum-level confidence disruption observed, or competing groups exploited the vacuum.
RECONSTITUTION IMPACT Could they rebuild?	Full reconstitution within 30 days at comparable or greater operational capacity.	Partial reconstitution at 31-90 days. Operating at reduced capacity or under a new brand with a smaller affiliate roster.	Failed or significantly delayed reconstitution. 90-plus days out, or successor brand still below 50% prior operational capacity at 180 days.

SCORING FORMULA AND CALIBRATION EXAMPLES

WAIS = Sum of four-dimension scores. Range: 4-12. Cooperation Output may be marked PENDING until debrief is complete.

Score 10-12: High ecosystem impact. Report as strategic-level success at macro layer.

Score 7-9: Moderate impact. Report as significant operational success at meso layer.

Score 4-6: Limited ecosystem impact. Report as operational activity. Do not inflate to strategic narrative.

Multi-arrest coordinated operations: score each arrest individually, then apply a +2 coordination bonus to the highest single WAIS score in the operation.

Calibration examples:

LockBit core administrator arrest: Node Criticality 3, Cooperation Output PENDING until debrief complete, Trust Cascade 3, Reconstitution Impact scored at 90 days. Expected range: 9-11.

Mid-tier IAB operator, third-country arrest, no cooperation: Node Criticality 2, Cooperation Output 1, Trust Cascade 1-2, Reconstitution Impact 2. Expected range: 6-7.

Single replaceable affiliate, no cooperation, full reconstitution within 30 days: Score 4-5. Do not present as ecosystem-level progress.

KPI B-2 | FSB/RIS Internal Strife Indicators: Two-Layer Architecture

Reliability: ● **ANALYST INFERENCE**

Internal strife cannot be systematically quantified. It can be systematically detected and classified. This KPI uses a two-layer architecture: proxy metrics for STRAT reporting and an event log for IC-level analysis.

INTERPRETATION WARNING

Layer 1 proxy metrics are interpreted only in context of the event log and node-level pressure data. Do not treat small quarter-to-quarter changes in any single proxy metric as a standalone signal. A single exit scam or a brief spike in forum dispute volume is noise until corroborated by event log entries or corresponding meso-layer pressure data. The event log is primary. The proxy metrics are a quick visual summary.

Layer 1 Proxy Metrics (Quantitative, Directional)

Proxy Metric	What It Measures	Confidence	Data Source
Affiliate defection rate	New group formations by known former affiliates of a disrupted brand within 90 days of disruption	CREDIBLE	Intel 471, Flashpoint, underground monitoring
Exit scam frequency	Admin wallet disappearances or sudden site closures not attributed to law enforcement action, per quarter. Distinguish from LE takedowns using Chainalysis wallet analysis.	CREDIBLE	Chainalysis, TRM, underground forum monitoring
Forum dispute volume	Arbitration requests and accusation threads against specific actors on Exploit and XSS. Track by target actor and time proximity to pressure actions.	CREDIBLE	Intel 471, Flashpoint
New RaaS brand emergence rate	Count of new RaaS brand launches per quarter. Rising fragmentation after a disruption is a strife or pressure cascade signal. Consolidation indicates ecosystem recovery.	ANALYST INFERENCE	Ransomlook, Ransomwatch, private sector threat intel
Recruitment term shifts	Changes in advertised affiliate split percentages or targeting rule relaxation. Sudden improvements in affiliate terms signal internal pressure to retain operators.	ANALYST INFERENCE	Underground forum monitoring, Intel 471

Layer 2 Strife Event Log (IC-Level Analysis)

Qualitative structured entries. This is the primary IC-value product. The Conti leak is the canonical reference: not a number, but an event whose ecosystem effects were measurable in the aftermath.

Field	Content
Event Type	Leak / Public Dispute / Exit Scam / Defection / Arrest-Triggered Fragmentation / Handler Complaint / Dox of Internal Actor
Source Reliability	CONFIRMED / CREDIBLE / ANALYST INFERENCE
Actors Involved	Actor handles and group affiliations. Move to controlled annex if named individually.
Ecosystem Effect Assessment	Did it produce operational disruption? Trust breakdown? Leadership vacuum? Krysha withdrawal?
Causal Link to Pressure Actions	Which prior disruption action, if any, preceded this event? Time lag?
Follow-On Indicators to Monitor	What should be watched in the next 30-90 days because of this event?

THEME C

Fewer Payments and Worse Economics. Degrade the business model, not just individual brands.

KPI C-1 | Ransom Payment Volume vs. Victim Count (Divergence Metric)

Reliability: ● **CREDIBLE**

Definition: Directional trend of total ransom payments against total victim count. The operationally meaningful signal is divergence. When victim counts hold steady or rise while payment volume falls, the business model is degrading independent of attack frequency. Payment volume alone is insufficient.

- **Formula:** Quarterly - payment volume trend plotted against victim count trend. Report the divergence ratio, not just one line.
- **Crypto price normalization:** Payment volume is tracked in USD but interpreted with awareness of major crypto-market movements. Large exogenous price swings are annotated in the pressure-effect ledger and are not attributed as disruption effects. A payment volume drop driven by a Bitcoin price collapse is not a KPI success.
- **Data Sources:** Chainalysis Crypto Crime Report (annual with mid-year updates), TRM Labs Illicit Crypto Report, leak site victim counts via Ransomlook and Ransomwatch
- **Known Limitation:** Structural undercounting is real and complicated. Monero payments, unreported incidents, and private negotiations are invisible. This metric is a directional trend only. Do not treat absolute figures as precise. Labeled CREDIBLE, not CONFIRMED.
- **Maturity:** LEVEL 1. Chainalysis and TRM data available now.

KPI C-2 | Victim Payment Rate by Sector

Reliability: ● **CREDIBLE**

Definition: Percentage of confirmed victims who paid ransom, tracked by sector (critical infrastructure, healthcare, financial services, general commercial). Declining payment rates indicate improved resilience or increased payment-discouragement policy effectiveness.

- **Formula:** Confirmed payments divided by confirmed victim incidents per sector, per quarter. Trend over rolling 4-quarter window.
- **Data Sources:** Coveware Ransomware Marketplace Report (quarterly), IR firm case data from Mandiant and CrowdStrike, sector Information Sharing and Analysis Center (ISAC) reporting
- **Known Limitation:** Denominator (total victim incidents) is significantly undercounted due to non-reporting. Sector breakdowns are approximate. Treat as directional.
- **Maturity:** LEVEL 1. Coveware quarterly data available.

KPI C-3 | Leak Site Three-Signal Composite

Reliability: ● **CONFIRMED**

Leak sites are the highest-quality real-time signal in the open-source environment. Three distinct signals are tracked independently. They measure different things and should not be collapsed into a single number.

Signal	What It Measures	Directional Interpretation	Confidence
Post Volume	Number of victims published per month across all active leak sites	Decrease signals operational tempo degradation or increased payments. Increase signals ecosystem health or escalating extortion pressure.	CONFIRMED
Time-to-Publish	Gap between confirmed compromise date and leak site	Compression means groups are escalating pressure because	CREDIBLE

Signal	What It Measures	Directional Interpretation	Confidence
	publication date	victims are not paying fast enough. Extension means victims are paying more readily or groups are operationally slower.	
Takedown/Relaunch Cycle	Time between a site going dark and a functional successor or replacement appearing	Longer cycle means higher resilience cost imposed. Sustained failure to relaunch indicates ecosystem degradation.	CONFIRMED

- **Data Sources:** Ransomlook, Ransomware.live, Ransomwatch, DarkFeed, cross-validated for accuracy
- **Known Limitation:** Measures published victims only. Groups collecting ransom without publishing are invisible here. Post volume is a floor, not a ceiling.
- **Maturity:** LEVEL 1. Open source, available now.

SECTION 3 | MESO LAYER: NODE CLUSTER METRICS

Meso-layer metrics are the causal attribution layer. When a macro metric moves, the meso layer explains why. Without it, macro numbers are undefendable in a STRAT briefing or oversight context. Node IDs map directly to the companion disruption playbooks (Phase A Nodes 01-03, Phase B Nodes 04/07/08, Phase C Nodes 05/06/09). Three clarifications. First, the marketplace-health cluster below is tracked as a supplement to Node 07; Dependency Map Node 11 (Crypter/Packer Services) carries no meso metric and is addressed through private-sector detection levers. Second, there is no M-06 metric ID: leak-site measurement is consolidated under KPI C-3 and rolled up in the Node 06 row. Third, Node 16 (Exploit/Vulnerability Brokers), added to the Dependency Map per Module 06, is not yet tracked at the meso layer and requires a policy-track metric set at the next framework revision.

DESIGN PRINCIPLE

Each node cluster has a designated owner responsible for metric population. Where ownership is currently unassigned, this document explicitly marks the gap. Visible gaps are budget arguments and interagency forcing functions, not deficiencies to be hidden.

Node	Priority	Key Metrics	Owner	Level
Node 01: OTC Crypto Brokers	CRITICAL	Percentage of top-20 OTC brokers under active designation. Average days to substitute broker identification post-designation. Volume of blockchain-attributed flows through designated vs. non-designated nodes.	OFAC / Treasury / Chainalysis	L1/L2
Node 02: High-Risk Exchanges	CRITICAL	Count of VASP enhanced-due-diligence referrals acted on. Proportion of ransomware-attributed withdrawal addresses flagged at exchange level. Correspondent banking friction events.	Treasury / FinCEN / FVEY financial partners	L1
Node 03: Bulletproof Hosting	CRITICAL	Average time-to-reconstitution post-takedown for BPH providers. Count of active providers vs. baseline. Infrastructure cost inflation proxy via new provider emergence rate.	FBI / NCA / Shadowserver	L1
Node 04: IAB Markets	HIGH	Monthly IAB listing volume on Exploit and XSS. Average asking price by access type (RDP, VPN, domain admin). Top-10 operator churn rate. Victim notification success rate.	Intel 471 / Flashpoint / CISA	L1
Node 05: Botnet/Loaders	HIGH	Time-to-reconstitution post-sinkhole, using the QakBot operation as the reference model. Infected host count reduction post-operation. Distribution infrastructure disruption events. Successor loader emergence lag.	FBI / NCA / Europol / national CERTs	L1/L2

Node	Priority	Key Metrics	Owner	Level
Node 06: Leak Site Hosting	HIGH	Rolled up from KPI C-3 leak site three-signal composite (Ransomlook, Ransomware.live, Ransomwatch, DarkFeed). Hosting provider churn rate post-takedown. Geographic migration patterns.	FBI / Europol / FVEY LE	L1
Node 07: Underground Trust Infrastructure	HIGH	Forum arbitration dispute volume. Escrow failure rate. Market exit scam frequency. Active forum health score using member activity and post volume.	Intel 471 / Flashpoint	L1
Node 08: Mixing/Obfuscation Services	HIGH	Count of active mixing services vs. baseline. Designation rate. Post-designation fund migration patterns. Time to substitute service identification.	Chainalysis / TRM / OFAC	L1
Node 09A: Mule Networks (Russia-Domestic)	HIGH	FNS anomalous lifestyle flags on mule accounts. CBR 115-FZ actions against mule front accounts. Domestic laundering pattern visibility vs. baseline.	Rosfinmonitoring / FNS / CBR channel	L2
Node 09B: Mule Networks (Third-Country)	HIGH	MLAT referral count and action rate. Third-country prosecution packages filed. Crypto-to-fiat nexus linkages confirmed.	FVEY LE / Europol / MLAT partners	L1/L2
Node 10: Stealer/Credential Markets	MEDIUM	Directional only: major stealer takedowns and observed IAB price response at a 60-90 day lag. Credential market listing volume trend. Attribution distance is high. Treat as ANALYST INFERENCE.	Intel 471 / Flashpoint / private sector	L1 (ANALYST INFERENCE)
Node 07 supplemental: Underground Marketplaces	MEDIUM	Forum health score trend. Migration events from forum to Telegram. New forum emergence rate. Migration must be tracked, not just the forum. A forum going dark does not equal disrupted.	Intel 471 / Flashpoint	L1 (ANALYST INFERENCE)

SECTION 4 | MICRO LAYER: PER-OPERATION LOG TEMPLATE

Every disruption action generates a micro-layer log entry. This is the foundational data that makes meso and macro metrics defensible. If this layer is not populated, the framework loses its causal chain.

The owning team or agency populates this log at three points: pre-action (expected effects), immediately post-action (observed immediate effects), and at 30, 90, and 180-day follow-up for reconstitution tracking.

Field	Content	When Populated
Operation ID	Unique identifier. Links to meso and macro tracking.	Pre-action
Target Node(s)	Which node(s) does this action target? Reference Section 3 node taxonomy and companion playbook phase.	Pre-action
Action Type	Designation / Takedown / Sinkhole / Referral / Arrest / Journalism Pipeline / Infrastructure Disruption	Pre-action
Expected Primary Effect	Specific observable effect expected within 30 days. Be precise.	Pre-action
Expected Secondary Effect	Compounding effect expected at 60-90 days, including interaction with other active pressure.	Pre-action
Backfire Risk Assessment	Low / Medium / High. Reference engagement triggers in companion playbooks.	Pre-action
Observed Immediate Effect	What actually happened within 30 days. Annotate divergence from expected.	30-day follow-up
Reconstitution Status at 90 Days	Full / Partial / Failed. Detail the form of reconstitution.	90-day follow-up
Reconstitution Status at 180 Days	Full / Partial / Failed. Flag if successor is same actor under a new brand.	180-day follow-up
WAIS Score (if arrest)	Weighted Arrest Impact Score. Populate all four dimensions per Section 2 KPI B-1. Mark Cooperation Output as PENDING if debrief is incomplete.	Post-arrest, updated at 90 days
Trust Cascade Observed	Yes / No / Partial. Describe observable underground forum or actor behavior changes.	30 and 90-day follow-up
Protection Layer Effect	Did this action affect any known krysha relationship? Describe status change if applicable.	90-day follow-up Level 2
Feed to Meso Metric	Which meso-layer node cluster metric does this entry update? List specific metric.	Post-population

SECTION 5 | INTERNAL STRIFE ARCHITECTURE

MEASUREMENT PRINCIPLE

Internal strife cannot be systematically quantified. It can be systematically detected and classified. The goal is not a strife index. The goal is a structured detection system that makes strife legible for STRAT reporting and preserves IC-level signal fidelity.

The STRAT-reportable output is not 'internal strife: high.' It follows a specific action, affiliate defection rate increased, two new splinter brands emerged within 60 days, and forum dispute volume against the targeted group spiked. Assessment: pressure-induced trust breakdown. Confidence: CREDIBLE.

5.1 Layer 1: Proxy Metrics (STRAT Reporting Layer)

Quantitative but directional. These do not measure strife directly. They measure conditions that strife produces or precedes. All carry ANALYST INFERENCE to CREDIBLE confidence. Do not interpret any single proxy metric as a standalone signal.

Metric	Operational Definition	Confidence	Data Source
Affiliate Defection Rate	New group formations by known former affiliates of a disrupted brand within 90 days. Count per disruption event and as quarterly aggregate.	CREDIBLE	Intel 471, Flashpoint, underground monitoring
Exit Scam Frequency	Admin wallet disappearances or site closures not attributed to LE action. Distinguish from law enforcement takedowns using Chainalysis wallet analysis.	CREDIBLE	Chainalysis, TRM, underground forum monitoring
Forum Dispute Volume	Arbitration requests and accusation threads against specific actors on Exploit and XSS. Track by target actor and time proximity to pressure actions.	CREDIBLE	Intel 471, Flashpoint
New RaaS Brand Emergence Rate	Count of new RaaS brand launches per quarter. Rising fragmentation after a disruption is a strife or pressure cascade signal. Consolidation indicates ecosystem recovery.	ANALYST INFERENCE	Ransomlook, Ransomwatch, private sector threat intel
Recruitment Term Shifts	Changes in advertised affiliate split percentages or targeting rule relaxation. Sudden improvements in affiliate terms signal internal pressure to retain operators.	ANALYST INFERENCE	Underground forum monitoring, Intel 471

5.2 Layer 2: Strife Event Log (IC-Level Analysis)

Qualitative structured entries. This is the primary IC-value product. Events are episodic and source dependent. The event log is the analytic anchor. Proxy metrics summarize its contents for STRAT audiences.

Event Type	Definition and Examples
LEAK	Internal communications, financial records, or operational data exposed, whether voluntarily by a disgruntled affiliate or involuntarily through LE or IC action. The Conti leaks (2022) and Black Basta leaks are reference examples.
PUBLIC DISPUTE	Open accusation threads, arbitration failures, or public naming of internal actors on underground forums or Telegram. Signals trust breakdown at affiliate or operator level.
EXIT SCAM	Admin-level wallet disappearance with no LE attribution. Indicates internal collapse or deliberate abandonment of brand, often preceding a rebrand under a new identity.
DEFECTION EVENT	Confirmed departure of affiliates or key operators to a competing group, with observable operational continuity under a new brand.
ARREST-TRIGGERED FRAGMENTATION	Following an arrest, observable disintegration of the affected group's operational structure. Distinct from temporary disruption. Measured by 90-day reconstitution failure or splinter emergence.
HANDLER COMPLAINT	Criminal actor publicly threatening to expose a handler, switching protection patrons, or demonstrating loss of confidence in a krysha relationship. Rare but high-signal.
DOX OF INTERNAL ACTOR	Identity or financial exposure of a core team member, protection officer, or key service provider through journalism, rival actors, or LE action.

SECTION 6 | WEIGHTED ARREST IMPACT SCORE, SCORING GUIDE

The WAIS translates arrest and prosecution events into ecosystem-effect assessments. A single affiliate arrest and a coordinated RaaS core team takedown are not the same event. WAIS makes that distinction explicit and defensible.

Dimension	Score 1 - Limited	Score 2 - Moderate	Score 3 - High
NODE CRITICALITY Who was arrested?	Replaceable affiliate or low-tier support actor. Substitutable within 30 days.	Mid-tier operator, specialist (IAB operator, mule coordinator, BPH contact). Substitutable with friction.	Non-substitutable node: RaaS core team member, key OTC broker, protection-layer officer. Loss creates a sustained gap.
COOPERATION OUTPUT What did the arrest yield? Mark PENDING if debrief data is unavailable.	No cooperation. Or cooperation produced no actionable intelligence beyond the arrested actor's own operations.	Partial cooperation. Yielded some identity, infrastructure, or financial data enabling follow-on investigation.	Full cooperation. Enabled follow-on arrests, exposed financial records at scale, or produced protection-layer intelligence.
TRUST CASCADE EFFECT What happened in the ecosystem?	No observable disruption. Underground ecosystem continued without visible behavioral change.	Localized disruption. Target's immediate network went dark, changed communications infrastructure, or showed elevated OPSEC behavior.	Broad cascade. Multiple actors burned infrastructure, forum-level confidence disruption observed, or competing groups exploited the vacuum.
RECONSTITUTION IMPACT Could they rebuild?	Full reconstitution within 30 days at comparable or greater operational capacity.	Partial reconstitution at 31-90 days. Operating at reduced capacity or under a new brand with a smaller affiliate roster.	Failed or significantly delayed reconstitution. 90-plus days out, or successor brand still below 50% prior operational capacity at 180 days.

SCORING FORMULA

WAIS = Sum of four dimension scores. Range: 4-12. Cooperation Output may be marked PENDING until debrief is complete.

Score 10-12: High ecosystem impact. Report as strategic-level success at macro layer.

Score 7-9: Moderate impact. Report as significant operational success at meso layer.

Score 4-6: Limited ecosystem impact. Report as operational activity. Do not inflate to strategic narrative.

Multi-arrest coordinated operations: score each arrest individually, then apply a +2 coordination bonus to the highest single WAIS score in the operation.

SECTION 7 | OWNERSHIP MAP

Ownership defines accountability. Every metric requires an agency or team responsible for population, maintenance, and quality control. Where ownership is currently unassigned, this document identifies the gap explicitly. Gaps are not deficiencies. They are the interagency coordination agenda.

Metric / Layer	Designated Owner	Status	Gap / Note
KPI A-1: Russian domestic enforcement actions	Open-source: Analyst team with RU investigative journalism access	L1 AVAILABLE	Seeded-referral attribution requires IC reporting feed. L2 gap.
KPI A-2: Referral-to-action lag	Owning operational team (internal log)	L2 PENDING	Requires formal internal operation log mandate. No current owner.
KPI A-3: Protection relationship inventory	IC analytic team - controlled annex	L2 PENDING	Requires classified reporting feed and analytic annex governance structure.
KPI B-1: WAIS scoring	Owning agency per arrest, aggregated by framework coordinator	L1/L2 PARTIAL	Node criticality and reconstitution: L1. Cooperation output: L2 pending debrief access.
KPI B-2: Strife proxy metrics	Intel 471 / Flashpoint primary, IC supplementary	L1 AVAILABLE	Event log requires dedicated analytic owner. Currently unassigned.
KPI C-1: Payment volume vs. victim count	Framework coordinator - Chainalysis and TRM primary sources	L1 AVAILABLE	Annual cadence from public sources. Quarterly cadence requires subscription access.
KPI C-2: Victim payment rate by sector	Framework coordinator - Coveware primary	L1 AVAILABLE	Sector breakdown granularity is Coveware-dependent. May require direct engagement.
KPI C-3: Leak site three-signal composite	Framework coordinator: Ransomlook, Ransomware.live, and Ransomwatch	L1 AVAILABLE	Automated tracking recommended at scale.
Node 01-02: OTC and Exchange metrics	OFAC / Treasury / Chainalysis	L1 AVAILABLE	Designation pipeline coordination with OFAC required for real-time tracking.
Node 03: BPH reconstitution	FBI / NCA / Shadowserver	L1 AVAILABLE	Post-action follow-up protocol required. Currently ad hoc.
Node 04: IAB market metrics	Intel 471 / Flashpoint / CISA	L1 AVAILABLE	Victim notification program requires ISAC coordination for closure rate tracking.
Node 05: Botnet/loader metrics	FBI / NCA / Europol / CERTs	L1/L2 PARTIAL	IC equities review protocol required before sinkhole victim data use.
Node 07: Underground trust metrics	Intel 471 / Flashpoint	L1 AVAILABLE	No current gap.
Node 08: Mixing and	Chainalysis / TRM / OFAC	L1 AVAILABLE	Requires OFAC designation

Metric / Layer	Designated Owner	Status	Gap / Note
obfuscation metrics			pipeline access for real-time tracking.
Node 09A: Domestic mule networks	Rosfinmonitoring / FNS / CBR channel	L2 PENDING	Highest-priority unassigned gap. Requires formal back-channel relationship.
Node 09B: Third-country mule networks	FVEY LE / Europol	L1/L2 PARTIAL	MLAT referral tracking requires formal reporting from partner agencies.
Node 10 / marketplace supplemental: Stealers and Marketplaces	Intel 471 / Flashpoint (ANALYST INFERENCE)	L1 AVAILABLE	Treat as indicative only. Attribution distance too high for operational weighting.
Micro-layer operation logs	Owning agency per action. No current aggregator.	L2 PENDING	CRITICAL GAP: Without a designated log aggregator, the causal chain from micro to macro cannot be maintained.

SECTION 8 | GOVERNANCE

8.1 Distribution Tiers

Tier	Content	Distribution
TIER 1: Leadership Dashboard	Macro KPIs (Themes A, B, C) with meso trend summaries. Confidence labels required on every metric. No individual officer names.	Senior IC/LE leadership, STRAT offices
TIER 2: Operational Reference	Full framework including meso node metrics, micro log template, WAIS scoring guide, strife proxy metrics	Interagency working groups, operational and analytic leads
TIER 3: Controlled Analytic Annex	Protection relationship inventory with individual officer and unit detail, event log with sourced entries, cooperation output data from debrief records	Restricted. Analytic teams with appropriate authorities only.

8.2 Protection-Layer Panel: Governance Note

MANDATORY GOVERNANCE REQUIREMENT

The protection-layer KPIs (KPI A-3, strife event log entries involving officers, Node 09A domestic mule tracking) are analytic products, not targeting directives. Any operational use of protection-layer analytic outputs must go through existing agency authorities and approval processes. This framework does not constitute operational authorization.

- At the Tier 1 leadership level: report counts and status categories only, for example '4 protection relationships assessed as strained this quarter.' No individual names.
- Individual officer-level data is maintained in the Tier 3 controlled analytic annex under existing foreign-intelligence minimization rules.
- Officer-level metrics are counts and trendlines of cases and relationship states, not a targeting panel.
- Sanctions packages are built from underlying case files with appropriate legal authority. The KPI summarizes the status of those packages. It does not drive them.
- If protection-layer analysis surfaces data on domestic persons of any nationality, apply standard minimization procedures immediately.

8.3 Analytic vs. Operational Distinction

This framework is analytic input for operational planning. It does not supersede agency-specific legal authorities or protocols. The KPI outputs are measurement and accountability tools.

- This framework does not constitute intelligence products for targeting.
- It does not replace agency-specific operational authorization requirements.
- It does not override classification and handling requirements for any underlying source material.
- Red flag: using macro KPI movements as justification for specific new operational authorities without showing corresponding micro and meso-level evidence. A macro number moving in the right direction is not sufficient basis for expanded authorities. The causal chain must be shown.

8.4 Framework Maintenance

- Review cadence: quarterly metric review, annual framework structure review
- Version control: maintained by framework coordinator. Changes require interagency working group concurrence.

- Metric retirement: any metric that cannot be populated with reliable data for three consecutive quarters is flagged for review and potential retirement or downgrade to ANALYST INFERENCE.
- Ownership gap resolution: unassigned Level 2 metrics are reviewed at each quarterly meeting for ownership assignment progress. Gaps are reported to senior leadership as interagency coordination requirements, not silently carried forward.

ANNEX A | QUICK REFERENCE: ALL KPIs

All KPIs are scoped to Russia/CIS-linked ransomware and associated enabling infrastructure unless otherwise specified.

KPI ID	Name	Theme	Confidence	Level
A-1	Russian Domestic Actions Against Ecosystem Actors	Domestic Enforcement	CREDIBLE	L1/L2
A-2	Referral-to-Action Lag	Domestic Enforcement	CREDIBLE	L2
A-3	Protection Relationship Status Inventory	Domestic Enforcement	ANALYST INFERENCE	L2
B-1	Weighted Arrest Impact Score (WAIS)	FSB/RIS Strife	CONFIRMED/CREDIBLE	L1/L2
B-2a	Strife Proxy Metrics: Layer 1	FSB/RIS Strife	ANALYST INFERENCE to CREDIBLE	L1
B-2b	Strife Event Log: Layer 2	FSB/RIS Strife	VARIES	L2
C-1	Payment Volume vs. Victim Count Divergence	Ecosystem Economics	CREDIBLE	L1
C-2	Victim Payment Rate by Sector	Ecosystem Economics	CREDIBLE	L1
C-3a	Leak Site Post Volume	Ecosystem Economics	CONFIRMED	L1
C-3b	Leak Site Time-to-Publish	Ecosystem Economics	CREDIBLE	L1
C-3c	Leak Site Takedown/Relaunch Cycle	Ecosystem Economics	CONFIRMED	L1
M-01	OTC Broker Designation Coverage	Node Pressure - Financial	CONFIRMED	L1
M-02	Exchange VASP Friction Metrics	Node Pressure - Financial	CONFIRMED	L1
M-03	BPH Reconstitution Speed	Node Pressure - Infrastructure	CONFIRMED	L1
M-04	IAB Market Volume and Pricing	Node Pressure - Access	CREDIBLE	L1
M-05	Botnet/Loader Reconstitution	Node Pressure - Delivery	CONFIRMED	L1/L2
M-07	Underground Trust Health	Node Pressure - Trust	CREDIBLE	L1
M-08	Mixer/Obfuscation Service Coverage	Node Pressure - Financial	CONFIRMED	L1
M-09A	Domestic Mule Network Visibility	Node Pressure - Laundering	CREDIBLE	L2

KPI ID	Name	Theme	Confidence	Level
M-09B	Third-Country Mule Prosecution Packages	Node Pressure - Laundering	CREDIBLE	L1/L2
M-10	Stealer/Credential Market Trends	Node Pressure - Supply	ANALYST INFERENCE	L1
M-11	Underground Marketplace Health	Node Pressure - Trust	ANALYST INFERENCE	L1