RANSOMWARE ECOSYSTEM DISRUPTION FRAMEWORK

Group Pressure Tracking Template

Version 0.2 | June 2026 | Working Document

Developed by Reno

HOW TO USE THIS TEMPLATE

This template is the operational instrument for group-level pressure tracking. When a working group initiates sustained operations against a specific ransomware actor or brand, this template is opened and populated from the start. It runs alongside the per-operation micro-layer log entries in the KPI framework.

The template serves two audiences: the operational team maintaining situational awareness on the target group, and leadership who need a pre/post picture of what specific pressure is producing against a specific actor.

RELATIONSHIP TO THE KPI FRAMEWORK

This template sits between the micro layer (per-operation logs) and the meso layer (node cluster metrics) in the KPI framework architecture.

Micro-layer operation logs document individual actions against this group. This template aggregates those actions and tracks the cumulative effect on the target group specifically.

Meso-layer node metrics track ecosystem-wide pressure. This template tracks group-specific effects that contribute to those meso metrics.

Leadership receives this template as a group-level summary, not a node-level or ecosystem-level report.

Population Instructions

- Open one template per active target group. Do not combine multiple groups in a single template.
- Populate Section 1 (Group Profile) before any pressure actions begin. This establishes the baseline.
- Populate Section 2 (Baseline Metrics) before any pressure actions begin. Baselines cannot be established retroactively.
- Update Section 3 (Pressure Action Log) after every action against this group.
- Update Section 4 (Observed Effects Tracker) at 30, 90, and 180-day intervals from the date of first action.
- Section 5 (WAIS Log) is populated only when an arrest occurs involving this group.
- Section 6 (Strife Event Log) is populated when any strife event type is observed.
- Section 7 (Assessment) is completed at each 90-day review cycle.

SECTION 1 | GROUP PROFILE

Populate before operations begin. Update when material changes are observed.

Group Name / Handle	Primary name and known aliases
Template ID	Unique identifier for this tracking file
Date Opened	Date this template was initiated
Owning Team / Agency	Primary team responsible for population
Operational Model	RaaS franchise / Closed hierarchical / Independent affiliate / Other
Estimated Active Since	Approximate date of first confirmed activity
Lineage	Known predecessor groups or personnel origins (e.g., former Conti operators)
Estimated Affiliate Count	Point-in-time estimate at template opening. Confidence level.
Primary RaaS Platform	If applicable: Exploit, XSS, private recruitment, or other
Known Operating Geography	Primary actor geography based on available intelligence

Node Exposure Assessment

For each ecosystem node, assess the target group's current dependency and known infrastructure. This drives which nodes to prioritize for pressure.

Node	Dependency Level	Known Infrastructure / Actors	Substitutability	Priority
Node 01: OTC Brokers	High / Medium / Low / Unknown		High / Medium / Low	
Node 02: High-Risk Exchanges	High / Medium / Low / Unknown		High / Medium / Low	
Node 03: BPH	High / Medium / Low / Unknown		High / Medium / Low	
Node 04: IAB Markets	High / Medium / Low / Unknown		High / Medium / Low	
Node 05: Botnet/Loaders	High / Medium / Low / Unknown		High / Medium / Low	
Node 06: Leak Site	High / Medium / Low / Unknown		High / Medium / Low	

Node	Dependency Level	Known Infrastructure / Actors	Substitutability	Priority
Node 07: Underground Trust	High / Medium / Low / Unknown		High / Medium / Low	
Node 08: Mixers	High / Medium / Low / Unknown		High / Medium / Low	
Node 09: Mule Networks	High / Medium / Low / Unknown		High / Medium / Low	

Protection Layer Assessment

Krysha Relationship Status	Active / Strained / Broken / Unknown / None Assessed
Assessed Protecting Entity	FSB unit / officer / MVD / Other / Unknown. Move specifics to Tier 3 annex.
Confidence Level	CONFIRMED / CREDIBLE / INDICATIVE
Protection Evidence Basis	Brief description of evidence basis. Full sourcing in controlled annex.
Backfire Risk Assessment	Low / Medium / High. Reference companion playbook engagement triggers.

SECTION 2 | BASELINE METRICS

Establish before any pressure actions begin. These are the pre-action reference points against which all observed effects will be measured. A baseline that cannot be established is marked UNKNOWN, not estimated.

BASELINE INTEGRITY RULE

Baselines must be established before the first action. Retroactive baseline establishment is not permitted because actions may already have affected the indicators. If a baseline cannot be established before action commences, mark it UNKNOWN and note the date of first action. Future measurements will be relative to the first post-action observation, which must be clearly labeled as such.

Operational Tempo Baseline

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
Leak site post volume (monthly average, 90-day window)					
Average time-to-publish (days from compromise to publication)					
Estimated active affiliate count					
Average ransom demand (USD, reported cases)					
Victim payment rate (confirmed payments / confirmed incidents)					
Average ransom demand fulfillment rate					

Financial Infrastructure Baseline

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
Primary OTC broker nodes (count of identified)					
Attributed wallet cluster activity (monthly volume, USD estimate)					
Primary mixing service usage (identified services)					
OFAC-designated wallet percentage (of attributed wallets)					

Access and Delivery Infrastructure Baseline

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
IAB sourcing pattern (primary forums and volume)					
Average IAB access cost (USD, by access type if available)					
BPH provider count (identified hosting nodes)					
Loader/botnet dependency (primary delivery mechanism)					

Underground Trust and Forum Health Baseline

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
Forum reputation score (Exploit/XSS, if available)					
Active dispute threads against group on monitored forums					
Affiliate recruitment activity (posts per month, approximate)					
Current affiliate split percentage (advertised)					

SECTION 3 | PRESSURE ACTION LOG

Add one row per action targeting this group. Cross-reference the operation ID to the micro-layer log entry in the KPI framework. Do not duplicate the full micro-layer log here: record the action type, expected effect, and reference the micro-layer entry for detail.

Date	Operation ID	Action Type	Target Node(s)	Expected Primary Effect (30 days)	Backfire Risk	Micro-Layer Log Ref
		Designation / Takedown / Sinkhole / Referral / Arrest / Journalism / Infrastructure			Low / Med / High	

SECTION 4 | OBSERVED EFFECTS TRACKER

Update at 30, 90, and 180 days from the date of first action. Compare against baselines in Section 2. Annotate any divergence from expected effects.

4.1 Operational Tempo Effects

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
Leak site post volume vs. baseline	See Section 2				
Time-to-publish vs. baseline	See Section 2				
Active affiliate count vs. baseline	See Section 2				
Average ransom demand vs. baseline	See Section 2				
Victim payment rate vs. baseline	See Section 2				

4.2 Financial Infrastructure Effects

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
OTC broker nodes active vs. baseline	See Section 2				
Attributed wallet activity vs. baseline	See Section 2				
Mixing service usage vs. baseline	See Section 2				
Designated wallet percentage vs. baseline	See Section 2				

4.3 Access and Delivery Effects

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
IAB access costs vs. baseline	See Section 2				
BPH provider count vs. baseline	See Section 2				
Loader/botnet delivery capacity vs. baseline	See Section 2				

4.4 Underground Trust Effects

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
Forum dispute volume vs. baseline	See Section 2				

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
Affiliate recruitment activity vs. baseline	See Section 2				
Affiliate split percentage vs. baseline	See Section 2				
New brand/splinter emergence	None at baseline				

4.5 Divergence Notes

Record any significant divergence between expected and observed effects here. Include the operation ID, the expected effect, what was actually observed, and a brief assessment of why the divergence occurred.

Date	Operation ID	Expected Effect	Observed Effect	Divergence Assessment

SECTION 5 | WAIS LOG

Populate when an arrest involving this group occurs. Score each arrest individually. Reference the full WAIS scoring guide in the KPI framework document, Section 6.

Field	Arrest 1	Arrest 2	Arrest 3
Operation ID / Date			
Actor Role / Node Criticality Score (1/2/3)			
Cooperation Output Score (1/2/3 or PENDING)			
Trust Cascade Effect Score (1/2/3)			
Reconstitution Impact Score (1/2/3)			
WAIS Total			
Coordination Bonus Applied (+2)?			
Final WAIS (with bonus if applicable)			
WAIS Category (High/Moderate/Limited)			
90-Day Update Required?	Yes / No	Yes / No	Yes / No

Cooperation Output PENDING follow-up:

Arrest ID	PENDING Since	Debrief Expected Date	Update When Available

SECTION 6 | STRIFE EVENT LOG

Populate when any strife event is observed involving this group. Use the event types defined in the KPI framework Section 5.2. Each event gets one row. Add rows as needed.

Date	Event Type	Source Reliability	Description	Ecosystem Effect Observed	Causal Link to Actions	Follow-On Indicators to Watch
	LEAK / PUBLIC DISPUTE / EXIT SCAM / DEFECTION / ARR-TRIGGERED FRAG / HANDLER COMPLAINT / DOX	CONFIRMED / CREDIBLE / INDICATIVE				

SECTION 7 | ASSESSMENT

Complete at each 90-day review cycle. This is the leadership-reportable summary for this group. One page maximum. Designed for Tier 1 leadership dashboard use.

7.1 Current Group Status

Assessment Date	
Overall Group Status	Fully Operational / Degraded / Significantly Degraded / Inactive / Dissolved
Operational Capacity vs. Baseline	Percentage estimate with confidence label
Financial Rail Status	Intact / Partially Disrupted / Significantly Disrupted
Protection Layer Status	Active / Strained / Broken / Unknown
Reconstitution Risk	Low / Medium / High. If high, what is enabling reconstitution?

7.2 Pressure Effect Summary

In plain language, what has the pressure campaign produced? What is working, what is not, and what is the next recommended action. Three to five sentences maximum.

7.3 Recommended Next Actions

Priority	Recommended Action	Target Node	Expected Effect	Owner
1				
2				
3				

7.4 KPI Framework Feed

Which macro and meso-layer KPIs are updated by this assessment? List the specific metrics and the direction of movement.

KPI ID	KPI Name	Direction of Movement	Confidence	Notes
		Improving / Worsening / No Change		

ANNEX A | EXAMPLE: PRE-POPULATED TEMPLATE (Qilin)

This annex shows what a partially populated template looks like for an active group. Qilin is used as the example because it is well-documented in open-source reporting and has been the dominant franchise since RansomHub went dark in April 2025 and its affiliate base dispersed. This is illustrative only: all data drawn from public sources, and fields that require operational intelligence are left blank. The RansomHub collapse that displaced the previous version of this example is itself a reference case for the Section 6 strife event log: an exit-scam-pattern shutdown, a public loyalty dispute, and affiliate migration to competing brands inside 60 days.

Section 1 Partial: Group Profile

Group Name / Handle	Qilin (formerly Agenda)
Template ID	EXAMPLE-QL-001
Date Opened	June 2026 (illustrative)
Operational Model	RaaS franchise. Open affiliate recruitment. Advertised affiliate split of 80 to 85 percent in favor of the affiliate, with added services (integrated DDoS capability, negotiation support) used as recruitment differentiators post-RansomHub. Confidence: CREDIBLE.
Estimated Active Since	Mid-2022 as Agenda; rebranded to Qilin by late 2022. Confidence: CONFIRMED.
Lineage	Original core assessed distinct from the Conti diaspora. Absorbed a significant share of displaced RansomHub affiliates after the April 2025 collapse; that roster itself carried former LockBit and BlackCat/ALPHV personnel. Confidence: CREDIBLE.
Estimated Affiliate Count	Unknown. Highest claimed-victim volume of any active brand since mid-2025; roster assessed large. Confidence: INDICATIVE.
Primary RaaS Platform	Private panel. Affiliate recruitment via Russian-language forums (RAMP primary) and direct outreach. Confidence: CREDIBLE.

Section 2 Partial: Operational Tempo Baseline (Illustrative)

> **NOTE**
> The following baseline values are drawn from open-source leak site tracking data (Ransomlook, Ransomware.live) and public reporting. They are illustrative of what a baseline entry looks like, not operational intelligence.

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
Leak site post volume (monthly average, trailing 12 months)	~100-120 victims/month; roughly 1,400 plus claims in the trailing 12 months (open-source trackers; tracker-dependent)				CREDIBLE
Average time-to-publish	~3-5 days post-compromise				INDICATIVE

Metric	Baseline (Pre-Action)	30-Day	90-Day	180-Day	Confidence
	(estimated)				
Estimated active affiliate count	Unknown. High volume suggests large roster.				INDICATIVE
Average ransom demand	Variable. High-value targets reported at $1M+				CREDIBLE

What a Pressure Campaign Against Qilin Would Track

Given the position Qilin holds as the dominant franchise since April 2025 and its absorption of displaced RansomHub affiliates, a pressure campaign would prioritize:

- Node 01 (OTC Brokers): identify and designate the OTC nodes serving Qilin admin wallet cash-out. With an 80/20 class split, admin flows run roughly 15 to 20 percent of ransom volume; at the current claim tempo that remains the highest-value financial target on the board.
- Node 04 (IAB Markets): monitor affiliate access purchasing patterns. A sustained claim tempo above 100 victims per month requires continuous access supply; IAB price increases and listing-volume reductions bite this group faster than lower-tempo brands.
- Node 07 (Underground Trust): the Qilin recruitment pitch rests on payment reliability and added services, marketed in direct contrast to the RansomHub collapse. Disrupting that reputation through escrow failures or dispute seeding is a high-value trust infrastructure action.
- Strife monitoring: watch for affiliate complaints about non-payment or delayed payment. Much of the roster has now survived two brand collapses (LockBit after Cronos, then RansomHub). Trust tolerance is minimal and strife indicators will surface fast; the April 2025 RansomHub end state, with the admin demanding a loyalty payment amid exit rumors, is the reference pattern.