RANSOMWARE ECOSYSTEM DISRUPTION FRAMEWORK

Historical Case Studies: KPI Framework Applied

Version 0.1 | April 2026 | Working Document

Developed by Reno

PURPOSE AND HOW TO USE THIS DOCUMENT

This document applies the Ransomware Ecosystem Disruption Measurement Framework retrospectively to five significant real-world operations and events. The purpose is threefold.

- Proof of concept: demonstrate that the KPI framework produces meaningful, defensible assessments when applied to documented events.
- Training: give analysts and operators a concrete reference for how to score events using the Weighted Arrest Impact Score (WAIS), how to read strife indicators, and how to connect node-level pressure to macro ecosystem effects.
- Baseline: establish reference points for what high-impact, moderate-impact, and limited-impact operations look like in practice, so future scoring is calibrated against real examples rather than abstract definitions.

IMPORTANT SCOPE NOTE

All analysis in this document draws exclusively on open-source reporting, public law enforcement disclosures, and blockchain forensics published by firms including Chainalysis and TRM Labs. No classified or law enforcement-sensitive material is incorporated. Confidence labels reflect the quality of available open-source evidence, not the totality of what may be known through other channels.

Each case study is structured identically: background, ecosystem role, framework layer analysis (macro/meso/micro), WAIS score where applicable, strife indicators observed, and key lessons for future operations.

Cases are presented in chronological order. The Conti case is the most thoroughly documented and serves as the primary calibration reference for the WAIS scoring system.

CASE STUDY 1 | CONTI COLLAPSE (2022)

Type: Internal Collapse triggered by External Leak | Date: February 2022 (leak) through mid-2022 (dissolution)

Background

Conti was among the most prolific and operationally sophisticated ransomware groups in documented history. Operating as a closed hierarchical RaaS with employed operators rather than independent affiliates, Conti was responsible for hundreds of confirmed attacks including multiple critical infrastructure incidents. At peak operation the group functioned as a structured criminal enterprise with departments, salaries, HR processes, and management hierarchy.

In February 2022, following Conti leadership's public statement of support for Russia's invasion of Ukraine, a disgruntled Ukrainian-affiliated member leaked approximately 60,000 internal chat messages, source code, and operational files. The leak exposed the group's internal structure, financial flows, personnel, infrastructure, and protection relationships in unprecedented detail.

Ecosystem Role at Time of Collapse

Dimension	Assessment
Node Criticality	Tier 1. Conti represented a non-substitutable brand at scale. Its closed operator model, established affiliate relationships, and infrastructure investment made it among the highest-replacement-difficulty actors in the ecosystem.
Revenue Share	Estimated 20-25% of total ransomware ecosystem revenue at peak operation, based on Chainalysis blockchain analysis of attributed wallet clusters.
Protection Layer Status	Active krysha relationship assessed. Internal chat logs surfaced in the leak referenced FSB contacts and protection payments. Relationship status post-leak: assessed as Strained then Broken as exposure became public.
Operational Model	Closed hierarchical group with employed operators. Approximately 100 personnel across technical, administrative, and operational functions based on leaked HR materials.

Framework Layer Analysis

Macro Layer Effects

- Payment volume: Chainalysis data shows Conti-attributed wallet activity dropped sharply through Q2-Q3 2022 as the brand dissolved. Total ecosystem payment volume did not fall proportionally, indicating rapid migration to successor brands.
- Victim count: leak site posting ceased within weeks of the internal collapse. No successor brand maintained the Conti name at operational scale.
- Domestic enforcement: no Russian domestic enforcement action against identified Conti principals has been publicly confirmed as of the date of this document.

Meso Layer Effects

Node	Observed Effect
Node 07: Underground Trust Infrastructure	Severe disruption. The leak exposed financial records, personnel identity, and internal dispute resolution processes. Forum trust in Conti-linked actors collapsed.

Node	Observed Effect
	Multiple former members reported being unable to establish new working relationships due to exposure risk.
Node 01: OTC Brokers	Partial disruption. Blockchain analysis identified several OTC nodes serving Conti. Post-collapse, fund flows through those nodes dropped. Some brokers subsequently served successor brands.
Node 04: IAB Markets	Moderate disruption. Conti's internal access sourcing model partially displaced IAB demand. Post-collapse, former Conti affiliates re-entered IAB markets as buyers, increasing demand temporarily.
Node 09: Mule Networks	Limited observable disruption. Laundering infrastructure for Conti proceeds largely persisted through successor relationships.

Micro Layer: Strife Event Log Entry

Field	Content
Event Type	LEAK
Source Reliability	CONFIRMED (60,000+ messages independently verified by multiple security researchers and journalists)
Actors Involved	Conti core leadership, approximately 100 operational personnel. FSB contact references surfaced. Specific officer identities not confirmed in open source.
Ecosystem Effect Assessment	Brand collapse within 90 days. Leadership vacuum filled by splinter brands. Trust breakdown across former affiliate and partner network. Protection relationship assessed as severed.
Causal Link to Pressure Actions	The leak was triggered by Conti leadership's political statement (Ukraine support declaration), not by a Western pressure action. External cause, but the cascading effects are consistent with what targeted exposure operations aim to produce.
Follow-On Indicators Observed	Black Basta emerged within 60 days of Conti dissolution, staffed by confirmed former Conti operators. Royal, Quantum, and BlackByte similarly incorporated former Conti personnel. Conti infrastructure was partially reused in successor operations before being abandoned.

Strife Proxy Metrics Observed

Metric	Observed Value	Signal
Affiliate Defection Rate	Near-total dissolution within 90 days	Maximum signal. Full fragmentation.
New RaaS Brand Emergence	5+ confirmed successor brands within 90 days	Highest fragmentation rate in documented ecosystem history.
Forum Dispute Volume	Significant spike in Exploit/XSS dispute threads involving Conti-linked handles in Q1-Q2 2022	Trust breakdown confirmed across multiple forum sources.
Exit Scam Frequency	Not applicable. Dissolution was involuntary, not admin-driven wallet exit.	N/A

Metric	Observed Value	Signal
Recruitment Term Shifts	Successor brands offered improved affiliate splits (80/20 vs Conti's 70/30) in recruitment advertising	Internal pressure to attract displaced Conti affiliates confirmed.

WAIS SCORE: 9+ (no arrest; 3 of 4 dimensions scored)/12 | Limited Impact

Node Criticality: 3/3 Non-substitutable core team. Tier 1 actor.
Cooperation Output: N/A No arrest. Not applicable.
Trust Cascade Effect: 3/3 Broad cascade. Full ecosystem-level trust disruption documented.
Reconstitution Impact: 3/3 Brand failed to reconstitute. Successor brands operating at fraction of prior capacity individually.

Note: WAIS is an arrest-scoring instrument. This case is scored on available dimensions to calibrate the Trust Cascade and Reconstitution Impact descriptors. Node Criticality and Cooperation Output require an arrest event to score fully.

Key Lessons for Framework Application

- The Conti collapse was not caused by Western pressure. It was caused by an internal political miscalculation. The ecosystem effects, however, are identical to what a successful targeted exposure operation would aim to produce. This case calibrates what maximum-effect strife looks like.
- Reconstitution did not fail because the criminal capacity was destroyed. It failed because the trust infrastructure was destroyed. Personnel dispersed into successor brands because no one trusted each other enough to rebuild under the Conti name. Trust infrastructure (Node 07) is the critical variable.
- Successor brand emergence was rapid (under 60 days) but fragmented. Individual successor brands never approached Conti's operational scale. This is the expected pattern after a high-trust-cascade event: ecosystem capacity is preserved but distributed, making it less efficient and more visible.
- The protection relationship status is the unresolved question. The leak exposed FSB contacts but no domestic Russian enforcement followed. This is consistent with the framework's analysis: FSB protection, once activated, is not reversed by embarrassment alone. It requires the krysha relationship to become an institutional liability, not just a visible one.

CASE STUDY 2 | QAKBOT TAKEDOWN: OPERATION DUCK HUNT (August 2023)

Type: Law Enforcement Takedown (Sinkhole and Infrastructure Seizure) | Date: August 2023

Background

QakBot (also known as Qbot and Pinkslipbot) was one of the most widely deployed malware loader ecosystems in operation, with an infection history spanning over 15 years. By 2023 it had become a primary delivery mechanism for ransomware payloads, having delivered Black Basta, Conti successor variants, and multiple other RaaS operations to victim networks at scale.

Operation Duck Hunt, executed by the FBI in coordination with international partners in August 2023, sinkholed QakBot's C2 infrastructure and pushed a removal tool to approximately 700,000 infected hosts. The operation represented the reference model for botnet/loader disruption and is cited explicitly in the framework's Node 05 playbook.

Ecosystem Role at Time of Takedown

Dimension	Assessment
Node	Node 05: Botnet/Loaders. Primary delivery mechanism for ransomware payloads at mass scale.
Infected Host Count	Approximately 700,000 confirmed at time of sinkhole, per FBI disclosure.
RaaS Customers	Black Basta, Royal, and multiple other active RaaS groups confirmed as primary customers of QakBot-delivered access.
Replace Difficulty	HIGH. QakBot represented 15+ years of infrastructure investment: spam networks, crypter relationships, C2 hierarchies, and affiliate distribution agreements.
Protection Layer	No confirmed Russian state protection relationship. QakBot operators assessed as criminal service providers without direct FSB krysha.

Framework Layer Analysis

Macro Layer Effects

- Payment volume: no statistically significant drop in ecosystem-wide ransom payment volume attributable to QakBot disruption in Q3-Q4 2023. Victims affected were remediated before ransomware deployment, preventing payments, but the ecosystem as a whole absorbed the disruption.
- Victim count: affiliated ransomware groups reported temporary slowdowns in victim pipeline. Black Basta activity dropped noticeably in the 30-60 day window post-takedown before recovering.
- This is the expected pattern for a node-level disruption without corresponding financial and meso-layer pressure on the same actor set simultaneously.

Meso Layer Effects

Node	Observed Effect
Node 05: Botnet/Loaders	Full disruption at time of sinkhole. 700,000 infected hosts severed from C2. Distribution infrastructure dismantled simultaneously. This is a CONFIRMED high-impact node-level disruption.
Node 03: BPH	Partial compounding effect. QakBot C2 servers had used a mix of BPH and legitimate VPS. BPH pressure was not applied simultaneously, limiting sustained disruption.
Node 04: IAB Markets	Temporary price spike in IAB listings observed in 30-60 day window post-takedown as ransomware affiliates sought alternative access sources. Consistent with framework prediction.
Reconstitution	QakBot operators began rebuilding infrastructure within approximately 6 months. By mid-2024, QakBot-attributed activity was observed at reduced but significant scale. Full reconstitution to prior capacity not confirmed.

Reconstitution Tracking (Node 05 Reference Model)

Timeframe	Status	Detail
0-30 days	Full disruption	All C2 connectivity severed. 700,000 hosts cleaned via sinkhole removal tool. No observed QakBot-attributed activity.
31-90 days	Rebuilding detected	New QakBot infrastructure identified by security researchers. Smaller scale, new C2 architecture, modified malware variants.
90-180 days	Partial reconstitution	QakBot activity at estimated 30-40% of prior volume. Ransomware customer relationships partially restored.
180+ days	Ongoing reduced capacity	QakBot not restored to pre-takedown operational scale as of available reporting. Successor loaders (Pikabot, DanaBot variants) filled partial gap.

WAIS SCORE: 9/12 (Moderate to High)/12 | Limited Impact

Node Criticality: 3/3 Non-substitutable at scale. 15+ year infrastructure, mass delivery capacity.
Cooperation Output: 2/3 Infrastructure seizure yielded significant technical intelligence. No confirmed arrests of operators with full cooperation.
Trust Cascade Effect: 2/3 Localized disruption to QakBot customer groups. No broad ecosystem-level trust cascade observed.
Reconstitution Impact: 2/3 Partial reconstitution at reduced capacity within 90-180 days. Did not reach prior operational scale.

The +2 coordination bonus does not apply as this was a single-operation action rather than a multi-arrest coordinated takedown.

Key Lessons for Framework Application

- Operation Duck Hunt is the reference model for Node 05 disruption. The simultaneous sinkhole plus victim notification plus removal tool delivery is the correct operational model. Any botnet/loader disruption that does not include all three components will score lower on Reconstitution Impact.

- The IAB price spike in the 30-60 day window post-takedown is a confirmed leading indicator. When Node 05 is disrupted, watch Node 04 IAB pricing immediately. Price increases confirm that the disruption imposed real access costs on ransomware affiliates.
- Reconstitution speed for this operation was faster than the framework's 90-day high-impact threshold would suggest. This reinforces the need for BPH pressure (Node 03) to be applied simultaneously or in advance. QakBot reconstituted partly because hosting infrastructure was not simultaneously degraded.
- No macro-level payment volume effect was observable. This is consistent with the framework's design: a single node disruption without coordinated pressure across financial and access nodes does not move macro metrics. It is a necessary but not sufficient condition for ecosystem-level degradation.

CASE STUDY 3 | LOCKBIT: OPERATION CRONOS (February 2024)

Type: Coordinated Law Enforcement Takedown with Arrests | Date: February 2024

Background

LockBit was the dominant RaaS franchise in the ecosystem at the time of Operation Cronos, accounting for an estimated 25-30% of all publicly claimed ransomware attacks in 2023 based on leak site data. It operated as a franchise model with a large affiliate roster, aggressive recruitment, and the highest public profile of any active group.

Operation Cronos, coordinated by the NCA with FBI, Europol, and multiple national law enforcement agencies, seized LockBit's infrastructure, took control of its leak site (publishing law enforcement content in place of victim data), arrested two LockBit-affiliated operators, and unsealed indictments against additional members including the identified administrator LockBitSupp.

Ecosystem Role at Time of Takedown

Dimension	Assessment
Market Position	Dominant. Estimated 25-30% of ecosystem attack volume by leak site count in 2023.
Affiliate Model	Open franchise. Large affiliate roster with reported 100+ active affiliates at peak. Lower trust requirements than closed models.
Replace Difficulty	MEDIUM-HIGH. The franchise model made the brand more substitutable than a closed group, but the infrastructure investment and affiliate network made full reconstitution non-trivial.
Protection Layer	Assessed as having some protection layer relationships based on operational longevity and Russia-based operation, but lower confidence than Tier 1 actors. LockBitSupp publicly stated Russian affiliation while claiming independence.

Framework Layer Analysis

Macro Layer Effects

- Leak site post volume: LockBit's leak site went dark at time of seizure. Law enforcement publishing victim decryption keys and criminal infrastructure details on the seized site created significant trust disruption.
- Takedown/Relaunch Cycle: LockBit relaunched a new leak site within approximately 5 days, claiming continued operations. However, post-relaunch victim posting volume was significantly reduced for 60-90 days.
- Market share: competitors including RansomHub and BlackCat/ALPHV successors absorbed displaced LockBit affiliates in the 30-90 day window.

Meso Layer Effects

Node	Observed Effect
Node 06: Leak Site Hosting	Full temporary disruption. Law enforcement seizure and reuse of the leak site for operational messaging was a high-impact trust cascade action beyond simple takedown.

Node	Observed Effect
Node 07: Underground Trust Infrastructure	Significant disruption. Law enforcement's publication of affiliate identities, decryption keys, and internal data on the seized site created affiliate-level trust breakdown. Affiliates could not be certain what data had been compromised.
Node 04: IAB Markets	Moderate disruption. LockBit affiliate purchasing patterns showed temporary reduction. Former LockBit affiliates migrated to competing franchises within 60-90 days.
Node 01: OTC Brokers	Limited observable effect. LockBit's financial rails were not simultaneously disrupted.

WAIS Scoring: LockBit Operator Arrests

Two arrests were made in connection with Operation Cronos. These are scored individually.

Arrest 1: LockBit-affiliated operator, third-country arrest

WAIS SCORE: 6-8 (PENDING Cooperation Output)/12 | Limited Impact

Node Criticality: 2/3 Mid-tier operator. Not core team.
Cooperation Output: PENDING Debrief status not confirmed in open source.
Trust Cascade Effect: 2/3 Localized disruption. Combined with simultaneous infrastructure action, cascade effect was elevated.
Reconstitution Impact: 2/3 Partial. LockBit reconstituted under same name at reduced capacity.
+2 coordination bonus applies to the operation as a whole given simultaneous infrastructure seizure.

Takedown/Relaunch Cycle Analysis

Metric	Value	Framework Signal
Time to relaunch	Approximately 5 days	Fast relaunch. High resilience. Reconstitution capacity was largely intact.
Post-relaunch posting volume (30 days)	Approximately 40% of pre-operation baseline	Partial degradation confirmed. Affiliate roster shrank measurably.
Post-relaunch posting volume (90 days)	Approximately 65-70% of pre-operation baseline	Partial reconstitution. Framework Reconstitution Impact score: 2 (partial at 31-90 days, reduced capacity).
Competitor absorption of affiliates	RansomHub emerged as primary beneficiary, rapidly growing affiliate roster post-Cronos	Ecosystem capacity preserved but redistributed. No net reduction in ecosystem attack volume.

Key Lessons for Framework Application

- The law enforcement reuse of the seized leak site for operational messaging (publishing affiliate data, decryption keys, and mocking the administrator) was a high-value trust cascade action not captured in standard takedown metrics. Future operations should plan this as a deliberate trust disruption step, not an afterthought.
- Fast relaunch (5 days) reflects the absence of simultaneous financial rail disruption. When OTC brokers and mixing services are not simultaneously pressured, the financial capacity to rebuild

infrastructure remains intact. Node 01 and Node 08 pressure must be coordinated with infrastructure takedowns to extend reconstitution time.

- RansomHub's emergence as the primary affiliate absorber was rapid and predictable. The framework's substitutability assessment requirement (identify the likely replacement actor before acting) would have flagged RansomHub as a pre-positioning target. Absent that pre-positioning, the ecosystem lost LockBit's brand but not its operational capacity.

CASE STUDY 4 | BLACKCAT/ALPHV: LAW ENFORCEMENT ACTION AND EXIT SCAM (December 2023, March 2024)

Type: Law Enforcement Disruption followed by Suspected Exit Scam | Dates: December 2023 (DOJ action), March 2024 (exit scam)

Background

BlackCat/ALPHV was a technically sophisticated RaaS group operating since late 2021, known for its Rust-based malware, triple extortion model (encryption, leak, and DDoS), and high-profile attacks including Change Healthcare. The DOJ disrupted BlackCat infrastructure in December 2023, obtaining a decryption key and seizing the leak site.

BlackCat regained control of the leak site briefly before the FBI re-seized it. In March 2024, following the Change Healthcare payment (reported at approximately 22 million USD), BlackCat administrators disappeared with the ransom proceeds in what was widely assessed as an exit scam against their own affiliates, with the likely intent of rebranding.

Why This Case Is Analytically Valuable

FRAMEWORK APPLICATION NOTE

This case demonstrates two distinct event types occurring in sequence: a law enforcement disruption followed by an exit scam. The framework treats these as separate events in the strife event log. The law enforcement action scores as a takedown/disruption. The exit scam scores as an EXIT SCAM event type in the Layer 2 strife event log. The interaction between the two is the analytically interesting element: the law enforcement action likely accelerated the exit scam by increasing pressure on the administrators and reducing their confidence in continued operations.

Framework Layer Analysis

Event 1: DOJ Infrastructure Disruption (December 2023)

Node	Effect
Node 06: Leak Site Hosting	Temporary seizure. BlackCat regained control within days, demonstrating resilience of the hosting infrastructure. Takedown/Relaunch Cycle: approximately 48-72 hours. Low reconstitution cost.
Node 07: Underground Trust	Moderate disruption. The seizure and re-seizure back-and-forth created uncertainty among affiliates about the reliability of the operation.
Macro	Limited immediate effect. BlackCat continued operations including the Change Healthcare attack post-disruption.

Event 2: Exit Scam (March 2024)

Field	Content
Event Type	EXIT SCAM
Source Reliability	CREDIBLE. Blockchain analysis by multiple firms confirmed the Change Healthcare payment wallet and traced funds to BlackCat administrator wallets. Affiliates publicly complained on underground forums confirming non-payment.

Field	Content
Ecosystem Effect	Affiliate trust destruction. Public affiliate complaints on Exploit and XSS confirmed non-payment of affiliate shares from Change Healthcare ransom. Brand collapsed within days of exit scam confirmation.
Causal Link to Prior Pressure	CREDIBLE inference. The sequence (law enforcement disruption followed by large payment followed by exit scam) is consistent with administrators taking a final large payment under pressure and exiting before reconstitution became necessary.
Follow-On Indicators	RansomHub rapidly emerged absorbing former BlackCat affiliates. Multiple former BlackCat personnel confirmed in RansomHub operations within 60 days.

Combined Effect Assessment

The two events together produced a higher ecosystem effect than either would have alone. The law enforcement disruption created instability; the exit scam destroyed the remaining trust. This is the compounding effect the framework is designed to produce through deliberate pressure: each action raises the cost of continued operation and lowers the benefit of loyalty to the brand.

Key Lessons for Framework Application

- Exit scams are predictable under certain conditions: large payment received, law enforcement pressure active, administrators facing personal exposure risk. The framework's exit scam frequency proxy metric should be read in context of simultaneous law enforcement activity against the same actor.
- The 48-72 hour relaunch of the leak site after the initial seizure reflects the importance of simultaneous action against hosting infrastructure (Node 03/06) rather than sequential. When hosting is re-seized quickly, it signals that BPH relationships are intact and the cost of reconstitution is low.
- The Change Healthcare payment illustrates the payment volume vs. victim count divergence metric in reverse: a single extremely large payment can move payment volume metrics significantly without representing ecosystem health. Large outlier payments must be annotated separately in KPI C-1 to avoid misinterpretation.

CASE STUDY 5 | BLACK BASTA LEAKS (February 2025)

Type: Internal Leak (Ongoing Event) | Date: February 2025

Background

Black Basta emerged in April 2022 as one of the most significant post-Conti successor groups, widely assessed to include former Conti operators. It operated as a closed hierarchical group with high operational security and targeted high-value victims. In February 2025, a large volume of internal Black Basta chat logs was leaked publicly, attributed to an internal dispute.

The leak exposed internal communications, operational processes, victim negotiation transcripts, and personnel information. The full downstream effects were still developing at the time this document was prepared.

Framework Layer Analysis

ANALYTICAL STATUS NOTE

This case is partially scored. The leak occurred in February 2025 and effects are still developing. 90-day and 180-day reconstitution tracking is not yet complete. This entry demonstrates how the framework handles an ongoing event: score what is observable now, mark future fields as PENDING, and schedule follow-up review.

Strife Event Log Entry

Field	Content
Event Type	LEAK
Source Reliability	CONFIRMED. Chat logs independently verified by multiple security research organizations.
Actors Involved	Black Basta core operators and administrators. Conti lineage personnel confirmed. Specific individuals identifiable from logs.
Immediate Ecosystem Effect	Significant trust disruption within Black Basta affiliate and partner network. Internal disputes visible in the leaked logs themselves, indicating pre-existing strife that the leak accelerated. Victim negotiation transcripts exposed, undermining future negotiation credibility.
Causal Link to Pressure Actions	Leak attributed to internal dispute, not a Western pressure action. However, the underlying strife may reflect accumulated pressure on the group including law enforcement attention, financial friction from sanctions on associated infrastructure, and OPSEC costs.
Follow-On Indicators to Monitor (PENDING)	Black Basta operational tempo post-leak. Affiliate defection rate. New brand emergence by identified personnel. Protection relationship status changes for any assessed krysha connections.

Comparison to Conti Leak

Dimension	Conti (2022)	Black Basta (2025)
Scale of leak	60,000+ messages, source code, financial records	Internal chat logs, negotiation transcripts, operational data

Dimension	Conti (2022)	Black Basta (2025)
Trigger	Political statement (Ukraine support)	Internal financial dispute, assessed
Pre-existing strife	Moderate: political tension over Ukraine affiliation	High: financial disputes visible within leaked content itself
90-day dissolution	Yes. Brand collapsed within 90 days.	PENDING. Effects developing.
Successor emergence	5+ successor brands within 60 days	PENDING.
Protection layer effect	Assessed as Strained to Broken post-leak	PENDING. Requires IC-level assessment.

Key Lessons for Framework Application

- The Black Basta case demonstrates how the framework handles ongoing events. Not every strife event resolves within 90 days. The Layer 2 event log format is designed to capture the event immediately and track effects over time, with PENDING fields updated as information becomes available.
- The pre-existing financial disputes visible in the leaked content are a confirmation of the recruitment term shifts proxy metric: when internal disputes are about financial splits, the group is under pressure. Monitoring affiliate compensation complaints on underground forums provides early warning before a leak event occurs.
- The Conti comparison is instructive for calibrating expected timelines. If the Black Basta leak produces effects comparable to Conti, 90-day dissolution and rapid successor emergence would be the expected pattern. If the group reconstitutes, it suggests the trust infrastructure was more resilient or the protection layer more intact than the Conti comparison would suggest.

SUMMARY: FRAMEWORK SCORING ACROSS ALL FIVE CASES

Case	Primary Event Type	WAIS (if applicable)	Trust Cascade	Reconstitution	Macro Effect
Conti (2022)	Internal Leak	N/A (no arrest)	3/3 Broad cascade	3/3 Brand dissolved	High: ecosystem-wide fragmentation
QakBot (2023)	Infrastructure Takedown	N/A (no arrests scored)	2/3 Localized	2/3 Partial at 90-180 days	Limited: no macro payment effect
LockBit (2024)	Coordinated Takedown plus Arrests	6-8 per arrest (PENDING coop)	2-3/3 with coordination bonus	2/3 Partial at 90 days	Moderate: affiliate redistribution
BlackCat (2023-24)	Takedown plus Exit Scam	Not scored (no qualifying arrests)	3/3 Exit scam destroyed residual trust	3/3 Brand dissolved	Moderate: RansomHub absorbed capacity
Black Basta (2025)	Internal Leak (ongoing)	N/A	PENDING	PENDING	PENDING: effects developing

CALIBRATION TAKEAWAY

High ecosystem impact (macro-level observable effects) requires at minimum two of the following three conditions to be present simultaneously: trust cascade at broad level (3/3), brand dissolution (reconstitution 3/3), and coordinated financial rail pressure. No case in this review produced sustained macro-level payment volume reduction from a single operation alone. Compounding pressure across multiple nodes and multiple timeframes is the necessary condition for macro-level movement.