ECOSYSTEM DEPENDENCY PROJECT

Module 07 — Ransomware Groups and RaaS Variants

HANDLING: INTERAGENCY

Field	Value
Module Number	07
Module Name	Ransomware Groups and RaaS Variants
EDP Node Reference	Cross-cutting — no single node; assessed on arrival (see Section 8 for Dependency Map update recommendation)
Ecosystem Layer	Core Operator / Central Monetization Layer
Upstream Connections	Node 04 (IAB Markets), Node 10 (Credential/Stealer Markets), Node 11 (Crypters/Packers), Node 03 (Bulletproof Hosting), Node 07 (Underground Forums)
Downstream Connections	Node 06 (Leak-Site Hosting), Node 01 (OTC Brokers), Node 02 (High-Risk Exchanges), Node 08 (Mixing/Obfuscation), Node 09 (Mule Networks)
Research Date	April 2026
Primary Researcher	Reno
Source Tools Used	Perplexity AI; Chainalysis 2025 Crypto Crime Report; Secureworks State of the Threat; Coveware Quarterly Reports; Corvus/Travelers Q4 2024; Vectra AI; ReliaQuest; KnowBe4; IBM; Arctic Wolf

CURRENCY NOTE (June 2026): Several passages in this module describe RansomHub as the dominant active brand. RansomHub infrastructure went dark on April 1, 2025; affiliates dispersed primarily to Qilin and DragonForce, and Qilin has held the highest claimed-victim volume since mid-2025. Read RansomHub references as historical unless marked otherwise. Full reassessment due at the next module revision.

SECTION 1 — WHAT IT IS

1.5 Structural Variants — Five Archetypes

The ransomware group landscape comprises five identifiable structural archetypes, each with distinct risk and disruption profiles:

Archetype 1 — Classic RaaS Platform Operators: Full-stack programs serving a broad affiliate pool. Operators develop and maintain encryptors, decryptors, and supporting tooling. They host Tor-based leak sites, payment portals, and affiliate dashboards. They define revenue models, enforce targeting rules (e.g., CIS exclusion filters), and provide branding and playbooks. LockBit, ALPHV/BlackCat, and RansomHub are exemplars; all three are defunct or disrupted as of mid-2026. Current archetype exemplars: Qilin, DragonForce.

Archetype 2 — High-End Big-Game Crews: RaaS variants optimized for large-enterprise targets. These groups prioritize victims with high revenue capacity, use advanced initial access methods (zero-day and N-day exploits against edge devices), and employ structured multi-stage extortion including triple extortion (encrypt, exfiltrate, notify customers/regulators). Cl0p, BlackCat in its mature phase, and Black Basta are exemplars.

Archetype 3 — Mass-Market RaaS Kits: Commodity platforms sold via subscription or one-time license to low-skill actors. These prioritize volume over per-victim value. Affiliates rely on phishing, basic IAB access, and

opportunistic exploitation rather than bespoke zero-days. Revenue per incident is lower but the affiliate pool is substantially larger.

Archetype 4 — Cartel-Style Coalitions: Post-disruption structures in which multiple groups share leak platforms, payment backends, and negotiation infrastructure under a loosely coordinated umbrella. These absorb displaced affiliates from disrupted major brands and use cartel-like coordination to manage victim negotiations and inter-group conflicts over access.

Archetype 5 — Operator-Affiliate Hybrids (Semi-RaaS): Groups that develop ransomware, run high-value campaigns internally, and selectively recruit a small affiliate cadre for secondary targets. These maintain centralized control over victim selection and negotiation. The Scattered Spider collaboration with ALPHV and later RansomHub is a documented example.

SECTION 2 — KEY ACTORS AND EXAMPLES

2.1 Named Actor Archetypes Table

Archetype	Key Named Groups	Key TTPs	Affiliate Model	Confidence
Classic RaaS Platform	LockBit 3.0, ALPHV/BlackCat, RansomHub (historical); Qilin, DragonForce (current)	Full-stack development; Tor-based leak sites and negotiation portals; affiliate dashboards; CIS/RU targeting filters; revenue split model	Open or semi-open recruitment; 60-80% affiliate share	CONFIRMED
Big-Game RaaS Crews	Cl0p, Black Basta, BlackMatter (legacy)	0-day/N-day exploit chains against MFT/VPN/edge devices; double and triple extortion; structured negotiation playbooks; multimillion-dollar ransom targets	Selective or closed recruitment; often tight partner circle	CONFIRMED
Mass-Market Kits	Multiple low-tier groups; frequently unnamed or short-lived	Turnkey panels; phishing-dependent access; volume over value; entry-level subscriptions $40-$100/month	Open subscription; affiliate retains 100% in license model	CONFIRMED
Cartel-Style Coalitions	Post-ALPHV/ LockBit fragmentation clusters; INC Ransom; Rhysida (partial)	Shared leak platforms; absorb displaced affiliates; coordinated negotiation; common payment backends	Shared infrastructure; variable split arrangements	CREDIBLE
Operator-Affiliate Hybrids	Scattered Spider (combined with ALPHV/RansomHub); specialized	Internal campaigns for high-value targets; bespoke tooling; selective	Invite-only; highly controlled affiliate circle	CREDIBLE

	EDR-bypass crews	external affiliate recruitment; centralized victim selection		

2.2 Notable Documented Examples

LockBit 3.0 / LockBit Black: The most prolific RaaS platform by victim count before its February 2024 disruption by Operation Cronos. LockBit operated an affiliate program with publicly posted revenue splits, a bug-bounty program, and a corporate-style brand. Post-disruption, core developers attempted to relaunch as LockBit 4.0 while affiliates migrated primarily to RansomHub and BlackSuit.

ALPHV/BlackCat: A sophisticated Rust-based RaaS that operated from 2021 to early 2024. Targeted healthcare extensively in its final months. Following a December 2023 FBI disruption and seizure, ALPHV operators conducted an apparent exit scam, withholding a USD $22M affiliate payment related to the Change Healthcare attack before shutting down infrastructure.

RansomHub: Emerged in early 2024 and rapidly absorbed displaced ALPHV and LockBit affiliates. By mid-2024 it was the most active group by victim postings. Operates as a classic affiliate split model; does not conduct intrusions directly. Notable for posting victims within days of breaches, applying aggressive leak-site pressure.

Cl0p: Persistently exploits mass-vulnerability events in file-transfer and managed-file-transfer products (MOVEit Transfer, GoAnywhere, Accellion FTA). Each campaign generates hundreds of simultaneous victims. Uses a hybrid model with an internal technical team conducting exploitation and an affiliate or partner layer for secondary monetization.

Black Basta: Operated primarily 2022-2025; targeted large enterprises in manufacturing, healthcare, and critical infrastructure. Used Qbot/QakBot loader (pre-takedown) and later Pikabot for initial access. Sophisticated double-extortion model with structured negotiation. Internal chat logs leaked in early 2025 revealed operational details and state-adjacency indications.

2.3 Geographic Concentration

Russia and CIS states remain the dominant hosting environment for major RaaS operator infrastructure and the primary language of top-tier affiliate communities. Key indicators:

- Virtually all major RaaS platforms embed CIS/RU targeting exclusion filters, limiting domestic victim exposure and signaling awareness of implicit state-tolerance arrangements.
- Primary developer and administrator personas for LockBit, ALPHV, Black Basta, and RansomHub have been assessed (CONFIRMED or CREDIBLE) as Russia-based through law-enforcement indictments, infrastructure analysis, and leaked communications.
- English-language actors (Scattered Spider/UNC3944) have demonstrated the ability to integrate into RaaS ecosystems as privileged affiliates, illustrating that the ecosystem is not exclusively Russian-operated at the affiliate layer.
- North Korean state-affiliated actors (Lazarus Group, TraderTraitor) use ransomware tactically for revenue generation but operate through separate infrastructure and TTPs distinct from the RaaS market.

2.4 Scale and Volume Table

Metric	Value	Period	Source	Confidence
Active double-extortion groups tracked	124	2025-26 timeframe	Vectra AI	CONFIRMED
New ransomware groups formed	55 (+67% YoY)	2024	Corvus/Travelers	CONFIRMED

Increase in active double-extortion groups	+30% YoY	July 2023 to June 2024	Secureworks	CONFIRMED
Groups posting victims in single month	40 groups in May 2024	May 2024	Secureworks	CONFIRMED
Leak site victims — quarterly peak	1,663 victims in Q4 2024	Q4 2024	Corvus/Travelers	CONFIRMED
Leak site victims — full year	7,458-7,960 victims (+53% YoY)	2025	Vectra AI	CONFIRMED
US share of global leak-site victims	~48%	2024-25	Vectra AI	CONFIRMED
Healthcare breach count	700+ double-extortion breaches	2024-25	Vectra AI	CONFIRMED
Healthcare records exposed	>275 million patient records	2024-25	Vectra AI	CONFIRMED
Total on-chain ransomware payments	~USD $813M	2024	Chainalysis	CONFIRMED
Change from prior year	Down from ~$1.25B in 2023 (~35% decline)	2023 vs 2024	Chainalysis	CONFIRMED
Payment-to-demand ratio	~53% gap (victims paid ~47% of demanded amount on average)	H2 2024	Chainalysis	CONFIRMED
Typical payment band	USD $150,000 to $250,000	H2 2024	Chainalysis	CONFIRMED

2.5 State Adjacency Assessment

Dark Covenant 3.0 screening is applicable to major RaaS operators. The following state-adjacency indicators are present:

- CIS/RU targeting exclusion filters embedded in operator platforms constitute the clearest structural indicator of implicit FSB/MVD tolerance, not passive; operators actively maintain rule-sets to protect domestic targets.
- ALPHV/BlackCat operations during 2023-2024 included targeting of organizations perceived as hostile to Russian state interests, suggesting possible opportunistic alignment rather than formal direction.
- Black Basta leaked chat logs (early 2025) referenced interactions with individuals assessed to have connections to Russian organized crime networks with state adjacency; confidence: CREDIBLE based on single-source reporting.
- No CONFIRMED evidence of direct GRU or SVR operational tasking of commercial RaaS groups exists in open reporting. FSB protection-tolerance relationship is the primary documented model.
- Analyst inference: Major RaaS operators operating at scale from Russian territory without disruption by Russian authorities are implicitly protected; operators who become inconvenient (politically or due to Western pressure) face selective enforcement (Revil 2022, post-Colonial Pipeline pressure).

Confidence note: **[CONFIRMED]** for CIS filter evidence; **[CREDIBLE]** for Black Basta state-link reporting; **[ANALYST INFERENCE]** for broader FSB protection model as applied to current operators.

SECTION 3 — INFRASTRUCTURE DEPENDENCIES

3.1 Upstream Dependencies

RaaS operators depend on the following upstream nodes from the EDP Dependency Map:

Upstream Node	EDP Node	Dependency Type	Operator Function Supported
Initial Access Broker Markets	Node 04	Critical	Affiliates purchase network access; operators direct affiliates to IAB markets for victim acquisition; without viable IAB supply, affiliate deployment rates drop.
Credential/Stealer-Log Markets	Node 10	High	Affiliates use credential dumps to identify and authenticate into victim networks; operators benefit from abundant, low-cost access material from stealer logs.
Crypter/Packer Services	Node 11	High	Operator payloads require crypter/packer services to evade EDR detection; some operators maintain in-house crypter capability while others outsource.
Bulletproof Hosting	Node 03	Critical	Operator infrastructure (C2, leak sites, payment portals, negotiation panels, affiliate dashboards) depends entirely on BPH providers for uptime and attribution resistance.
Underground Forums and Dark Web Markets	Node 07	High	Primary affiliate recruitment channel; operator reputation management; sourcing of tooling and services; dispute resolution for affiliate conflicts.
Exploit/Vulnerability Brokers	EDP Module 06	Moderate-High (big-game archetypes)	Big-game crews and hybrid operators require 0-day/N-day exploits for edge-device mass exploitation; sourced from exploit brokers or maintained in-house.

3.2 Downstream Outputs

Operator activity drives demand and revenue into the following downstream nodes:

Downstream Node	EDP Node	Relationship
Leak-Site Hosting Stack	Node 06	Operators depend on BPH-hosted Tor leak sites for double-extortion pressure; leak site operational capability is a core operator asset.
OTC Crypto Brokers	Node 01	Operator and affiliate ransom proceeds exit through OTC brokers; this is the primary cash-out mechanism for large ransom payments.
High-Risk/Non-Compliant Exchanges	Node 02	Secondary cash-out channel; high-risk exchanges process operator and affiliate funds without KYC/AML compliance.
Mixing/Obfuscation Services	Node 08	Operators route victim payments through mixers and cross-chain bridges before splitting affiliate shares to obscure fund flows.
Mule/Money Laundering Networks	Node 09	Final conversion of crypto proceeds to fiat; used by both operators and affiliates for physical cash or asset acquisition.

3.3 Critical Chokepoints

Chokepoint	Why Critical	Disruption Owner	Backfire Risk
Decryption key management servers	Operators retain exclusive control of keys; seizure renders all deployed ransomware non-monetizable and undermines affiliate confidence in the platform.	FVEY LE + IC (covert server access)	LOW (infrastructure action)
Payment portal and negotiation infrastructure	Victim payments and negotiations flow through operator-controlled Tor portals; disruption prevents revenue collection and pressures victim toward non-payment.	FVEY LE + IC	LOW
Affiliate dashboard and builder panel	Affiliates access tooling and submit victim data through operator-controlled panels; disruption severs operator-affiliate coordination.	FVEY LE	LOW
Leak-site hosting (Node 06)	Double-extortion model depends on functional leak sites for victim pressure; takedown degrades extortion	FVEY LE + upstream hosting providers	LOW

	leverage.		
Crypto payment wallet addresses	Operator-controlled wallets receive victim payments; blockchain tracing and designation by OFAC degrades payment processing.	Treasury/OFAC + Chainalysis/TRM	LOW
Underground forum recruitment channels (Node 07)	Affiliate recruitment and operator reputation management; disruption degrades affiliate supply and brand trust.	FVEY LE + private sector monitoring	LOW

3.4 Technical Infrastructure

- Tor-based hidden services for leak sites, payment portals, and negotiation chat; hosted on BPH providers (Node 03) to resist law-enforcement seizure.
- Affiliate management panels running custom or adapted web applications; typically hosted on BPH infrastructure with multi-layered access controls.
- Ransomware builder tools — configurable payload generators allowing affiliates to create victim-specific executables with embedded payment addresses and ransom note templates.
- Cryptocurrency payment infrastructure using Monero (increasingly) and Bitcoin; victim payments received in operator-controlled wallets; affiliate splits routed through automated or manual mixing.
- Exfiltration staging infrastructure (EDP Node 14) used by affiliates to hold stolen data prior to operator-controlled leak-site posting.
- Operational security tooling: VPNs, residential proxies, and anonymization layers (EDP Node 15) used by operators and affiliates to mask administrative access to infrastructure.

3.5 Cross-Module Linkages

EDP Module	Linkage Type	Description
Module 01 — Stealers	Input	Stealer logs provide credential material that affiliates use for initial access, supplementing or replacing IAB purchases.
Module 02 — Loaders	Input	Loaders (Qbot, IcedID, Pikabot) serve as the primary delivery mechanism for ransomware payloads deployed by affiliates.
Module 03 — Crypters/Packers	Input	Crypter services protect ransomware payloads from EDR detection; critical for affiliate operational success rates.
Module 04 — Callers/Spammers	Indirect Input	Caller/vishing operations (e.g., Scattered Spider) are used by privileged affiliates to manipulate IT helpdesks for credential reset access.
Module 05 — IABs	Critical Input	IAB markets are the primary source of pre-compromised network access for the majority of RaaS affiliates.

Module 06 — Exploit/Vuln Brokers	Input (big-game)	Big-game crews source 0-day/N-day exploits for mass exploitation campaigns; Cl0p is the primary exemplar.
Module 08 — Leak Site Operations	Output	Operator-controlled leak sites (hosting, content, posting cadence) are the primary extortion amplifier.
Module 09 — BPH	Critical Infrastructure	BPH providers host all operator-facing infrastructure; operator capability is ceiling-bounded by BPH resilience.
Module 10 — Underground Forums	Market	Forums facilitate affiliate recruitment, reputation management, tooling acquisition, and ecosystem coordination.
Module 11 — Crypto Mixers	Cash-Out	Mixing services obfuscate payment flows between victim payment and affiliate/operator cash-out.
Module 12 — OTC Brokers	Cash-Out	Primary mechanism for converting large ransom payments to fiat without triggering exchange compliance systems.
Module 13 — Exchanges	Cash-Out	Secondary mechanism for smaller or more fragmented payment flows.
Module 14 — Mule Networks	Cash-Out	Final cash conversion layer; used particularly for mid-tier ransom payments.
Module 15 — Negotiation Services	Adjacent	Some operators use or compete with third-party negotiation services; understanding negotiation dynamics informs payment rail disruption.

SECTION 4 — DISRUPTION LEVERAGE POINTS

4.1 Primary Disruption Levers

RaaS operators are the highest-value disruption target in the ecosystem due to their aggregation function. However, direct operator-level disruption (arrest, indictment, infrastructure seizure) is resource-intensive, and groups reconstitute quickly. The following levers are assessed in order of leverage-to-cost ratio:

Lever	Mechanism	Primary Owner	Best Method	Expected Effect	Backfire Risk
Crypto payment rail disruption	Trace and designate operator-controlled wallet addresses; blockchain analysis to map affiliate payout flows; OFAC	Treasury/OFAC + Chainalysis/TRM/Elliptic	Designation + victim notification to discourage payment; blockchain forensics to pursue through mixer/exchange	Increased non-payment rate; degraded affiliate revenue; reduced ecosystem profitability	LOW

	designation of RaaS payment infrastructure				
Decryption key server seizure	Covert or overt access to operator C2/key management infrastructure; publication or provision of decryption keys to victims	FVEY LE + IC (NCA, FBI, Europol)	Joint LE operation (Operation Cronos model); decryptor tool publication	Neutralizes deployed ransomware; undermines operator credibility with affiliates; forces rebranding	LOW
Leak-site takedown (Node 06)	Seize or disable Tor-based leak site hosting; notify victims directly; disrupt extortion pressure mechanism	FVEY LE + upstream BPH providers (Node 03)	Joint LE seizure + domain/server disruption; victim rapid notification	Reduces extortion leverage; lowers payment rate; damages operator brand	LOW
Affiliate trust disruption	Publicize operator malfeasance (exit scams, withheld payments); introduce uncertainty about platform reliability; law-enforcement engagement with known affiliates	FVEY LE + IC + private sector	Public reporting; seizing affiliate dispute evidence and publicizing; co-opting disgruntled affiliates as sources	Degrades affiliate recruitment; increases defection from platforms; fragments ecosystem	LOW-MEDIUM
Operator individual attribution and indictment	Identify, indict, and publicize operator identities; disrupt operator ability to operate openly; impose reputational and psychological costs	FVEY LE (FBI, NCA, Europol)	Grand jury indictment + INTERPOL Red Notice + public unsealing	Forces operational security increases; may cause operator to cease operations; sets deterrence precedent	MEDIUM-HIGH (Dark Covenant 3.0 screening required)
BPH infrastructure disruption (Node 03)	Degrade BPH providers hosting operator infrastructure; force migration of leak sites, payment portals, and affiliate panels	FVEY IC + LE + upstream ISPs and registrars	Upstream provider engagement; server seizure; network blocking	Forces infrastructure migration; degrades uptime; imposes operational costs	LOW-MEDIUM

4.2 Compounding Disruption Actions

The following actions compound the primary levers when executed concurrently or in rapid sequence:

- Simultaneous leak-site seizure and decryptor publication: Removes both extortion pressure and technical leverage from operator in a single operation. Demonstrated effectively in Operation Cronos against LockBit.
- OFAC designation timed with law-enforcement press conference: Combines financial isolation with reputational damage and affiliate deterrence in a single message cycle.
- Affiliate diaspora tracking following major takedown: Post-disruption monitoring of underground forums (Node 07) for affiliate migration patterns to emerging brands; allows early pressure on successor groups before they consolidate.
- Decryptor tool release to victims concurrent with media outreach: Reduces victim payment incentive, degrading operator revenue and demonstrating law-enforcement capability to the affiliate community.
- Blockchain wallet cluster designation: Following identification of a new RaaS payment wallet cluster, rapid OFAC designation creates compliance obligations for any exchange or OTC broker processing funds from those addresses.
- Healthcare-sector rapid notification: Given the disproportionate targeting of healthcare (700+ breaches, 275M+ records), rapid victim notification programs and sector-specific decryptor provision reduces payment rates in the highest-profile vertical.

SECTION 5 — RESILIENCE AND REPLACE DIFFICULTY

5.1 Replace Difficulty Assessment

Level	Assessment	Rationale
Individual operator (developer/admin)	MEDIUM	Core developers are rare and hard to replace; arrest or indictment of a lead developer degrades platform quality. However, code can be forked, and the ransomware toolkit market allows new operators to build on leaked or purchased source code.
Specific RaaS brand (LockBit, ALPHV)	LOW-MEDIUM	Post-disruption history shows rapid brand reconstitution or affiliate migration to successor brands within weeks. The brand itself is easily replaced; the affiliates and the code are the durable assets.
Affiliate pool (collective)	LOW	Affiliates migrate freely between programs; 55 new groups in 2024 absorbed displaced affiliates with minimal disruption to total ecosystem deployment capacity.
Operator capability (function, not brand)	MEDIUM-HIGH	The functional capacity to develop, maintain, and operate a competitive RaaS platform requires significant technical expertise; not easily replaced at the top tier. Entry-level kit operators face lower barriers.
Full ecosystem disruption (cross-node)	HIGH	Disrupting the RaaS layer in isolation without simultaneous pressure on BPH (Node 03), IAB markets (Node 04), and payment rails (Nodes 01, 02, 08) produces

		cosmetic disruption only; the ecosystem reconstitutes quickly.

5.2 Redundancy and Structural Resilience

- The RaaS ecosystem is structurally resilient because operator disruption directly produces affiliate diaspora, which seeds new groups. Each major takedown (REvil 2021, LockBit 2024, ALPHV 2024) resulted in measurable new group formation within 60-90 days.
- Brand fragmentation increases total ecosystem attack surface: 55 new groups in 2024 means law enforcement must monitor more targets with similar resources. Fragmentation is a resilience feature, not a vulnerability.
- Ransomware source code leakage (LockBit 3.0 builder leak 2022, Babuk leak 2021, Conti leak 2022) has dramatically lowered barriers to entry for new operators; new groups do not need to develop encryption capability from scratch.
- CIS exclusion filters create a protected domestic operating environment; Russian state tolerance (Dark Covenant model) provides structural protection from the most capable law-enforcement actors.
- Operational security improvements post-2022 (increased use of Monero, end-to-end encrypted negotiation, shorter operational lifespans for individual brands) reflect ecosystem-level adaptation to law-enforcement pressure.

5.3 Historical Reconstitution Table

Group	Disruption Event	Date	Reconstitution / Outcome
REvil/Sodinokibi	Server seizures; FSB arrests following Colonial Pipeline pressure	Jan 2022	FSB arrests dampened operations temporarily; core infrastructure was offline. Partial reconstitution attempts failed. Affiliates migrated to BlackCat, LockBit.
Conti	Internal chat leak; reputational collapse; Ukrainian researcher breach	2022	Conti formally disbanded but core team reconstituted as multiple successor groups (Black Basta, Royal, Silent Ransom, Karakurt, Quantum). Functional replacement within 3-4 months.
Hive	FBI covert infiltration; decryptor keys obtained and distributed; infrastructure seizure	Jan 2023	Core Hive operations ceased. No direct reconstitution identified; affiliates dispersed to other programs. Estimated USD $130M in victim payments avoided due to FBI key distribution.
ALPHV/BlackCat	FBI infiltration; decryptor publication; DOJ seizure	Dec 2023	Operators conducted apparent exit scam (withheld $22M affiliate payment); infrastructure shut down. RansomHub

			emerged as primary affiliate absorber within weeks.
LockBit 3.0	Operation Cronos: NCA-led multi-country infrastructure seizure; admin deanonymization; decryptors published	Feb 2024	Core infrastructure seized; LockBit admin (LockBitSupp) publicly identified. Operator attempted relaunch as LockBit 4.0 with limited success. Affiliates migrated to RansomHub and BlackSuit. LockBit brand activity significantly reduced but not eliminated.

5.4 Ecosystem Adaptation Patterns

The ransomware ecosystem has demonstrated consistent adaptation patterns in response to law-enforcement pressure:

- Operational lifespan reduction: Groups operate for shorter periods under a single brand before rebranding; reduces cumulative intelligence collection value of any single brand.
- Infrastructure decentralization: Post-Cronos, operators have increased use of decentralized hosting, multiple redundant leak sites, and faster infrastructure rotation.
- Affiliate trust degradation response: Following ALPHV exit scam, some operators have published "proof of funds" or escrow arrangements to reassure affiliates; illustrates ecosystem-level reputational management.
- Monero adoption: Increasing migration from Bitcoin to Monero for affiliate payouts and some victim payments; directly responds to Chainalysis tracking capability.
- Target profile normalization: Shift toward "scalability" model (repeatable, systematic recon and exploitation) rather than bespoke operations; reflects affiliate preference for reliable income over high-risk high-reward single events.

5.5 Durability Assessment

Factor	Rating	Notes
Technical barrier to entry (toolkit availability)	LOW	Leaked source code, commodity builders, and kit markets have reduced technical barriers substantially.
Financial incentive durability	HIGH	Even at $813M in 2024 (down 35%), ransomware remains among the highest-return criminal enterprises per operator.
State protection durability	HIGH	Russia/CIS state tolerance is structurally stable absent major geopolitical shifts; operator community manages risk through CIS filters.
Law-enforcement attrition rate	LOW-MEDIUM	Major operations (Cronos, Hive) achieve meaningful disruption at the brand level but ecosystem-level attrition remains low; new groups

		form faster than LE can disrupt them.
Victim payment behavior trend	IMPROVING (for disruption)	Non-payment rate is increasing; H2 2024 shows 53% gap between demanded and paid amounts. Declining payment rate degrades ecosystem profitability.
Overall ecosystem durability	HIGH	The RaaS ecosystem is structurally durable at the function level; individual brands are fragile, but the function reconstitutes rapidly and reliably.

SECTION 6 — INDICATORS AND KPIs

6.1 Health Indicators — Normal vs. Under Pressure

Indicator	Normal / Stable State	Under Pressure
Active group count	60-124 active groups tracked	Rapid drop in named active groups; fewer new postings across platforms
New victim postings per month	600-800+ victims across all groups	Sustained drop to <300/month would indicate significant ecosystem disruption
Total on-chain payments	USD $800M-$1.25B annually	Drop below $500M annually with stable victim count would indicate degraded payment collection
Payment-to-demand ratio	40-60% of demanded amount paid	Sustained drop below 30% indicates victim community increasingly refusing to pay
Affiliate recruitment activity on forums	Regular "partner program" postings on XSS, RAMP, and Telegram channels	Absence of recruitment postings; operators going dark; affiliate disputes increasing
Time to reconstitution post-disruption	30-90 days for brand reconstitution or affiliate migration	Extended silence (>180 days) from major brand without successor emergence
Monero vs. Bitcoin payment ratio	Increasing Monero share	Continued Monero migration indicates sustained blockchain-tracing pressure
Healthcare and critical sector targeting rate	700+ breaches annually; ~48% US victim share	Significant decline would indicate effective victim hardening or targeting filter expansion

6.2 Disruption KPIs

KPI	Baseline (2024-25)	Disruption Target (18-month)	Collection Method

Active double-extortion group count	124 groups	<75 active groups	Leak site monitoring (Secureworks, Corvus, Mandiant)
Monthly leak-site victim postings	~650 avg/month (7,800 annualized)	<400/month sustained	Leak site aggregator monitoring
Annual on-chain ransom payments	~$813M (2024)	<$500M	Chainalysis / TRM annual report
Payment-to-demand ratio	~47% of demanded amount paid	<30%	Coveware quarterly victim survey
Days from disruption to active successor brand	30-90 days average (post-Cronos, post-ALPHV)	>180 days average across major disruptions	Forum and leak-site intelligence
New group formation rate	55 new groups in 2024 (+67% YoY)	Year-on-year decline in new group formation	Threat intelligence provider tracking
OFAC-designated RaaS wallet addresses	Growing designation list	Designation of top-5 active operator wallet clusters within 12 months	Treasury OFAC public designation list
Decryptor tools publicly released	Infrequent (Hive 2023, LockBit 2024)	Decryptor release within 30 days of each major operator takedown	CISA / law-enforcement press releases

6.3 Collection Methods

- Leak-site aggregation platforms (Secureworks CTU, Corvus, Mandiant, Group-IB) provide near-real-time victim posting data; this is the most reliable open-source indicator of ecosystem health.
- Blockchain forensics platforms (Chainalysis, TRM Labs, Elliptic) provide on-chain payment flow data; annual reports provide validated payment totals; real-time wallet tracking requires platform access.
- Underground forum monitoring (Intel 471, Flashpoint, Recorded Future) tracks affiliate recruitment patterns, operator reputation, and new program launches.
- Coveware quarterly ransomware marketplace reports provide victim-side data on payment rates, ransom demands, and negotiation outcomes; uniquely valuable because they reflect actual victim behavior rather than leak-site claims.
- Law-enforcement operational outcomes (FBI, NCA, Europol press releases; DOJ indictments) confirm group attribution and operational impact.

6.4 Baseline Data

Metric	Baseline Value	Period	Source
Active groups	124	2025-26	Vectra AI
New groups per year	55 (+67% YoY)	2024	Corvus/Travelers
Victims on leak sites (annual)	7,458-7,960 (+53% YoY)	2025	Vectra AI
Victims on leak sites (quarterly peak)	1,663 (Q4 2024)	Q4 2024	Corvus/Travelers
Annual on-chain payments	~$813M	2024	Chainalysis
Prior year payments	~$1.25B	2023	Chainalysis

Typical payment band	$150k-$250k	H2 2024	Chainalysis
Payment-to-demand gap	~53%	H2 2024	Chainalysis
US share of victims	~48%	2024-25	Vectra AI
Healthcare breaches	700+	2024-25	Vectra AI
Patient records exposed	>275M	2024-25	Vectra AI
Affiliate revenue share	60-80%	Market standard	Multiple sources
Operator platform fee	20-40%	Market standard	Multiple sources
Subscription kit price range	$40-$100/month	Current	Vectra AI, NMFTA
One-time license price range	$500-~$84,000	Current	Wikipedia, NMFTA

6.5 Alert Thresholds

Threshold Event	Trigger Level	Recommended Action
New high-volume group emergence	>100 victims posted within first 60 days of group appearance	Immediate profiling; forum and infrastructure attribution; OFAC wallet cluster identification
Healthcare victim surge	>50 healthcare victims in any 30-day period across all groups	Sector-specific rapid notification; coordinate with HHS; escalate to CISA
Total payment reversal (increase)	Annual on-chain payments exceed $1B again	Indicates ecosystem recovery; escalate cross-node disruption pressure (Nodes 01, 02, 08)
Rapid new group formation spike	>10 new groups in any 60-day window	Indicates major operator disruption with inadequate affiliate containment; surge forum monitoring
US victim share increase	US share exceeds 55% of global victims	Indicates targeting shift or filter modifications; escalate IC collection on CIS filter status
Monero payment share increase	>50% of victim payments routed through Monero	Indicates degraded blockchain tracing capability; escalate Monero de-anonymization technical efforts

SECTION 7 — SOURCES AND CONFIDENCE

7.1 Primary Sources

Threat Intelligence and Ecosystem Reporting:

- Vectra AI — "How Ransomware as a Service Helps Attackers Scale" and "Double Extortion Ransomware" (group counts, affiliate pricing, leak-site victim statistics 2025).
- Corvus Insurance / Travelers — Q4 2024 Cyber Threat and Ransomware Statistics Report (new group formation counts, quarterly victim peak, 67% YoY group increase).

- Secureworks CTU — "State of the Threat" annual reporting (double-extortion group growth, post-ALPHV/LockBit fragmentation analysis).
- Coveware — Q1 2024 Ransomware Marketplace Report (affiliate trust degradation, "take what we can get" targeting analysis, RaaS developer credibility issues).
- ReliaQuest — "Ransomware and Cyber Extortion in Q4 2024" (affiliate migration patterns, RansomHub emergence, Scattered Spider collaboration).

Financial Intelligence:

- Chainalysis — 2025 Crypto Crime Report and associated coverage (total on-chain ransomware payments 2024: ~$813M; payment-to-demand gap; typical payment band $150k-$250k; 2023 comparison $1.25B).

Ecosystem Structure and Technical Analysis:

- IBM Security — "What is Ransomware-as-a-Service (RaaS)?" (baseline definitions, revenue model architecture, operator-affiliate separation of function).
- Arctic Wolf — "Ransomware-as-a-Service will continue to grow in 2024" (RaaS ecosystem evolution, affiliate recruitment, tooling supply).
- Menlo Security — "Ransomware-as-a-service (RaaS) kits will be a problem" (mass-market kit structure, affiliate duties, phishing-dependent access patterns).
- Wikipedia — "Ransomware as a service" (structured summary of subscription, affiliate, and license model economics).
- KnowBe4 / Coveware summaries — "Ransomware Gangs are Big Game Hunting" (median victim size increases, big-game hunting motivation).
- LinkedIn / threat-intel blogs — "How Ransomware Gangs Select Their Victims" (targeting logic, CIS filters, Cl0p campaign targeting analysis).
- NMFTA (National Motor Freight Traffic Association) — ransomware economics documentation (revenue models, affiliate split ranges).

7.2 Secondary Sources

- SC World / Secureworks — active group count during May 2024 (40 groups posting victims); 30% YoY increase in double-extortion groups.
- KnowBe4 — big-game targeting analysis and victim size data.
- Investing.com — secondary coverage of Chainalysis 2025 Crypto Crime Report financial statistics.
- DOJ press releases — LockBit (Operation Cronos), ALPHV, Hive disruption announcements; indictment details for operator attribution.
- NCA / Europol operational announcements — Operation Cronos technical details and LockBit admin deanonymization.

7.3 Gaps and Uncertainties

- Operator identity and precise location: Most operator attribution is CREDIBLE based on infrastructure analysis and forum personas; CONFIRMED identification requires law-enforcement indictment or confession.
- Affiliate pool composition: The total number and identity of active affiliates is unknown; forum monitoring captures recruitment signals but not the full affiliate roster for any platform.
- State-directive relationship: FSB protection/tolerance is CONFIRMED structural; evidence of active state tasking of commercial RaaS operators (beyond opportunistic tolerance) is CREDIBLE at best in open reporting.

- Monero payment volumes: On-chain Monero flows are substantially less transparent than Bitcoin; Chainalysis figures reflect visible Bitcoin-denominated payments and may undercount total ecosystem revenue.
- RansomHub operator identity and jurisdiction: As of April 2026, RansomHub operator identity and national base are assessed as likely Russia/CIS but not CONFIRMED in open reporting.
- Post-2025 group fragmentation trajectory: Whether the fragmentation trend stabilizes or continues is unknown; 124 groups may represent a ceiling or a continuing trend.

7.4 Confidence Notes

Claim / Finding	Confidence	Basis
Total 2024 on-chain ransomware payments (~$813M)	CONFIRMED	Chainalysis 2025 Crypto Crime Report; multiple secondary citations
55 new ransomware groups in 2024 (+67% YoY)	CONFIRMED	Corvus/Travelers Q4 2024 report; corroborated by Secureworks
7,458-7,960 leak-site victims in 2025 (+53% YoY)	CONFIRMED	Vectra AI 2025 reporting; consistent with quarterly trend data
Affiliate revenue split 60-80%; operator take 20-40%	CONFIRMED	Multiple sources (IBM, Wikipedia, NMFTA, Coveware); market-standard range
CIS/RU targeting exclusion filters as standard practice	CONFIRMED	Multiple documented instances across LockBit, ALPHV, RansomHub, others
FSB protection/tolerance model for major operators	CREDIBLE	Strong structural inference; REvil selective enforcement 2022 is confirming data point
Black Basta state-adjacency indicators in leaked chats	CREDIBLE	Single-source (leaked chat analysis); not independently corroborated
RansomHub operator as Russia-based	ANALYST INFERENCE	CIS filter presence; RU-language operational security; no public indictment
Active GRU/SVR tasking of commercial RaaS groups	NOT SUPPORTED IN OPEN REPORTING	No open-source evidence; absence of evidence is not evidence of absence

SECTION 8 — ANALYST ASSESSMENT

8.1 Key Takeaway

Ransomware Groups and RaaS Variants are the central aggregation function of the EDP ecosystem — not a discrete node but the mechanism by which every upstream supply chain component is monetized and every downstream cash-out channel is activated. Disrupting individual RaaS brands produces measurable short-term effects but structurally inadequate long-term impact. The 2024 ecosystem delivered 7,460-7,960 publicly named victims and approximately $813M in confirmed payments despite the two most significant law-enforcement operations in the history of the sector (Operation Cronos against LockBit; FBI against ALPHV). This outcome confirms that brand-level disruption without simultaneous pressure on the ecosystem nodes that sustain it — BPH (Node 03), IAB markets (Node 04), underground forums (Node 07), mixing services (Node 08), and OTC cash-out

(Node 01) — produces affiliate diaspora, new brand formation, and ecosystem continuation at near-baseline levels.

Two countervailing trends create a narrow leverage window: total payments are declining (-35% from 2023 to 2024) while victim counts are rising (+53% YoY in 2025). This divergence indicates that the victim community is increasingly refusing to pay, which is the single most potent structural threat to operator profitability. Policies, technologies, and practices that increase non-payment rates are the highest-return disruption investment available, because they attack operator revenue without triggering ecosystem reconstitution.

8.2 Priority Recommendations

Recommendation 1 — Prioritize Payment Rail Disruption Over Brand Disruption

The declining payment-to-demand ratio (53% gap in H2 2024) reflects market forces that are more durable than law-enforcement takedowns. OFAC designation of active operator wallet clusters, combined with victim rapid-notification programs and public decryptor availability, sustains and accelerates this trend. Each designation of a payment address cluster creates compliance obligations for every exchange, OTC broker, and mixer downstream. This is Phase A and Phase B EDP playbook work (Nodes 01, 02, 08) executed in direct support of Phase C operator disruption.

Recommendation 2 — Healthcare Sector Requires Dedicated Rapid-Response Architecture

With 700+ double-extortion breaches and over 275 million patient records exposed in 2024-25, healthcare is the highest-impact vertical and a potential policy forcing function. A dedicated healthcare ransomware rapid-response capacity — combining CISA/HHS victim notification, FBI decryptor deployment, and pre-positioned technical assistance — would reduce payment rates in the highest-profile sector and generate deterrence signals to affiliates who disproportionately target it.

Recommendation 3 — Affiliate Diaspora Containment as Post-Takedown Priority

Post-Cronos and post-ALPHV experience demonstrates that affiliate migration to successor brands (primarily RansomHub) occurs within weeks. A systematic post-takedown affiliate monitoring and early-pressure protocol — targeting successor brand infrastructure before it consolidates affiliate trust — would compress the reconstitution window. This requires pre-positioned forum intelligence (Node 07) and rapid wallet cluster identification for emerging brands.

Recommendation 4 — Dark Covenant 3.0 Screening Before Individual Attribution

Any individual attribution action against Russia-based RaaS operators requires prior FSB/MVD protection-relationship screening. Attribution of a protected individual without this screening risks diplomatic friction disproportionate to enforcement value. Infrastructure and financial designation actions (Nodes 01, 02, 03, 06, 08) carry LOW backfire risk and should proceed without this constraint.

8.3 Connection to EDP Disruption Playbook

Module 07 is cross-cutting and activates all three disruption phases. The sequencing logic is:

- Phase A (Nodes 01, 02, 03 — Financial and Infrastructure Foundation): Targeting OTC brokers (Node 01), high-risk exchanges (Node 02), and BPH providers (Node 03) degrades the payment collection and infrastructure capacity of RaaS operators. Phase A disruption should precede or run concurrent with any direct operator action, as it degrades the reconstitution capability of successor groups.
- Phase B (Nodes 04, 07, 08 — Market and Trust Infrastructure): Targeting IAB markets (Node 04) degrades the access supply that affiliates depend on; targeting forums (Node 07) disrupts affiliate recruitment and brand reputation management; targeting mixing services (Node 08) intercepts payment routing. Phase B disruption is the complement to payment rail designation.
- Phase C (Nodes 05, 06, 09 — Delivery and Monetization): Targeting loader ecosystems (Node 05) degrades the delivery mechanism for ransomware payloads; targeting leak sites (Node 06) removes the double-extortion mechanism; targeting mule networks (Node 09) disrupts the final cash conversion layer.

Phase C is the most operationally visible layer and should be timed to maximize psychological effect on the affiliate community.

Module 07 therefore serves as the prioritization rationale for all three phases: because operators aggregate all upstream supply chain functions and direct all downstream cash-out flows, sustained disruption of the operator layer requires concurrent pressure on all phase nodes. A single-phase approach produces temporary brand disruption; a multi-phase approach degrades the economic viability of the function.

8.4 EDP Dependency Map Update Recommendations

Recommendation	Proposed Change	Tier	Replace Difficulty	Primary Owner	Backfire	Rationale
Add Node 16 — RaaS Operator / Core Group Infrastructure	New dedicated node for the RaaS operator function (developer/operator layer, not the broader affiliate ecosystem)	CRITICAL	HIGH	FVEY LE (FBI, NCA, Europol) + IC; OFAC for financial targeting	LOW (infrastructure/financial); MEDIUM-HIGH (individual attribution — Dark Covenant screening required)	The current map has no node representing the operator function itself. This gap means the map does not capture the primary aggregation and monetization node of the entire ecosystem. All 15 current nodes either feed into or are sustained by the operator layer. Adding Node 16 corrects this structural omission.
Add Node 17 — Affiliate Ecosystem and Recruitment Markets	New supplemental node for the affiliate layer distinct from individual upstream nodes	HIGH	LOW	FVEY LE + private sector forum monitoring	LOW	Affiliates are a distinct actor class from operators. Their recruitment, vetting, and lifecycle management constitute a separable function with distinct disruption levers (affiliate trust attacks, forum recruitment disruption). A

						dedicated node would allow the playbook to address affiliate containment as a post-takedown protocol distinct from operator infrastructure targeting.

Note: The Dependency Map currently contains 15 nodes. These recommendations would expand it to 17. Both new nodes represent functions that are structurally central to the ransomware supply chain but are presently subsumed under the cross-cutting designation applied to Module 07. Analyst assessment confidence for these recommendations: **[ANALYST INFERENCE]** — based on cross-module analysis of all 7 completed modules and the EDP dependency mapping framework.

8.5 Follow-On Research Priorities

Research Question	Priority	Rationale	Suggested Source/Method
RansomHub operator attribution: Is RansomHub Russia-based, and what is its FSB protection status? (Question retains value for successor and affiliate tracking despite the April 2025 collapse.)	HIGH	RansomHub absorbed the largest share of the post-ALPHV/LockBit affiliate diaspora and was the dominant active brand until it went dark in April 2025; Qilin then absorbed the largest share of its displaced affiliates. Attribution is required before individual action can be contemplated.	IC collection; blockchain forensics on RansomHub payment wallets; forum persona analysis (Recorded Future, Intel 471)
Affiliate pool composition post-LockBit/ALPHV: How many active affiliates migrated, and to which programs?	HIGH	Affiliate containment following future takedowns requires knowing the current affiliate pool distribution.	Flashpoint/Intel 471 underground monitoring; Coveware victim-side TTP analysis
Healthcare targeting driver: Are specific affiliate archetypes disproportionately targeting healthcare, or is it a platform-level pattern?	HIGH	If healthcare over-targeting is driven by specific affiliates rather than operator choice, disruption strategy differs.	Coveware TTP data; CISA sector analysis; FBI sector-reporting data
Monero adoption rate trajectory: At what point does Monero dominance materially degrade blockchain-tracing effectiveness?	MEDIUM	Current Chainalysis figures rely on Bitcoin payment visibility; if Monero crosses a threshold share, reported payment totals become systematically understated.	Chainalysis/TRM Monero tracing capability briefings; on-chain analysis
Post-fragmentation stabilization: Will the 124-group ecosystem	MEDIUM	Stabilization into 5-10 dominant brands would change disruption priority;	Corvus/Secureworks quarterly tracking; forum monitoring for

consolidate or continue fragmenting?		continued fragmentation would favor cross-ecosystem pressure over brand-specific targeting.	consolidation signals
Dark Covenant 3.0 screening for Qilin, Play, and INC Ransom (RansomHub defunct April 2025; BlackSuit disrupted July 2025)	HIGH	Four of the most active current groups have not been publicly screened for FSB protection relationships; screening is required before individual attribution actions.	IC collection; Recorded Future Insikt Group analysis

8.6 Module 07 Assessment Summary

The ransomware group and RaaS operator layer is simultaneously the highest-value disruption target in the EDP ecosystem and the most structurally resilient. Its resilience does not derive from technical sophistication alone but from the structural properties of the RaaS model: separation of development from deployment; a large and mobile affiliate pool; abundant replacement tooling from leaked source code; and sustained state tolerance from the Russian government. Direct brand disruption has produced measurable but temporary effects. The leverage that will produce durable ecosystem degradation lies not in defeating individual brands but in making the operator function economically unviable — through sustained payment rail pressure, victim non-payment normalization, and simultaneous disruption of the upstream supply nodes without which affiliates cannot function effectively.