EDP ECOSYSTEM DEEP-DIVE

EDP SUPPLEMENT: NEGOTIATION SERVICES

ANALYTICAL SCOPE NOTE

Module 15 has a dual character unlike any other module in this series. It covers both criminal-side negotiation services (internal RaaS functions and rogue recovery intermediaries that facilitate ransomware monetization) and legitimate defender-side negotiation firms (IR-side providers that function as disruption multipliers by reducing payment rates and improving victim outcomes). These two categories are analytically distinct and require separate assessment frameworks. Criminal-side functions are evaluated as ecosystem participants; legitimate negotiation firms are evaluated as structural countermeasures and ecosystem leverage points. The module proceeds accordingly.

Module Number	15
Module Name	Negotiation Services
EDP Node Reference	No dedicated EDP node. Criminal-side negotiation is internal to ransomware operations (cross-cutting); rogue recovery companies cross-reference Node 07 (Underground Forum Trust Infrastructure). Legitimate negotiation firms function as disruption multipliers. See Section 8 for Dependency Map recommendations.
Ecosystem Layer	Extortion Interface / Victim-Attacker Monetization Bridge
Upstream Connections	Ransomware/RaaS Operations (Module 07 / cross-cutting); Leak Site Operations (Module 08 / Node 06); Underground Forums (Module 10 / Node 07)
Downstream Connections	OTC Brokers (Module 12 / Node 01) and financial chain when payment occurs; victim recovery chain when payment is avoided
Research Date	April 2026
Primary Researcher	Reno
Source Tools Used	Perplexity AI; ReliaQuest; Coveware by Veeam; GuidePoint Security; CyberSecOp; Cyber Centaurs; Sophos; Chainalysis/CyberScoop; Cyble
Handling	INTERAGENCY

SECTION 1: WHAT IT IS

Definition and Ecosystem Position

Negotiation services occupy the extortion interface of the ransomware supply chain — the operational space between the moment a victim receives a ransom demand and the moment a payment decision is made (or refused). They are not infrastructure in the sense of BPH, forums, or mixing services; they are human-mediated functions that determine the conversion efficiency of the extortion stage. On the criminal side, effective negotiation specialists increase the proportion of victims who pay and the average value of ransoms collected. On the

defender side, professional negotiators reduce payment rates, lower settlement amounts, and provide governance and compliance infrastructure that manages sanctions risk.

This dual character makes Module 15 structurally different from all prior modules. Modules 01 through 14 cover criminal ecosystem supply chain components. Module 15 covers both a criminal function (criminal-side negotiation) and its primary countermeasure (legitimate negotiation and IR services). The module treats these separately, assessing criminal-side negotiation as an ecosystem participant and legitimate negotiation firms as structural disruption mechanisms — the most direct and empirically validated countermeasures in the ransomware supply chain.

Criminal-Side Negotiation: How It Functions

RaaS programs and their affiliates operate semi-scripted negotiation playbooks that have evolved significantly from early ransomware extortion. Current criminal-side negotiation TTPs include time-pressure tactics (countdown timers, escalating demand deadlines), discount offers positioned as limited-time windows, "PR damage" threats tying payment to data publication on leak sites, victim-specific taunts using exfiltrated data samples to prove access, and pseudo-SLA language ("we can restore your systems in X hours") that mimics legitimate service provider communications.

[CREDIBLE] ReliaQuest notes that in Q3 2024, ransomware groups continued to refine their extortion operations and leak-site threat mechanisms. RaaS operators that successfully scale victim counts rely on affiliates and internal negotiation specialists to manage dozens of concurrent chats per operator — negotiation is a bottleneck function that limits operator throughput. ReliaQuest forecasts LLM-supported negotiation as a realistic medium-term development that would allow criminal operators to manage significantly more victims simultaneously, overcoming language barriers and scaling communications capacity.

Legitimate-Side Negotiation: How It Functions

Professional IR-side negotiation firms provide a structured engagement model that includes 24/7 incident response hotlines, threat-actor communications management, ransom demand analysis using historical case data, settlement logistics, and OFAC/sanctions compliance documentation. Their primary value proposition to victims is not simply price reduction but decision-quality intelligence: knowing the decryptor reliability of specific ransomware strains, the re-extortion risk profile of specific crews, and the realistic probability of data recovery from backups versus payment.

Coveware by Veeam reports that with its incident-response retainer, more than 70% of supported clients avoid paying ransom entirely, relying on restore and recovery instead. This figure represents the most strategically significant metric in this module: it means that professional negotiation engagement — before the payment decision — produces a non-payment outcome in the majority of cases. The implication for ecosystem-level disruption is direct: scaling access to professional negotiation services is a validated demand-side countermeasure that reduces ransomware revenue more reliably than most enforcement actions.

The Rogue Recovery Company Problem

[CONFIRMED] GuidePoint Security's investigation documented a case in which a commercial "recovery company" inserted itself into an existing victim-attacker chat portal and privately negotiated with the ransomware affiliate — not to reduce the ransom, but to secure a $250,000 side payment from the affiliate in exchange for convincing the victim to pay $3.75M instead of accepting the lower $3.5M settlement the victim's team had negotiated. The recovery company representative was working against the victim's interest while presenting as a victim-side advocate.

This "RecoveryCo" archetype represents a documented criminal infiltration of the legitimate negotiation market. These operators typically present commercially as legitimate recovery services, claim proprietary decryption capabilities (which are in fact reused attacker-provided decryptors purchased at a markup), and maintain undisclosed financial relationships with ransomware affiliates. They are financially incentivized to maximize ransom payments, not minimize them — an exact inversion of their stated purpose.

[ANALYST INFERENCE] The RecoveryCo phenomenon likely understates the scale of undisclosed criminal-side intermediaries operating within the commercial negotiation market. The GuidePoint case was identified through exceptional circumstance (investigators independently monitoring the affiliate's chat portal). Most cases involving

rogue recovery intermediaries would not produce equivalent visibility. Regulatory frameworks for negotiation service providers — analogous to law enforcement licensing requirements for private investigators — do not currently exist in most jurisdictions.

SECTION 2: KEY ACTORS AND EXAMPLES

Actor Typology: Criminal Side

Actor Type	Function	Key TTPs	Ecosystem Impact	Confidence
RaaS affiliate internal negotiation specialists	Manage victim chat sessions; run extortion playbook; coordinate with leak-site publication timing	Semi-scripted playbooks: countdown timers, discount windows, PR damage threats, pseudo-SLA language; increasingly businesslike tone; victim-specific taunts using exfiltrated data samples	Direct impact on victim payment conversion rate; negotiation quality limits attacker throughput at scale	**[CREDIBLE]** Moderate-High — operational TTPs documented; individual operator identities rarely attributed
Rogue recovery / "RecoveryCo" intermediaries	Insert into victim-attacker negotiations; maximize ransom paid while extracting side payment from affiliate	Present as victim-side advocates; reuse attacker decryptors as proprietary tools; negotiate for affiliate interest while billing victim; take percentage of ransom as undisclosed commission	Increases average ransom paid in affected cases; corrupts information environment for victims making payment decisions; potentially increases ransomware profitability on a per-case basis	**[CONFIRMED]** High — GuidePoint documented case with specific financial terms; $250k side payment confirmed in investigation
LLM-augmented negotiation operators (emerging / forecast)	Use AI language model assistance to manage concurrent victim chats at scale; overcome language barriers; generate victim-specific pressure communications	Multi-chat concurrent management; automated personalization of extortion communications; language-barrier elimination enabling RU-speaking crews to negotiate directly with English, French, Spanish, and other-language victims	Would significantly increase per-operator throughput; potential multiplier on RaaS program scalability and revenue	**[ANALYST INFERENCE]** Analyst Inference / Forecast — ReliaQuest identifies as realistic medium-term development; not confirmed as operational as of April 2026

Actor Typology: Legitimate / Defender Side

Actor / Firm	Type	Key Capabilities	Documented Outcomes	Confidence

Coveware by Veeam	IR-integrated ransomware negotiation and response; retainer-based	24/7 incident response hotline; threat-actor communications; decryptor reliability analysis; OFAC/sanctions checks; >70% non-payment rate for retainer clients	>70% of supported clients avoid payment entirely; primary emphasis is backup recovery enablement and negotiation as time-buying while IR proceeds	**[CONFIRMED]** High — Coveware publishes quarterly ransomware reports with disclosed methodology
GuidePoint Security	Full-spectrum cybersecurity IR firm with dedicated ransomware negotiation capability	Threat-actor-specific intelligence; structured negotiation strategy; documented "RecoveryCo" investigation capability; settlements with reductions exceeding 85% in some engagements	85%+ demand reductions cited in some cases; specific aggregate statistics not published; also documented rogue recovery company infiltration in 2024	**[CONFIRMED]** High — GuidePoint published the RecoveryCo case; negotiation capability well-documented
CyberSecOp	Mid-tier ransomware negotiation and recovery services firm	200+ cases per year throughput; claims 99% full decryption success rate; generally reduces demands to below 50% of initial ask	200+ cases/year indicates significant market share for mid-tier firm; claimed outcomes not independently verified at aggregate level	**[CREDIBLE]** Credible — figures self-reported; methodology not independently disclosed; directionally consistent with industry
Cyber Centaurs	Specialized ransomware negotiation boutique	Rapid-response focus; experience reducing ransom demands; smaller throughput than CyberSecOp or Coveware	Outcomes not publicly specified beyond marketing claims; consistent with broader IR-side negotiation market	**[CREDIBLE]** Credible — operational firm; aggregate outcome data not available
Insurance-aligned negotiation and case management services	Negotiation capability embedded in cyber insurance carrier panels or IR firms prioritized by carriers	Coordinate between victim, carrier, IR teams, and counsel; manage OFAC compliance documentation; manage claims data and precedent for bargaining position; determine payment permissibility and insurability	Insurance-aligned negotiators may face structural incentives to minimize payment (carrier loss control) or accept payment (claims processing efficiency); alignment varies by carrier	**[CREDIBLE]** Moderate-High — structural role well-documented; carrier-specific alignment data not publicly available

GuidePoint RecoveryCo Case: Documented Rogue Intermediary Flow

Stage	Actor	Action	Financial Terms
Initial victim engagement	RecoveryCo representative	Contacts victim presenting as a commercial decryption/recovery service; victim accepts RecoveryCo as advocate	Commercial recovery fee to victim not disclosed in reporting
Unauthorized chat portal access	RecoveryCo representative	Inserts into victim's existing ransomware affiliate chat portal without victim's full	N/A

		understanding; begins communicating with the LockBit-like affiliate	
Criminal-side side-deal negotiation	RecoveryCo representative + affiliate	Privately negotiates with the affiliate; affiliate offers $250,000 to RecoveryCo if they can convince a different victim to pay $3.75M instead of the $3.5M already negotiated	$250,000 side payment offered by affiliate to RecoveryCo
Victim outcome impact	Victim (unaware)	Victim would have paid $250,000 more than the amount their team had independently negotiated, with the excess going to the affiliate and the intermediary	$250,000 additional ransom; split between affiliate and RecoveryCo per undisclosed arrangement
Investigation and exposure	GuidePoint Security	GuidePoint investigators monitoring the affiliate's chat portal independently identified the RecoveryCo representative's intervention and the side-deal offer	Case documented and published as industry warning; no confirmed prosecution as of April 2026

SECTION 3: INFRASTRUCTURE DEPENDENCIES

Criminal-Side Dependencies

Ransomware/RaaS operational infrastructure: Criminal-side negotiation is fully internal to RaaS operations — it requires no external service infrastructure beyond the ransom chat portals and communication channels embedded in the ransomware kit or operated by the RaaS platform. Chat portals are typically Tor-hosted web interfaces accessible via onion link embedded in the ransom note.

Leak site hosting (Node 06 / Module 08): Leak site publication is the primary escalation lever available to criminal negotiators. The threat of data publication — and the credible demonstration of access via sample data releases — is the core pressure mechanism. Leak site disruption (Phase C / Node 06) directly degrades the value of this negotiation lever.

Underground forums (Node 07 / Module 10): Rogue recovery companies recruit criminal-side affiliate relationships and advertise their services through underground forum channels. Forum reputation infrastructure enables the trust relationships that make RecoveryCo-style side deals operationally viable.

Legitimate-Side Dependencies

Ransomware intelligence data: Legitimate negotiation firms depend on accumulated case data — decryptor reliability by strain, average reduction achievable by group, re-extortion risk profiles — to provide value beyond simply relaying communications. This intelligence compounds over case volume and is not replicable without sustained market presence.

OFAC/Treasury sanctions guidance: Legitimate negotiators must maintain current awareness of OFAC designations and guidance on ransomware payment compliance. The 2020 OFAC advisory on ransomware payments and subsequent guidance create a compliance infrastructure requirement that professional negotiators integrate into their engagement workflow — and that directly prevents payments to designated groups.

Incident response and insurance ecosystem: Legitimate negotiation firms operate within a broader IR and cyber insurance ecosystem. Insurance carriers panel specific IR firms; counsel retains specific negotiators. The negotiation firm's position in this referral network determines case volume more than marketing — creating a structural barrier to entry for new legitimate entrants.

Critical Chokepoints (Criminal Side)

Chokepoint	Description	Primary Owner	Disruption Method
Ransom chat portal infrastructure	Tor-hosted chat interfaces are the primary criminal negotiation channel; portal access is the mechanism through which rogue recovery companies insert themselves into victim-attacker communications	FVEY IC and LE (BPH disruption upstream); private sector IR firms (monitoring and detection)	BPH disruption (Phase A/C) degrades hosting for chat portals; IR firm monitoring of chat portals enables rogue intermediary detection (GuidePoint model)
Leak site publication as negotiation leverage	Criminal negotiators use leak site publication threats as primary pressure tool; without credible leak site capability, the core negotiation lever is significantly degraded	FVEY LE + IC; upstream hosting providers (Phase C / Node 06)	Leak site takedowns directly degrade criminal negotiation leverage; reduces attacker's ability to maintain credible publication threat during negotiations
Rogue recovery company market access	Rogue intermediaries depend on victim trust to insert themselves into negotiations; market access depends on absence of licensing or vetting requirements for commercial negotiation services	National cybersecurity regulatory bodies; FTC; sector regulators (healthcare, financial services)	Minimum disclosure requirements for commercial negotiation services; licensing or registration frameworks; industry self-regulatory standards with enforcement mechanisms

Cross-Module Linkages

Module	Node	Linkage Type	Direction	Description
07 Ransomware / RaaS	Cross-cutting	Operational context	Upstream	Criminal-side negotiation is internal to RaaS operations; negotiation quality determines affiliate throughput and conversion rate
08 Leak Site Operations	06	Negotiation leverage	Upstream	Leak site publication threat is the primary escalation lever for criminal negotiators; leak site disruption directly degrades this lever's credibility
10 Underground Forums	07	Criminal recruitment	Upstream	Rogue recovery companies recruit affiliate relationships and may advertise through forum channels; forum trust infrastructure enables undisclosed side-deal relationships
12 OTC Brokers	01	Financial outcome	Downstream	When payment occurs, funds enter OTC broker / financial chain; successful legitimate negotiation that prevents payment is a direct upstream disruption to the entire financial chain (Nodes 01, 02, 08, 09)
09 BPH	03	Infrastructure	Upstream (criminal side)	BPH hosts the Tor-based ransom chat portals that are the operational interface for criminal negotiation; BPH disruption degrades chat portal availability

SECTION 4: DISRUPTION LEVERAGE POINTS

Criminal-Side Disruption Levers

Lever	Owner	Best Method	Backfire Risk	EDP Phase
Leak site takedown (principal negotiation lever degradation)	FVEY LE + IC; upstream hosting providers	Phase C Node 06 BPH and hosting disruption that removes the attacker's primary escalation tool; victim willingness to negotiate without payment increases when data publication threat is less credible	**LOW**	Phase C — direct lever on criminal negotiation capability
Ransom chat portal disruption (BPH upstream action)	FVEY IC and LE; upstream BPH providers	Phase A BPH disruption that degrades Tor-hosted chat portal infrastructure; increases friction in victim-attacker communications and may trigger attacker errors or impatience that benefit victim	**LOW-MEDIUM** — chat portals reconstitute quickly; disruption windows are short	Phase A/C — indirect; compound with BPH action
Rogue recovery company enforcement	FTC; DOJ (wire fraud, extortion facilitation); sector regulators	Prosecution of documented rogue intermediaries under wire fraud and extortion facilitation statutes; mandatory disclosure requirements for commercial negotiation services; licensing or registration frameworks	**LOW**	Regulatory / LE — not tied to a specific EDP phase; standalone enforcement action
LLM negotiation capability disruption (future / conditional)	Platform providers (OpenAI, Anthropic, Google); sector regulators	Terms of service enforcement by AI providers against ransomware negotiation use cases; detection of LLM-generated extortion communications; pre-positioned monitoring for LLM-assisted criminal negotiation patterns	**LOW** — not yet an active threat; requires pre-positioning	Emerging / Phase B-C — pre-positioning action recommended

Legitimate-Side Scaling as Disruption Mechanism

Expanding victim access to professional negotiation services is a validated demand-side disruption mechanism with measurable impact. Coveware's >70% non-payment rate for retainer clients demonstrates that professional negotiation engagement — not enforcement action, not technical controls, but a human-mediated decision-support service — produces non-payment outcomes in the majority of cases. Scaling this capability to victims who currently lack access is a direct ransomware revenue reduction mechanism.

Scaling Mechanism	Description	Owner	Expected Impact
CISA-facilitated free or subsidized negotiation support for critical infrastructure	Government-funded or government-coordinated access to professional negotiation services for critical infrastructure sectors that lack in-house capability or IR retainers	CISA; HHS (healthcare); sector-specific agencies; major IR firms as contractors	Extends >70% non-payment rate to critical infrastructure victims currently making payment decisions without professional negotiation support
Non-payment norm reinforcement through outcome transparency	Public disclosure (with victim consent) of cases where professional negotiation enabled non-payment and successful recovery; counters attacker	CISA; FBI; private sector IR firms; cyber insurance associations	Normalizes non-payment as an achievable outcome; reduces cognitive anchoring to payment as default response; degrades attacker negotiation leverage

	narrative that payment is the only viable path		
OFAC compliance integration standards for negotiation firms	Formal standards or guidance requiring all commercial negotiation services to conduct OFAC screening, maintain communication logs, and document compliance with payment advisory requirements	Treasury/OFAC; CISA; FTC	Closes the rogue recovery company disclosure gap; creates paper trail for enforcement; prevents payment to designated groups in cases involving non-professional intermediaries
Cyber insurance non-payment incentive structures	Insurance carrier policy structures that reward non-payment (e.g., lower deductibles, higher limits, preferred panel IR access) to create financial incentives for victim non-payment decisions	Cyber insurance carriers; Lloyd's market; sector regulators	Aligns carrier financial interest with non-payment outcomes; currently mixed — some carrier incentives favor payment as faster claims resolution

Compounding Actions

- Scale professional negotiation access to sectors with low current penetration (small and mid-sized healthcare, local government, education). These sectors have the highest ransomware vulnerability and the lowest professional IR/negotiation capability — the gap where the non-payment rate differential between supported and unsupported victims is largest.
- Establish minimum disclosure standards for commercial ransomware recovery services. Requiring firms to disclose any financial relationship with threat actors, identify all parties to negotiations, and maintain communication logs would eliminate the undisclosed-affiliate-relationship model that enables RecoveryCo-type operations.
- Pre-position LLM-use monitoring: engage AI platform providers now to develop detection capabilities for ransomware-specific LLM use patterns before criminal adoption of AI negotiation tools becomes operational. The window for pre-positioning is currently open; once LLM-assisted negotiation is operationally deployed by major ransomware groups, reactive detection is significantly harder.
- Use leak site takedowns (Phase C / Node 06) to compound negotiation disruption: each credible leak site takedown reduces the threat actor's negotiation leverage, increases victim willingness to refuse payment, and degrades the criminal-side negotiation playbook in real time.

SECTION 5: RESILIENCE AND REPLACE DIFFICULTY

Criminal-Side Resilience

Criminal-side negotiation is a function internal to RaaS operations rather than an external service dependency. It is therefore not subject to replace difficulty in the same sense as external supply chain nodes. RaaS programs that lose an effective internal negotiation specialist can reassign the function to other affiliate members, develop new specialists, or — in the emerging scenario — adopt LLM tools to reduce the skill requirement. The criminal-side negotiation function has no single external chokepoint.

[ANALYST INFERENCE] The most significant structural vulnerability in criminal-side negotiation is the LLM adoption trajectory. If major ransomware groups adopt LLM tools for victim communications before law enforcement and platform providers develop detection and disruption capabilities, the per-operator throughput multiplier could substantially increase ransomware revenue per group — reversing some of the gains from the 2024 payment decline. This is a genuine emerging threat that deserves pre-positioning attention disproportionate to its current operational status.

Rogue Recovery Company Resilience

Rogue recovery companies are resilient because they operate in the absence of regulatory barriers to entry. The legitimate-looking commercial recovery market has no licensing requirement, no disclosure standards, and no enforcement mechanism for undisclosed affiliate relationships. A new rogue recovery company can establish a professional website, purchase advertising, and begin inserting itself into victim negotiations within days. The GuidePoint-documented case has produced no confirmed prosecution — suggesting that the existing enforcement framework for this activity is unclear or untested.

Legitimate Firm Resilience and Market Dynamics

Factor	Current State	Trend	EDP Implication
Firm count and market competition	Small number of established firms (Coveware, GuidePoint, CyberSecOp, Cyber Centaurs, others); market concentrated among retainer-based IR firms	Growing demand; new entrants expected; but trust and case-data barriers create incumbent advantage	Legitimate market consolidation is not itself an EDP concern; scale-out to underserved sectors is the priority
Non-payment rate sustainability	>70% non-payment for Coveware retainer clients; claims of 50%+ demand reduction across mid-tier firms	Attacker adaptation (more aggressive leak threats, shorter deadlines, LLM scaling) may erode non-payment rates over time	Non-payment rate is a leading indicator for ecosystem-level disruption effectiveness; monitoring for rate decline signals attacker negotiation capability improvement
OFAC compliance integration	Professional negotiation firms conduct OFAC screening; some sectors (healthcare, critical infrastructure) increasingly require documented compliance	OFAC advisory guidance expanding; post-2024 designation actions have increased the compliance burden on negotiation firms	OFAC compliance integration by negotiation firms is a structural enforcement mechanism that prevents payment to designated groups independent of direct LE action
Insurance carrier alignment	Carriers panel preferred IR firms; some carriers create de facto negotiation service access for insured victims	Carrier incentive structures are mixed; some carriers favor rapid claims resolution (payment) over longer negotiation (non-payment but higher IR costs)	Regulatory engagement with cyber insurance carriers on carrier incentive structures that favor non-payment would amplify legitimate firm non-payment rate effects

SECTION 6: INDICATORS AND KPIs

Ecosystem Health Indicators

Indicator	Normal State (2024-2025 Baseline)	Pressure / Degradation Signal
Ransomware non-payment rate (victims using professional negotiation support)	>70% non-payment for Coveware retainer clients (2024-2025 baseline); lower for victims without professional support	Declining non-payment rate signals attacker negotiation improvement or LLM adoption; INCREASING non-payment rate signals defender-side scaling effectiveness
Average ransom demand reduction achieved by professional negotiators	CyberSecOp: generally below 50% of initial ask; GuidePoint: 85%+ in some engagements; Coveware: non-payment preferred over reduction	Declining reduction rates signal attacker adaptation (more aggressive tactics, shorter deadlines); may precede LLM negotiation adoption

Ransomware total revenue (annual, USD)	$813.5M in 2024 (down 35% from $1.25B in 2023); decline attributed partly to more victims refusing to pay or negotiating aggressively	Revenue rebound above $1B signals either enforcement gap, attacker capability improvement, or negotiation service access deficit in high-victim sectors
Reported rogue recovery company cases	GuidePoint 2024 case is the only publicly documented confirmed case; others likely unreported	Increase in reported cases signals growing rogue intermediary market; absence of reported cases does not indicate absence of activity given detection difficulty
LLM-assisted criminal negotiation indicators	Not currently confirmed as operational (April 2026); ReliaQuest identifies as forecast/emerging	Detection of LLM-characteristic language patterns in ransomware communications; increase in concurrent victim management per operator; language barrier elimination in attacker communications

Disruption KPIs

KPI	Baseline	Target	Collection Method
Non-payment rate for critical infrastructure victims (annual)	No sector-specific baseline available; Coveware overall >70% for retainer clients; lower for non-retainer/unassisted victims	Critical infrastructure non-payment rate above 60% sustained across two consecutive years; CISA-facilitated support program as mechanism	CISA incident reporting data; FBI IC3 ransomware data; cyber insurance industry claims data (via NAIC or Lloyd's)
Annual ransomware total revenue (ecosystem-wide)	$813.5M in 2024 (Chainalysis-based)	Below $600M sustained over two consecutive years; not attributable to reduced attack volume alone (cross-reference DLS victim counts)	Chainalysis annual report; TRM Labs crypto crime report; cross-reference with DLS victim volume and non-payment rate trend
Commercial negotiation service OFAC compliance rate	Major established firms (Coveware, GuidePoint) conduct OFAC screening; no formal standard; smaller/rogue firms have no compliance requirement	100% of commercial negotiation services for which OFAC guidance applies conducting documented screening; achieved via mandatory disclosure standards	OFAC advisory compliance tracking; DOJ enforcement actions for unlicensed ransomware payment facilitation; FTC enforcement referrals
Rogue recovery company enforcement actions (annual)	Zero confirmed prosecutions as of April 2026 despite documented GuidePoint case	At least 1 prosecution per year for confirmed rogue intermediary; mandatory disclosure framework in place within 24 months	DOJ/FTC press releases; state AG enforcement actions; industry self-regulatory reporting

Alert Thresholds

Threshold	Trigger Condition	Response
Non-payment rate for professional-negotiation-supported victims declines below 60%	Coveware or equivalent reporting shows year-over-year decline in non-payment rate below 60% for retainer clients	Assess for attacker negotiation capability improvement; investigate for LLM-assisted negotiation deployment by major RaaS groups; consider defensive countermeasures briefing for IR community

Confirmed LLM-assisted criminal negotiation detected in operational case	IR firm or LE confirms LLM-characteristic patterns in ransomware victim communications with supporting technical analysis	Immediate interagency briefing; engage AI platform providers on detection and countermeasure development; assess for non-payment rate impact; accelerate CISA-facilitated negotiation support program
Second confirmed rogue recovery company case in single calendar year	Two or more documented cases of commercial recovery firms with undisclosed affiliate relationships in a 12-month period	Initiate regulatory action on commercial negotiation service disclosure requirements; FTC referral; assess for DOJ wire fraud prosecution pathway for documented cases
Ransomware revenue rebounds above $1B annually	Chainalysis or TRM Labs documents annual rebound above $1B after 2024 decline	Full assessment of negotiation service penetration in affected victim sectors; compare with OFAC designation activity (Modules 11-13); determine whether negotiation gap or enforcement gap is primary driver

SECTION 7: SOURCES AND CONFIDENCE

Primary Sources

Legitimate Negotiation Firms and IR Research:

- Coveware by Veeam — incident-response and retainer materials; quarterly ransomware reports; >70% non-payment rate for retainer clients; 24/7 negotiation and threat-actor analytics; OFAC/sanctions check integration; primary source for legitimate-side outcome data.
- GuidePoint Security — "Ransomware Negotiation Services" documentation; published investigation of third-party "RecoveryCo" rogue intermediary case (2024); $250,000 side payment documentation; 85%+ demand reductions in some engagements.
- CyberSecOp — "Ransomware Negotiation and Recovery Services" marketing materials; 200+ cases per year throughput; below 50% demand reduction claim; 99% full decryption success rate claim.
- Cyber Centaurs — "Ransomware Negotiation Services" rapid-response marketing materials.

Threat Intelligence:

- ReliaQuest — "Ransomware and Cyber Extortion in Q3 2024": criminal negotiation evolution; LLM-based negotiation forecast for medium-term; concurrent victim management as RaaS bottleneck.
- Cyble / threat-intel summaries — "Ransomware Tactics by Threat Actors in 2024": evolution of extortion and communication tactics; victim-specific taunting and pseudo-SLA language documentation.

Macro Ransomware Context:

- Chainalysis / CyberScoop / HackerNews — 2024 ransomware revenue figures ($813.5M, down 35% from $1.25B in 2023); attribution of lower payments to victim negotiation resistance and enforcement.
- Sophos — "The State of Ransomware in Healthcare 2024": 60%+ of attacked healthcare organizations experienced data encryption; significant share recovered without full payment via backups or third-party assistance; sector-specific payment behavior context.

Confidence Assessment by Topic

Topic	Confidence Level	Basis	Key Limitations
Coveware >70% non-payment rate	**[CREDIBLE]** CREDIBLE	Coveware publishes quarterly ransomware reports with stated methodology; figure consistent across multiple reporting periods	Applies to Coveware retainer clients — a self-selected population more likely to have good backup posture and IR capability; not representative of all victim outcomes

GuidePoint RecoveryCo case documentation	**[CONFIRMED]** CONFIRMED	GuidePoint published detailed case documentation including specific financial terms ($250,000 side payment, $3.75M versus $3.5M ransom) and methodology of investigation	Single documented case; frequency of similar undisclosed arrangements is not quantifiable from open sources
CyberSecOp 99% decryption success and 50% reduction claims	**[CREDIBLE]** CREDIBLE — self-reported; not independently verified	Commercially published claims; directionally consistent with industry outcomes; CyberSecOp is an operational firm with market presence	Self-reported outcome statistics without disclosed methodology; case selection and outcome definition may differ from Coveware's published framework
ReliaQuest LLM negotiation forecast	**[ANALYST INFERENCE]** ANALYST INFERENCE — forecast, not confirmed	ReliaQuest Q3 2024 report identifies LLM adoption as realistic medium-term development based on observed RaaS capability investment patterns	Not confirmed as operational; forecast is speculative; timeline and adoption rate are unknown; major RaaS groups have not publicly disclosed LLM negotiation tool use as of April 2026
35% ransomware revenue decline partly attributable to victim negotiation resistance	**[CREDIBLE]** CREDIBLE	Chainalysis 2024 annual report; multiple reporting outlets cite negotiation resistance alongside enforcement as contributing factors	Causal attribution to negotiation versus enforcement versus victim backup improvement is not independently quantified; likely all three factors contributed

Intelligence Gaps

- Rogue recovery company prevalence: The GuidePoint case is the only publicly documented confirmed instance. Actual prevalence of undisclosed affiliate relationships in the commercial recovery market is unknown and likely significantly underestimated given detection difficulty.
- Non-payment rate by sector: The Coveware >70% figure applies to retainer clients broadly. Sector-specific non-payment rates — particularly for healthcare, local government, and education (the sectors with lowest professional negotiation access) — are not published.
- Criminal negotiation specialist identities: Internal RaaS affiliate negotiation specialists are not publicly attributed in open sources. Understanding their profiles, compensation structures, and operational role within specific RaaS programs would inform disruption targeting.
- LLM adoption signals: No confirmed open-source indicator of operational LLM use in criminal ransomware negotiations as of April 2026. Pre-positioning monitoring frameworks for early detection remain undeveloped.

SECTION 8: ANALYST ASSESSMENT

Key Takeaway

Module 15 is the only module in this series where the primary disruption mechanism is not enforcement or financial action but rather scaling access to a defender-side countermeasure. Coveware's >70% non-payment rate for professional negotiation clients is the most direct ransomware revenue reduction figure in the entire EDP dataset — more immediate and measurable than any single enforcement action, and achievable without interagency coordination, foreign policy constraints, or blockchain forensics. The central recommendation of this module is simple: the gap between the non-payment rate for professionally supported victims and the non-

payment rate for unsupported victims is the largest unaddressed disruption opportunity in the ransomware supply chain.

Two secondary threats require pre-positioning attention that is disproportionate to their current operational status. First, the rogue recovery company phenomenon is an unregulated criminal infiltration of the legitimate negotiation market that is likely more prevalent than the single documented case suggests and for which no enforcement framework currently exists. Second, the LLM-assisted criminal negotiation trajectory — if realized — would represent a meaningful multiplier on RaaS operator throughput and revenue that would partially reverse the gains from the 2024 payment decline. Neither threat is currently receiving regulatory or enforcement attention commensurate with its potential impact.

Priority Recommendation

Immediate: CISA should pilot a federally facilitated professional negotiation support program for critical infrastructure victims in sectors with demonstrated low IR retainer penetration (healthcare, local government, education). Even a modest increase in professional negotiation access in these sectors — moving sector non-payment rates from an estimated 30-40% without support toward the 70%+ achievable with professional support — would produce a measurable reduction in ransomware revenue targeting US critical infrastructure.

Near-term: Establish minimum disclosure standards for commercial ransomware negotiation and recovery services. Require registered firms to: (1) disclose any financial relationship with ransomware threat actors or affiliates; (2) identify all parties to negotiations in which they participate; (3) conduct and document OFAC screening; and (4) maintain communication logs for a minimum retention period. These requirements directly close the regulatory gap that enables RecoveryCo-type operations.

Medium-term: Engage AI platform providers (OpenAI, Anthropic, Google, Mistral) on ransomware-specific LLM use monitoring before operational criminal adoption makes detection reactive. The pre-positioning window is currently open. Developing detection signatures for LLM-characteristic patterns in ransomware communications now — while adoption is still pre-operational — is significantly lower cost than developing them after major RaaS groups have deployed and optimized AI-assisted negotiation tools.

Framing note: Legitimate negotiation services are not an EDP supply chain node. They are the most scalable, lowest-backfire disruption mechanism in the ransomware ecosystem. The appropriate policy posture is to fund, scale, and regulate them — not to monitor them as adversary infrastructure.

Connection to EDP Disruption Playbook

Module 15 does not map to any existing EDP Disruption Playbook phase. Criminal-side negotiation is internal to RaaS operations and disrupted indirectly via Phase C leak site actions (Node 06); rogue recovery companies require standalone enforcement action outside the current phase framework; legitimate negotiation services are a demand-side countermeasure that complements but does not replace the Phase A/B/C financial and infrastructure actions.

The module's most important Playbook connection is a framing one: the 35% ransomware revenue decline in 2024 reflects the compound effect of Phase A financial actions (OTC, exchange enforcement), Phase B/C enforcement, AND increased victim resistance and non-payment — a demand-side effect that the EDP Playbook does not currently model. Adding a demand-side countermeasure layer to the EDP framework, anchored by scaled professional negotiation access, would give the Playbook a more complete picture of the disruption mechanisms available across the full ecosystem.

Dependency Map Update Recommendations

Recommendation	Current State	Proposed Change	Rationale
No EDP node for negotiation services	No dedicated node; "assess on arrival" per module plan	Do not add a dedicated node for negotiation services. Criminal-side negotiation is internal to RaaS operations. Legitimate negotiation is a countermeasure, not a supply chain component.	A dedicated node would create a category error: legitimate IR firms are not criminal ecosystem actors. Internal RaaS negotiation is already captured under cross-

			cutting ransomware operations. A separate node adds analytical complexity without structural insight.
Add demand-side countermeasure layer to EDP framework	EDP framework covers supply-side (criminal ecosystem nodes) and enforcement (disruption playbook phases)	Add a Demand-Side Countermeasures annotation or appendix to the EDP framework documenting scaled professional negotiation access as a validated, empirically supported disruption mechanism complementary to the supply-side Phases A, B, C	The >70% non-payment rate for professionally supported victims is the most directly validated disruption outcome in the entire EDP dataset. Excluding it from the framework understates the full disruption option set available to policy and enforcement actors.
Rogue recovery company enforcement gap	No regulatory framework; no confirmed prosecution; single documented case	Flag as a standalone enforcement gap requiring FTC and DOJ attention; recommend mandatory registration and disclosure framework for commercial ransomware negotiation services	The RecoveryCo archetype is a documented criminal facilitation of ransomware monetization operating in the absence of any enforcement framework. It does not fit existing EDP node categories but represents a specific, actionable enforcement gap.
LLM negotiation threat tracking	Not tracked; identified as forecast by ReliaQuest	Add LLM-assisted criminal negotiation as a monitored emerging threat indicator under the EDP framework; assign pre-positioning tasking to IC and private sector partners	If realized, LLM-assisted negotiation would increase RaaS operator throughput and partially reverse 2024 payment decline gains. Pre-positioning detection capability costs significantly less than reactive development after operational adoption.

Follow-On Research

- Sector-specific non-payment rate mapping: commission or task analysis of non-payment rates by victim sector (healthcare, local government, education, financial services, critical infrastructure) to identify the highest-gap sectors for prioritized professional negotiation access expansion.
- Rogue recovery company market survey: structured analysis of commercial ransomware recovery firms' disclosed practices, client agreements, and regulatory status; assess prevalence of undisclosed affiliate relationship indicators beyond the single documented GuidePoint case.
- LLM adoption monitoring framework: develop detection signatures for LLM-characteristic patterns in ransomware extortion communications; engage AI platform providers on ransomware-specific use-case monitoring; establish baseline for measuring adoption onset.
- Cyber insurance carrier incentive structure analysis: assess whether current carrier incentive structures (deductibles, panel IR firm access, claims processing speed) favor payment or non-payment outcomes; develop regulatory engagement pathway for incentive structure reform.
- CISA facilitated negotiation support program feasibility: assess legal authority, funding mechanism, staffing model, and scope for a CISA-coordinated professional negotiation support capability for critical infrastructure victims lacking IR retainers.

EDP SERIES: MODULE COMPLETION STATUS

Module 15 is the final module of the EDP Ecosystem Deep-Dive series. All 15 modules covering the Russia/CIS ransomware supply chain have been completed. See the vetted output folder for the full module set.

Modules 01-15 complete: Stealers, Loaders, Crypters, Callers/Spammers, IABs, Exploit Brokers, Ransomware/RaaS, Leak Site Operations, BPH, Underground Forums, Crypto Mixers, OTC Brokers, Money Launderers/Exchanges (pending), Mule Networks, Negotiation Services.