RANSOMWARE ECOSYSTEM

DEPENDENCY MAP, REFINED

Priority-Weighted Disruption Reference

Developed by Reno

ID	Node	Tier	Replace Difficulty	Primary Owner	Backfire Risk
01	OTC Crypto Brokers	**CRITICAL**	HIGH	Treasury / OFAC + FVEY financial partners	LOW: financial actions do not trigger FSB protection reflexes
02	High-Risk / Non-Compliant Exchanges	**CRITICAL**	HIGH	Treasury / OFAC + FVEY financial regulators + blockchain forensics firms	LOW
03	Bulletproof Hosting (BPH) Providers	**CRITICAL**	HIGH	FVEY IC + LE + upstream provider engagement (ISPs, registrars, CDN providers)	LOW-MEDIUM: target providers, not individuals
04	Initial Access Broker (IAB) Markets	**HIGH**	MEDIUM	FVEY LE + private sector threat intel (Intel 471, Flashpoint)	LOW
05	Botnet / Loader Ecosystems	**HIGH**	HIGH	FVEY IC + LE (FBI, NCA, Europol)	LOW-MEDIUM
06	Leak-Site Hosting Stack	**HIGH**	MEDIUM	FVEY LE + IC (for attribution); upstream hosting providers (for takedown)	LOW
07	Underground Forum Trust Infrastructure	**HIGH**	HIGH	FVEY LE + private sector underground monitoring (Intel 471, Flashpoint)	LOW
08	Mixing / Obfuscation Services	**HIGH**	MEDIUM	OFAC + blockchain forensics firms (Chainalysis, TRM, Elliptic)	LOW
09	Mule / Money Laundering Networks	**HIGH**	MEDIUM	FVEY LE FOs + FNS referral channel (domestic framing) + Rosfinmonitoring pipeline	LOW-MEDIUM

ID	Node	Tier	Replace Difficulty	Primary Owner	Backfire Risk
10	Credential / Stealer-Log Markets	**MEDIUM**	LOW-MEDIUM	FVEY LE + private sector (takedown / purchase disruption)	LOW
11	Crypter / Packer Services	**MEDIUM**	LOW	Private sector (AV/EDR vendors, signature development); LE for high-volume providers	LOW
12	Gray-Market VPS / Reseller Networks	**MEDIUM**	MEDIUM	Private sector (abuse reporting) + LE (for egregious providers)	LOW
13	Domain Reseller / DNS Ecosystems	**MEDIUM**	MEDIUM	Private sector (registrar engagement, domain clustering analysis) + LE	LOW
14	Data Exfiltration Staging Infrastructure	**MEDIUM**	MEDIUM	LE FOs (where victims cooperate and report) + IC	LOW
15	Operational Proxy / Anonymization Services	**MEDIUM**	LOW	IC + LE (for attribution, not disruption)	LOW

PRIORITY TIER: CRITICAL

NODE 01, OTC CRYPTO BROKERS [CRITICAL]

What It Enables	Large-volume cash-out and laundering coordination; converts ransom proceeds to fiat at scale
What Breaks	Large ransom payments cannot be liquidated; admin cut becomes frozen or stranded; operational income collapses
Replace Difficulty	HIGH: few brokers operate at the volume needed for high-value ransoms; OTC relationships are trust-dependent and slow to rebuild
Primary Owner	Treasury / OFAC + FVEY financial partners
Disruption Method	Designation / VASP KYC pressure / correspondent banking exposure
Backfire Risk	**LOW: financial actions do not trigger FSB protection reflexes**
Analyst Notes	Most durable pressure vector. Infrastructure rebuilds in days; financial exposure compounds over time. Top 20 OTC node designation is a defined investment priority. Chainalysis/TRM tracing is prerequisite.

NODE 02, HIGH-RISK / NON-COMPLIANT EXCHANGES [CRITICAL]

What It Enables	Conversion of cryptocurrency ransom payments to fiat; primary cash-out gateway for mid-tier volumes
What Breaks	Funds remain in crypto and cannot enter financial system; purchasing power inaccessible; actors forced to higher-friction alternatives
Replace Difficulty	HIGH: VASP compliance pressure has materially narrowed the compliant exchange landscape; non-compliant alternatives face increasing designation risk
Primary Owner	Treasury / OFAC + FVEY financial regulators + blockchain forensics firms
Disruption Method	Designation / enhanced due diligence referrals / VASP engagement
Backfire Risk	**LOW**
Analyst Notes	Closely linked to OTC node (01). Sanctions designation of exchange clusters compounds over time. Track sanctioned wallet activity post-designation as KPI, continued activity signals compliance gap.

NODE 03, BULLETPROOF HOSTING (BPH) PROVIDERS [CRITICAL]

What It Enables	Durable hosting for C2 servers, affiliate panels, leak sites, and negotiation infrastructure
What Breaks	Operations lose stable infrastructure; forced into gray-market VPS churn which increases detection risk and operational cost
Replace Difficulty	HIGH: full-service BPH with abuse-resistant upstream relationships is scarce; substitution requires time and criminal trust relationships
Primary Owner	FVEY IC + LE + upstream provider engagement (ISPs, registrars, CDN providers)
Disruption Method	ISP/ASN notifications / upstream provider engagement / infrastructure takedown
Backfire Risk	**LOW-MEDIUM: target providers, not individuals**
Analyst Notes	Move from BPH brand targeting to provider-of-provider leverage: registrar, nameserver, ASN, CDN dependencies per BPH operator. Upstream dependency graph is a defined investment priority. Document infrastructure fingerprints before takedown for

[redacted]	reconstitution tracking.

PRIORITY TIER: HIGH

NODE 04, INITIAL ACCESS BROKER (IAB) MARKETS [HIGH]

What It Enables	Sale of pre-compromised corporate network footholds (RDP, VPN, domain admin) to ransomware affiliates
What Breaks	Victim supply pipeline to affiliates shrinks; affiliates must conduct own intrusion (slower, higher exposure); operational tempo declines
Replace Difficulty	MEDIUM: IAB market is distributed; individual broker disruption is absorbed, but coordinated market pressure raises prices and slows supply
Primary Owner	FVEY LE + private sector threat intel (Intel 471, Flashpoint)
Disruption Method	Undercover market operations / infiltration / takedown / broker arrests
Backfire Risk	**LOW**
Analyst Notes	IAB disruption is low-backfire-risk, these actors are not typically state-protected. Rising IAB prices compress affiliate margins and reduce franchise attractiveness. Track new IAB listings per month as ecosystem health KPI.

NODE 05, BOTNET / LOADER ECOSYSTEMS [HIGH]

What It Enables	Mass malware delivery; loaders distribute ransomware payloads at scale to pre-compromised hosts
What Breaks	Payload distribution slows dramatically; campaigns require resource-intensive manual intrusion per victim
Replace Difficulty	HIGH: mature loader ecosystems (QBot, IcedID successor variants) represent years of infrastructure investment; rebuilding distribution capacity is slow
Primary Owner	FVEY IC + LE (FBI, NCA, Europol)
Disruption Method	Infrastructure takedown / sinkholing / C2 disruption
Backfire Risk	**LOW-MEDIUM**
Analyst Notes	Sinkholing operations produce intelligence on victim population and actor TTPs simultaneously with disruption. Coordinate with ISACs and private sector (Microsoft DART, Mandiant) for victim notification. High intelligence yield before takedown.

NODE 06, LEAK-SITE HOSTING STACK [HIGH]

What It Enables	Publication of stolen victim data to pressure payment; core extortion leverage mechanism for modern ransomware
What Breaks	Extortion leverage collapses without credible publication threat; victim payment incentive declines; double-extortion model degrades
Replace Difficulty	MEDIUM: new leak sites can be stood up in days, but with loss of SEO, victim following, and affiliate confidence
Primary Owner	FVEY LE + IC (for attribution); upstream hosting providers (for takedown)
Disruption Method	Takedown / trust destruction / decryptor release (undermines payment incentive)
Backfire Risk	**LOW**
Analyst Notes	Takedown of leak site simultaneously disrupts operations and signals to victims that payment may not be necessary. Combine with decryptor release where possible

	(Operation Cronos model). Post-takedown: monitor for reconstitution as intelligence on actor resilience.

NODE 07, UNDERGROUND FORUM TRUST INFRASTRUCTURE [HIGH]

What It Enables	Escrow services, arbitration, reputation systems, and forum administration that enable criminal market function
What Breaks	Market trust collapses; transaction costs rise; affiliate recruitment becomes unreliable; criminal commerce slows
Replace Difficulty	HIGH: trust relationships are person-dependent and non-transferable; escrow operators and forum admins have irreplaceable reputation capital
Primary Owner	FVEY LE + private sector underground monitoring (Intel 471, Flashpoint)
Disruption Method	Trust node disruption / reputation attacks / forum seizure / infiltration
Backfire Risk	**LOW**
Analyst Notes	Non-technical nodes are ecosystem-critical and low-backfire-risk. 'Top 10 trust nodes' targeting list is a defined investment priority. Disrupting escrow operators and arbitrators degrades market function independent of any technical action. Dependency analysis of removal effects is prerequisite.

NODE 08, MIXING / OBFUSCATION SERVICES [HIGH]

What It Enables	Transaction laundering and fund tracing disruption; enables actors to obscure ransom flows before cash-out
What Breaks	Blockchain tracing becomes significantly easier; actors forced to expose funds to enhanced due diligence at exchanges
Replace Difficulty	MEDIUM: multiple mixing alternatives exist; designation of one node pushes to next; but each shift raises friction and tracing cost for actors
Primary Owner	OFAC + blockchain forensics firms (Chainalysis, TRM, Elliptic)
Disruption Method	Designation / tracing / exchange-level flagging
Backfire Risk	**LOW**
Analyst Notes	Track 'share of ecosystem funds forced onto higher-friction rails' as KPI. Closely linked to exchange and OTC nodes (01, 02). Each designation raises actor cost even if alternative exists. Coordinate designations with exchange KYC pressure for compounding effect.

NODE 09, MULE / MONEY LAUNDERING NETWORKS [HIGH]

What It Enables	Fiat currency movement post cash-out; layering and integration of criminal proceeds; front company operation
What Breaks	Proceeds cannot enter financial system cleanly; actors accumulate crypto they cannot spend; operational costs rise
Replace Difficulty	MEDIUM: mule recruiters operate continuously; disruption of network requires sustained pressure rather than single action
Primary Owner	FVEY LE FOs + FNS referral channel (domestic framing) + Rosfinmonitoring pipeline
Disruption Method	Mule arrests / recruitment disruption / front company exposure / FNS referrals
Backfire Risk	**LOW-MEDIUM**

Analyst Notes	Mule recruitment pipeline disruption raises operational costs and slows scaling. FNS lifestyle inconsistency referrals (unexplained wealth vs. declared income) are domestic-law-framed and lower backfire risk than cyber-specific charges. Intermediary cash-out mapping is a defined investment priority.

PRIORITY TIER: MEDIUM

NODE 10, CREDENTIAL / STEALER-LOG MARKETS [MEDIUM]

What It Enables	Bulk stolen credentials used for initial access and lateral movement; feeds IAB pipeline
What Breaks	Credential reuse attacks decline; access costs rise for affiliates; IAB supply quality degrades
Replace Difficulty	LOW-MEDIUM: stealer log markets are numerous and distributed; disruption of individual markets is quickly absorbed
Primary Owner	FVEY LE + private sector (takedown / purchase disruption)
Disruption Method	Market takedown / bulk credential invalidation notifications / vendor engagement
Backfire Risk	**LOW**
Analyst Notes	Lower standalone impact than IAB markets (node 04) but feeds the IAB pipeline. Most effective when combined with IAB disruption. Victim notification programs (HaveIBeenPwned model) reduce attacker value of seized credential sets.

NODE 11, CRYPTER / PACKER SERVICES [MEDIUM]

What It Enables	Malware obfuscation to evade AV/EDR detection; extends operational lifespan of ransomware payloads
What Breaks	Detection rates increase; campaigns burn faster; actors must invest more in payload maintenance
Replace Difficulty	LOW: crypter services are commoditized; disruption of one provider causes rapid substitution
Primary Owner	Private sector (AV/EDR vendors, signature development); LE for high-volume providers
Disruption Method	Signature development / provider disruption / malware analysis
Backfire Risk	**LOW**
Analyst Notes	Best addressed through private sector detection investment rather than LE action. Each new crypter requires new signatures; detection arms race favors defenders when endpoint coverage is high. Track detection rate improvement as indirect KPI.

NODE 12, GRAY-MARKET VPS / RESELLER NETWORKS [MEDIUM]

What It Enables	Rapid redeployment and infrastructure churn after takedowns; fills gap between BPH and legitimate hosting
What Breaks	Recovery time increases after takedowns; actors face higher friction in spinning up replacement infrastructure
Replace Difficulty	MEDIUM: numerous reseller networks exist, but quality (abuse-tolerant, fast) providers are more limited
Primary Owner	Private sector (abuse reporting) + LE (for egregious providers)
Disruption Method	Abuse notifications / registrar engagement / ISP upstream pressure
Backfire Risk	**LOW**
Analyst Notes	Most effective as part of sustained infrastructure pressure alongside BPH targeting (node 03). Alone, impact is temporary. Key lever: upstream transit provider engagement, who sells IP space to the resellers?

NODE 13, DOMAIN RESELLER / DNS ECOSYSTEMS [MEDIUM]

What It Enables	Domain churn, phishing infrastructure, fast-flux hosting; enables rapid replacement of seized domains
What Breaks	Campaign infrastructure becomes easier to trace and seize; phishing and C2 rotation slows
Replace Difficulty	MEDIUM: domain churn is fast but leaves registration patterns; clustering analysis produces predictive attribution
Primary Owner	Private sector (registrar engagement, domain clustering analysis) + LE
Disruption Method	Registrar disruption / fast-flux tracking / DNS provider pressure
Backfire Risk	**LOW**
Analyst Notes	Infrastructure persistence tracking (Shadowserver, Censys) surfaces reconstitution patterns quickly. Document registration fingerprints before takedown. Most effective when combined with BPH/VPS pressure (nodes 03, 12).

NODE 14, DATA EXFILTRATION STAGING INFRASTRUCTURE [MEDIUM]

What It Enables	Temporary storage for stolen data before extortion; enables double-extortion model
What Breaks	Leak-site extortion operations slow or fail; actors must maintain victim access longer, increasing detection risk
Replace Difficulty	MEDIUM: staging infrastructure can be rebuilt, but disruption mid-operation forces re-exfiltration
Primary Owner	LE FOs (where victims cooperate and report) + IC
Disruption Method	Seizure / monitoring / victim cooperation
Backfire Risk	**LOW**
Analyst Notes	Intelligence value of monitoring staging infrastructure before seizure is high, reveals victim list, data held, and negotiation timeline. Victim cooperation is prerequisite; under-reported in current environment.

NODE 15, OPERATIONAL PROXY / ANONYMIZATION SERVICES [MEDIUM]

What It Enables	Conceals true server location and operator origin; degrades infrastructure attribution
What Breaks	Infrastructure attribution becomes easier; actor operational security degrades
Replace Difficulty	LOW: numerous VPN and proxy alternatives; disruption of individual services is quickly absorbed
Primary Owner	IC + LE (for attribution, not disruption)
Disruption Method	Attribution analysis; targeted disruption for high-value operators
Backfire Risk	**LOW**
Analyst Notes	Better treated as an attribution problem than a disruption target. Most value comes from using proxy metadata for operator identification, not from taking the proxy offline. Low standalone disruption value. Reassessment flag (June 2026): the First VPN takedown (Operation Saffron, May 2026) found one criminal-dedicated VPN serving 25 plus ransomware groups across 33 seized servers in 27 countries. Criminal-dedicated anonymization is more concentrated, and more disruptable, than this rating assumes. Revisit tier and disruption method at the next quarterly review.

NODE 16, EXPLOIT / VULNERABILITY BROKERS [CRITICAL]

What It Enables	Zero-day and N-day exploit acquisition for affiliates and operators; bypasses the IAB market entirely for targets requiring stealth or specific access capabilities; enables intrusion against hardened networks that resist commodity IAB techniques
What Breaks	High-value stealth access capability eliminated; operators restricted to commodity IAB-sourced access; attacks against hardened targets (critical infrastructure, financial sector) become significantly harder to initiate
Replace Difficulty	HIGH: zero-day market is concentrated among a small number of trusted brokers; relationships are reputation-dependent and slow to rebuild; bug class exhaustion following coordinated disclosure permanently degrades specific exploit families
Primary Owner	Policy lead: CISA + NSA (coordinated vulnerability disclosure, bug bounty scaling) | OFAC (designation of brokers serving state-adjacent customers) | FVEY IC (broker attribution)
Disruption Method	Coordinated vulnerability disclosure (CVD) reform to reduce unpatched windows; scaled bug bounty programs to exhaust bug classes before criminal market acquisition; OFAC designation of identified brokers with state-adjacent customer base; IC-led broker attribution
Backfire Risk	**LOW-MEDIUM: policy-track actions (CVD, bug bounty) carry no backfire risk; OFAC designation or public attribution of brokers with FSB/GRU customer adjacency carries medium risk; sequence policy actions first**
Analyst Notes	Added per EDP Module 06 assessment (CRITICAL tier recommendation). Not in original 15-node map. Disruption logic differs from all other nodes: primary lever is policy-track (CVD reform, bug bounty scaling), not law enforcement. Suggested placement: Phase A+ or Phase B-pre, as a prerequisite assessment before IAB-market operations. No dedicated EDP playbook phase currently exists for this node.

PARTNER LANE MATRIX

P = Primary lane. S = Supporting role. Use this matrix to assign workstream ownership and avoid duplication. Nodes with multiple primary lanes require a coordination lead.

Node	Tier	FVEY LE FOs	FVEY IC	OFAC / Treasury	Private Sector
OTC Crypto Brokers	CRITICAL	,	S	**P**	**P (Chainalysis/TRM)**
High-Risk Exchanges	CRITICAL	S	,	**P**	**P (blockchain forensics)**
Bulletproof Hosting	CRITICAL	S	**P**	,	**P (ISPs, registrars, CDNs)**
IAB Markets	HIGH	**P**	S	,	**P (Intel 471, Flashpoint)**
Botnet / Loaders	HIGH	**P**	**P**	,	**P (Microsoft, Mandiant)**
Leak-Site Hosting	HIGH	**P**	**P**	,	S (upstream hosting)
Underground Trust Infra	HIGH	**P**	S	,	**P (Intel 471, Flashpoint)**
Mixing / Obfuscation	HIGH	,	S	**P**	**P (Chainalysis/TRM)**
Mule / Money Laundering	HIGH	**P**	,	S	S
Credential / Stealer Mkts	MEDIUM	**P**	,	,	**P (takedown support)**
Crypter / Packer Services	MEDIUM	S	,	,	**P (AV/EDR vendors)**
Gray-Market VPS	MEDIUM	S	,	,	**P (abuse reporting)**
Domain / DNS Ecosystems	MEDIUM	S	,	,	**P (registrar engagement)**
Exfil Staging Infra	MEDIUM	**P**	S	,	S
Proxy / Anonymization	MEDIUM	S	**P**	,	S

Note on private sector integration: The private sector gap is most acute in three areas: (1) blockchain forensics firms feeding OFAC designations, (2) underground monitoring firms providing IAB and trust-node intelligence, and (3) upstream infrastructure providers taking voluntary abuse action. A structured referral-and-feedback loop is the missing piece, currently operating ad hoc.

TOP INVESTMENT PRIORITIES (GAP-WEIGHTED)

The following five investments produce the highest disruption-per-unit-of-effort based on current analytic coverage gaps. Drawn from structural ecosystem analysis and cross-referenced against the node map. See companion KPI Measurement Framework for full metric definitions.

1. Intermediary Cash-Out Mapping Program *(Nodes: Nodes 01, 02, 09)*

Convert laundering concepts into repeatable, case-linked cash-out graphs covering top 20 OTC/broker nodes, mule recruitment patterns, and 3 to 5 end-to-end case exemplars. Feeds OFAC designations and VASP engagement directly.

2. Underground Governance and Trust Node Mapping *(Nodes: Node 07)*

Identify top 10 escrow operators, forum administrators, and arbitrators. Dependency analysis showing how removal changes market behavior. Low-backfire-risk targets with high ecosystem impact.

3. Upstream Infrastructure Dependency Graph *(Nodes: Nodes 03, 12, 13)*

Move from BPH brand lists to provider-of-provider leverage: registrar, nameserver, ASN, CDN, and payment acceptance per major BPH operator. Minimum deliverable: per top reseller/BPH, registrar + nameserver + ASN + payment rails + redundancy assessment.

4. Measurement Layer Build-Out *(Nodes: All nodes)*

Implement KPI dashboard (monthly cadence) and pressure-effect ledger tied to every major action. Without this, effectiveness claims rest on narrative alone. Refer to the companion Ransomware Ecosystem Disruption Measurement Framework document for the full KPI set, confidence labeling system, and per-operation log template.

5. Identity and Continuity Package *(Nodes: Nodes 03, 04, 07)*

Cross-platform handle mapping, PGP reuse tracking, panel fingerprints, and brand-asset reuse patterns for top 10 groups. Makes actor rebranding expensive. Minimum deliverable: cross-platform handle map + PGP reuse database + brand-asset reuse patterns.

RECOMMENDED NEXT STEPS

This document is the analytical foundation. The logical next step is individual node playbooks for CRITICAL and HIGH priority nodes.

Recommended sequencing for node playbook development:

- **Phase A (CRITICAL nodes, build first): OTC Crypto Brokers, High-Risk Exchanges, Bulletproof Hosting. These three together cover the financial backbone and primary infrastructure layer. Node 16 (Exploit/Vulnerability Brokers) is assessed as a Phase A+ prerequisite per EDP Module 06: policy-track actions (CVD reform, bug bounty scaling, broker licensing) should be scoped concurrently with Phase A financial and infrastructure operations.**
- **Phase B (HIGH nodes, build in parallel): IAB Markets, Underground Trust Infrastructure, Mixing/Obfuscation. These are the operational engine and market-function nodes.**
- **Phase C (HIGH nodes, operational): Botnet/Loaders, Leak-Site Hosting, Mule Networks. Higher coordination complexity; benefits from Phase A/B groundwork.**
- **Phase D (MEDIUM nodes): Fold into relevant higher-tier node playbooks where dependencies exist; standalone playbooks only where partner ownership is clear.**

Each node playbook should include:

- Node description and ecosystem role
- Priority tier and substitutability assessment
- Partner lane assignments (primary and supporting)
- Action sequence (low to high backfire risk)
- Engagement triggers to avoid (cross-reference Playbook Section 8)
- KPIs and measurement approach
- Reconstitution monitoring protocol

Document maintenance: review and update quarterly, or following any major takedown, actor rebrand, or material change in VASP/infrastructure compliance posture.

Note: Nodes 01-11 are tracked in the companion KPI Measurement Framework and node playbooks (Phase A, B, C). Nodes 12-15 are mapped here for structural completeness and will be incorporated into meso-layer KPI tracking in a future framework update. Node 16 (Exploit/Vulnerability Brokers) was added per EDP Module 06 assessment as a CRITICAL-tier node; it is not yet assigned to a playbook phase and requires a dedicated policy-track action plan before full integration.