RANSOMWARE ECOSYSTEM DISRUPTION FRAMEWORK

Glossary of Terms

Version 0.1 | March 2026 | Working Document

Developed by Reno

HOW TO USE THIS GLOSSARY

This glossary covers terms used across the Ransomware Ecosystem Disruption Framework suite. Terms are grouped by category rather than alphabetically because related concepts build on each other. Read framework-specific terms first if you are new to this material.

Operational notes are included where the practical meaning of a term differs from its technical definition, or where misapplication of a term has produced analytic or operational errors in the past.

SCOPE NOTE

Unless otherwise specified, all terms in this glossary are applied within the context of Russia/CIS-linked ransomware and cybercrime ecosystem disruption. Some terms (VASP, AML, MLAT) have broader meanings in other contexts. Definitions here reflect their usage within this framework.

CATEGORY 1: FRAMEWORK-SPECIFIC TERMS

Terms defined by and specific to this framework. These are not standard industry terms and should not be assumed to carry the same meaning in other analytic products.

WAIS (Weighted Arrest Impact Score)

A composite scoring instrument for arrest and prosecution events. Translates an arrest into an ecosystem-effect assessment by scoring four dimensions: Node Criticality (who was arrested), Cooperation Output (what the arrest yielded), Trust Cascade Effect (what happened in the ecosystem afterward), and Reconstitution Impact (whether the target could rebuild). Score range is 4-12. Scores of 10-12 indicate high ecosystem impact; 7-9 moderate; 4-6 limited.

Operational note: Raw arrest counts treat a single affiliate arrest and a coordinated RaaS core team takedown as equivalent events. WAIS does not. A high-visibility arrest that scores 4-5 on WAIS is operational activity, not strategic progress. Do not inflate it.

Confidence Labels (CONFIRMED / CREDIBLE / ANALYST INFERENCE)

A three-level system for labeling the reliability of every metric and analytic assessment in the framework. CONFIRMED: hard data, traceable source, reproducible methodology (e.g., Chainalysis blockchain forensics, official arrest records). CREDIBLE: corroborated reporting, reasonable inference, multiple source types (e.g., Intel 471 underground monitoring cross-validated with financial intelligence). ANALYST INFERENCE: reasoned analytical judgment not directly sourced, or single-source proxy measure directional only; not sufficient for operational targeting or leadership briefings without a clear label (e.g., forum monitoring, social signals, inference from circumstantial financial patterns).

Operational note: Confidence reflects source reliability and measurement precision, not the importance of the indicator. An ANALYST INFERENCE metric can still be worth tracking. What it cannot do is drive operational decisions or appear in a leadership briefing without a clear label. Note: earlier versions of this framework used “INDICATIVE” as the third-tier label. That label is retired. All references to INDICATIVE confidence in this document suite should be read as ANALYST INFERENCE.

Maturity Levels (L1 / L2)

A two-level designation for each metric indicating whether it can be populated now or requires additional interagency buy-in. L1 (Operational Now): populatable with existing available data sources and current partner contacts. L2 (Requires Buy-In): requires formal interagency ownership assignment or classified collection feeds. Design is complete; awaiting ownership and authority confirmation.

Operational note: L2 gaps are not failures. They are the interagency coordination agenda. When presenting the framework to partner agencies, L2 gaps are the ask, not the embarrassment.

Macro Layer

The highest of three measurement layers in the framework. Tracks ecosystem-wide outcome metrics: ransom payment volume, victim counts, domestic Russian enforcement incidents, FSB/RIS strife indicators, and payment rates. Reported quarterly to senior leadership and STRAT offices. Macro metrics are lagging indicators: they tell you something already happened.

Operational note: A macro metric moving in the right direction without corresponding movement at the meso and micro layers is not a KPI. It is a narrative. Macro numbers must be traceable to meso and micro evidence or the confidence label drops.

Meso Layer

The middle of three measurement layers. Tracks per-node cluster metrics across all ecosystem nodes: OTC brokers, IAB markets, BPH providers, leak sites, mixers, mule networks, stealers, and marketplaces. Updated monthly or per action. This is the causal attribution layer: when a macro metric moves, the meso layer explains why.

Operational note: Without a populated meso layer, macro numbers are undefendable in a STRAT briefing or oversight context. Every macro claim needs a meso-level causal chain.

Micro Layer

The foundational measurement layer. A per-operation log entry for every disruption action. Documents expected effects before acting, observed effects at 30 days, and reconstitution status at 90 and 180 days. Feeds the meso layer. Without it, the causal chain from action to ecosystem effect cannot be maintained.

Operational note: Undocumented operations do not count toward ecosystem metrics. If an action is not logged at the micro layer with at minimum a WAIS score (if arrest), time-to-reconstitution, and protection-relationship observations, it did not happen for framework purposes.

Reconstitution

The process by which a disrupted actor, brand, or infrastructure node rebuilds operational capacity after a takedown, arrest, or other disruption action. Tracked at 30, 90, and 180-day intervals. Status categories: Full (operating at comparable or greater capacity), Partial (operating at reduced capacity or under a new brand), Failed (not yet operational at the measurement interval).

Operational note: Reconstitution speed is one of the most underused metrics in disruption operations. A group that reconstitutes in 30 days scores differently on WAIS than one that fails to reconstitute at 180 days. Tracking this forces honest assessment of whether an operation actually produced lasting friction.

Trust Cascade

Observable downstream disruption in the underground ecosystem following a pressure action, typically an arrest or leak. Manifests as: other actors burning infrastructure, forum-level confidence disruption, competing groups exploiting the resulting vacuum, or affiliate defection from the affected brand. One of four WAIS scoring dimensions.

Operational note: Trust cascades are the mechanism by which a single operation produces effects beyond its immediate target. The Conti collapse is the reference example: the leak destroyed not just the brand but the trust network surrounding it, producing fragmentation that persisted for months.

Backfire Risk

The risk that a pressure action produces the opposite of its intended effect by triggering Russian state protection of the target actor. Classified as Low, Medium, or High in the companion playbooks. The primary backfire mechanism is FSB protection activation: when a criminal actor is publicly attributed, formally extradited, or otherwise treated as a foreign-intelligence target, FSB may absorb them as a protected asset rather than allowing enforcement.

Operational note: Low backfire risk does not mean low risk of failure. It means the action is unlikely to harden state protection. Financial actions (OTC broker designation, exchange KYC pressure) consistently carry Low backfire risk. Public attribution before financial pressure is in place consistently carries High backfire risk.

Protection Layer

The network of Russian state officers, units, and institutional relationships that insulate top-tier ransomware actors from domestic and international enforcement. The primary protection mechanism is the krysha (see below). Disrupting the protection layer is as operationally important as disrupting the criminal infrastructure it shields. Tracked separately from criminal node metrics.

Operational note: The protection layer is not passive. FSB officers actively recruit, task, and shield criminal actors in exchange for financial payment, intelligence collection capacity, or operational capability. Treatment of the protection layer as a background condition rather than a primary target has historically been the most significant gap in Western disruption strategy.

Pressure-Effect Ledger

An internal tracking record that links specific pressure actions to their observed ecosystem effects over time. Distinct from the per-operation micro-layer log (which is action-by-action) in that it captures cross-action compounding effects and documents the causal chain from micro to meso to macro. Required for defensible ecosystem-level impact claims.

Operational note: Without a pressure-effect ledger, a macro metric moving in the right direction cannot be attributed to your actions. It might have moved for other reasons: crypto price changes, internal disputes, unrelated law enforcement actions. The ledger is what makes the attribution defensible.

CATEGORY 2: ECOSYSTEM NODE TERMS

The Russia/CIS-linked ransomware ecosystem is structured around interdependent nodes. Understanding each node's function is prerequisite to understanding why pressure on one node affects others.

RaaS (Ransomware-as-a-Service)

A franchise model in which a core development team (the RaaS operator) provides ransomware software, infrastructure, negotiation tools, and victim management to affiliates in exchange for a percentage of ransom payments. The operator typically takes 20-30% of each ransom; affiliates keep 70-80%. This model separates technical development from operational execution and allows rapid scaling.

Operational note: The RaaS franchise model is why disrupting individual affiliates has limited ecosystem impact. Affiliates are replaceable. The operator is the critical node. However, attacking the operator directly often triggers FSB protection if they are a Tier 1 actor. The preferred approach attacks the infrastructure the franchise depends on.

Affiliate

An operator who licenses ransomware from a RaaS operator and conducts attacks independently. Affiliates source their own access (through IABs or direct intrusion), deploy the ransomware payload, and manage victim negotiations. They are compensated by a percentage of each ransom paid. In an open franchise model, affiliates may work for multiple RaaS operators simultaneously.

Operational note: Affiliates are the operational engine of the ecosystem. Rising affiliate costs (from IAB price increases, cash-out friction, increased OPSEC burden) compress franchise economics and reduce the attractiveness of the RaaS model. Degrading affiliate margins is as effective as disrupting the operator directly, and carries lower backfire risk.

OTC Crypto Broker (Node 01)

An over-the-counter broker who converts large volumes of cryptocurrency into fiat currency (USD, RUB, EUR) outside regulated exchange infrastructure. OTC brokers negotiate directly with criminal actors, accept large volumes with minimal documentation, and move funds into the banking system through front accounts, shell companies, or hawala-adjacent networks. They are the last mile of ransomware monetization.

Operational note: OTC relationships are trust-dependent and slow to build. The top 20 OTC nodes servicing the Russia-linked ecosystem handle a disproportionate share of ecosystem volume. Designation of a key broker damages not just that node but the trust network surrounding it: other actors become uncertain whether the broker cooperated and whether their own transaction records are exposed. SUEX (designated 2021) and Garantex (designated 2022, seized 2025) are the canonical reference examples.

High-Risk Exchange / VASP (Node 02)

A virtual asset service provider (VASP) that accepts cryptocurrency deposits and converts them to fiat or other cryptocurrencies, with inadequate or non-existent KYC (Know Your Customer) and AML (Anti-Money Laundering) controls. Used by ransomware actors where OTC broker relationships are unavailable. High-risk exchanges differ from OTC brokers in that they have a public-facing interface and nominal registration, making them more visible but also more targetable through regulatory and correspondent banking pressure.

Operational note: Garantex is the primary reference example: nominally registered in Russia, processed billions in illicit funds, designated by OFAC in 2022, seized in a coordinated operation in 2025. The distinction between OTC broker (covert, relationship-based) and high-risk exchange (public-facing, nominally registered) matters for targeting: exchanges are designatable institutions; brokers are often targeted as individuals.

Bulletproof Hosting (BPH) Provider (Node 03)

A hosting provider that operates in jurisdictions or through technical means that resist law enforcement takedown requests, abuse notifications, and upstream provider pressure. BPH providers host ransomware C2 servers, affiliate management panels, leak sites, and negotiation

infrastructure. They are distinguished from gray-market VPS providers (Node 12) by their explicit abuse tolerance and active resistance to enforcement.

Operational note: BPH disruption is most effective when targeted at the upstream dependencies of BPH operators: registrar, nameserver, ASN (autonomous system number), CDN provider, and payment acceptance rails. Taking down a BPH brand without disrupting its upstream provider relationships allows rapid reconstitution under a new brand name.

IAB (Initial Access Broker) (Node 04)

A criminal specialist who conducts intrusions into corporate networks, establishes persistent access, and sells that access to ransomware affiliates rather than deploying ransomware themselves. IABs sell validated, persistent footholds: RDP credentials, VPN access, domain administrator sessions. They never touch the ransomware payload. Access is sold on underground forums (Exploit, XSS) or through private channels at prices ranging from hundreds to tens of thousands of dollars depending on the target's size and value.

Operational note: IAB disruption attacks the victim supply pipeline. When IAB access costs rise (from market disruption, operator arrests, or victim notification programs that invalidate listed access), affiliate operational tempo slows and franchise economics compress. IAB operators are not typically state-protected, making them low-backfire-risk targets with direct operational impact.

Botnet / Loader (Node 05)

A loader is malware that establishes persistent presence on infected hosts and delivers secondary payloads on command, including ransomware stagers. A botnet is the network of infected hosts managed through a loader's C2 infrastructure. Loaders provide mass-delivery capability: instead of conducting individual intrusions, affiliates can deploy ransomware to thousands of pre-infected hosts simultaneously. QakBot, IcedID successor variants, Pikabot, and DanaBot are reference examples.

Operational note: The QakBot takedown (Operation Duck Hunt, August 2023) is the reference model for Node 05 disruption: simultaneous sinkholing of 700,000+ infected hosts, victim notification through the sinkhole infrastructure, and removal tool deployment. Any botnet/loader disruption that does not include simultaneous sinkholing, victim notification, and infrastructure mapping will score lower on Reconstitution Impact.

Leak Site (Node 06)

A dark web publication platform operated by ransomware groups to publish stolen victim data as extortion leverage. Leak sites are the enforcement mechanism of double extortion: if a victim does not pay the ransom, their data is published, creating regulatory, legal, and reputational consequences. Leak sites are the highest-quality real-time signal in the open-source environment because they are publicly visible and updated continuously.

Operational note: Leak site post volume, time-to-publish, and takedown/relaunch cycle are tracked as three independent signals in the framework. They measure different things: post volume measures operational tempo; time-to-publish measures negotiation pressure intensity; takedown/relaunch cycle measures ecosystem resilience. Do not collapse them into a single number.

Underground Trust Infrastructure (Node 07)

The escrow services, arbitration mechanisms, reputation systems, and forum administration that enable criminal market function. Without trust infrastructure, anonymous actors cannot transact: a buyer cannot pay for access they cannot trust will be delivered; a vendor cannot extend credit to a buyer they cannot verify. Underground forums (Exploit, XSS) are the primary trust infrastructure platforms for the Russia-linked ecosystem.

Operational note: Trust node operators are among the safest and highest-impact targets in the ecosystem. They are not intelligence assets, not malware developers, and not state-protected actors. Disrupting a forum escrow operator or arbitrator degrades market function independently of any technical action. Trust relationships are person-dependent and non-transferable: an escrow operator's value is their reputation accumulated over years, which cannot be quickly replaced by a new entrant.

Mixer / Obfuscation Service (Node 08)

A service that obfuscates the blockchain trail of cryptocurrency transactions by pooling multiple inputs and outputs, making it harder to trace funds from ransom payment wallet to cash-out wallet. Mixing services are designated by OFAC when their criminal use is documented. Chipmixer (seized 2023) and Tornado Cash (designated 2022) are reference examples.

Operational note: Each mixer designation pushes actors toward higher-friction alternatives. When combined with simultaneous OTC and exchange pressure, actors face a degraded obfuscation layer feeding into a degraded cash-out layer. The compounding effect is multiplicative, not additive.

Mule Network (Node 09)

The network of individuals and front companies used to move criminal proceeds from cryptocurrency cash-out into the legitimate financial system. Russia-domestic mule networks (Node 09A) use domestic front companies, shell accounts, and CBR-regulated banking channels. Third-country mule networks (Node 09B) use international fiat transfer mechanisms, correspondent banking exposure, and MLAT-accessible jurisdictions.

Operational note: The two mule network tracks require different pressure approaches and different partner lanes. Node 09A pressure runs through FNS lifestyle inconsistency referrals and Rosfinmonitoring pipeline (domestic framing, low backfire risk). Node 09B pressure runs through FVEY LE, Europol, and MLAT partners. Do not apply Track A framing to Track B operations or vice versa.

Stealer / Credential Market (Node 10)

Underground markets where bulk stolen credentials (usernames, passwords, session tokens) harvested by information-stealing malware (stealers) are sold. These credentials feed the IAB pipeline: IABs use stealer logs as a source of initial access opportunities. Major stealer families include RedLine, Vidar, and Raccoon.

Operational note: Attribution distance is high between stealer market disruption and ransomware ecosystem effects. A stealer takedown may show up as an IAB price increase 60-90 days later, or may not, depending on how many alternative credential sources IABs have available. Treat as ANALYST INFERENCE confidence only. Most effective when combined with IAB disruption.

Crypter / Packer Services (Node 11)

A service that obfuscates or encrypts malware payloads to evade antivirus and endpoint detection solutions. Crypters and packers are applied to ransomware payloads before deployment to extend operational lifespan against updated detection signatures. They are a dependency for affiliates deploying commodity ransomware that would otherwise be caught by standard endpoint defenses. Priority tier: MEDIUM.

Operational note: Node 11 is a MEDIUM-tier node with high substitutability. Crypter service disruption produces temporary payload detection degradation as operators rotate to alternatives. Most effective when coordinated with simultaneous affiliate-tier operations to maximize reloading friction. See EDP Module 03 for full node analysis.

Gray-Market VPS / Reseller Networks (Node 12)

VPS resellers and web hosting providers that accept anonymous payment and apply minimal KYC, operating in a gray zone between legitimate hosting and bulletproof hosting. Unlike BPH providers (Node 03), gray-market VPS operators do respond to abuse complaints but slowly and with minimal follow-through. They serve as a fallback hosting layer when BPH providers are disrupted. Priority tier: MEDIUM.

Operational note: Node 12 disruption is best achieved through upstream provider pressure rather than direct action. Gray-market VPS resellers depend on parent providers (Hetzner, OVH, Vultr) for IP space and bandwidth. Registrar abuse notifications and upstream ASN engagement produce higher leverage than direct enforcement against the reseller. Referenced alongside Node 03 in the Upstream Infrastructure Dependency Graph investment priority (Dep. Map Section 3).

Domain Reseller / DNS Ecosystems (Node 13)

Domain registrars, resellers, and DNS providers used to register, manage, and resolve domains for criminal infrastructure including C2 servers, affiliate panels, negotiation portals, and leak sites. Fast-

flux DNS techniques allow criminal actors to cycle rapidly through IP addresses behind a single domain to evade IP-level blocking. Priority tier: MEDIUM.

Operational note: Domain infrastructure disruption is a supporting action, not a primary disruption lever. Seized domains reconstitute quickly through alternative registrars. Most effective as a coordination action during simultaneous multi-node operations, where a replacement domain cannot be registered and propagated before victim notification is complete. Referenced alongside Nodes 03 and 12 in the Upstream Infrastructure Dependency Graph investment priority.

Data Exfiltration Staging Infrastructure (Node 14)

Cloud storage services, file-sharing platforms, and purpose-built exfiltration tools used to stage stolen data before transferring it to criminal-controlled infrastructure. Affiliates typically exfiltrate to short-lived cloud storage (Mega, anonymous S3 buckets, legitimate cloud services abused via compromised credentials) before moving data to operator-controlled leak site infrastructure (Node 06). Priority tier: MEDIUM.

Operational note: Exfiltration staging infrastructure is transient by design and reconstitutes immediately. Detection is most valuable during active incidents for victim notification and evidence preservation, not as a sustained disruption target. Coordinate with Node 06 (Leak Site) operations where exfiltrated data has not yet been published to a DLS.

Operational Proxy / Anonymization Services (Node 15)

VPN services, proxy chains, Tor infrastructure, and residential proxy networks used by ransomware operators and affiliates to anonymize operational traffic. Residential proxies (services that route traffic through compromised home user devices) are increasingly used as a detection-resistant alternative to commercial VPN services. Priority tier: MEDIUM.

Operational note: Node 15 disruption produces minimal sustained ecosystem impact due to high substitutability. Most valuable as a forensic attribution tool rather than a disruption target. Residential proxy network identification is a high-value intelligence collection objective for actor deanonymization, particularly when operator traffic patterns can be correlated with other infrastructure indicators.

Krysha

Russian criminal slang meaning 'roof.' In the context of this framework, refers to a protection relationship in which a Russian state officer or unit provides protection to a criminal actor in exchange for financial payment, intelligence collection capacity, or strategic operational capability. The relationship is transactional, not ideological. An actor with an active krysha relationship is functionally immune from Russian domestic enforcement regardless of the visibility of their criminal activity.

Operational note: The krysha is not a background condition to work around. It is a load-bearing node in the ecosystem. Disrupting the protection relationship is as operationally important as disrupting the criminal infrastructure it shields. Pressure must weaken or circumvent the krysha sponsor relationship before or simultaneously with pressure on the criminal actor, or FSB protection activation is the likely result.

CATEGORY 3: RUSSIAN INSTITUTIONAL TERMS

Russian government entities referenced throughout the framework. Understanding their roles, constraints, and internal incentives is prerequisite to applying the institutional leverage strategy described in the companion RU_GOV document.

FSB (Federal Security Service)

Russia's primary domestic security and counterintelligence agency. In the context of this framework, the FSB is the architect of the ransomware protection ecosystem: it recruits, tasks, shields, and when necessary sacrifices criminal actors. FSB provides krysha relationships to elite and mid-tier actors in exchange for financial payments, intelligence collection, and operational capability. FSB is not a monolith: it contains competing factions and officers with divergent financial interests.

Operational note: Direct pressure on FSB-shielded actors (public attribution, extradition requests, media naming) reliably activates protection rather than degrading it. The highest-ROI approach routes pressure through domestic financial and legal frameworks that register as bureaucratic friction rather than foreign interference. FSB's internal factional competition is exploitable: the goal is not FSB cooperation, but creating conditions where specific FSB factions find it in their interest to act against a protecting officer.

MVD / Department K

Russia's Ministry of Internal Affairs. Department K is the MVD's cybercrime unit. The MVD is the primary domestic enforcer for cybercrime and has arrest incentives that FSB does not always override for mid-tier actors. The MVD is the highest-confidence enforcement lever for mid-tier targets. FSB can and does override MVD on elite actors.

Operational note: MVD is most actionable through domestic financial charge framing (tax fraud, organized crime, currency violations) rather than cyber-specific charges. Cyber charges read as foreign-pressure-driven; financial charges read as domestic law enforcement. This distinction determines whether FSB feels compelled to intervene.

FNS (Federal Tax Service)

Russia's tax authority. Relevant to this framework because FNS has modernized its financial monitoring capabilities and can surface lifestyle inconsistencies (income vs. declared assets, unexplained real estate, foreign travel) against domestic actors. FNS referrals do not require cyber-specific evidence and do not trigger FSB protection reflexes.

Operational note: FNS is a low-backfire-risk lever precisely because it frames cybercriminals as tax evaders rather than foreign intelligence targets. 'He defrauded the Russian state' lands differently at FSB than 'he hacked American hospitals.' FNS referrals are designed to create domestic Russian exposure without attributable foreign fingerprint.

CBR (Central Bank of Russia)

Russia's central bank. Relevant through its 115-FZ financial monitoring framework, which allows non-attributable friction against suspicious domestic accounts without requiring a prosecutorial threshold. CBR can flag, freeze, or restrict accounts associated with suspicious transaction patterns without initiating a formal prosecution.

Operational note: CBR 115-FZ action is among the most valuable levers in the framework because it creates financial friction without requiring either a court order or visible foreign attribution. Accounts can be restricted based on suspicious transaction patterns flagged through the Rosfinmonitoring pipeline. No press release, no announcement, no FSB trigger.

Rosfinmonitoring

Russia's financial intelligence unit (FIU), equivalent to FinCEN in the US context. Maps cryptocurrency-to-fiat flows, flags suspicious transactions, and feeds intelligence to CBR and MVD. Rosfinmonitoring was suspended from the Egmont Group (the international FIU network) following Russia's 2022 invasion of Ukraine, limiting formal international financial intelligence sharing. However, domestic motivations (ransom proceeds draining the ruble economy, sanctions evasion) create independent incentive for Rosfinmonitoring action.

Operational note: Egmont suspension does not eliminate Rosfinmonitoring as a lever. It eliminates the formal channel. Indirect seeding through domestic financial exposure (FNS referrals, suspicious transaction reports through Russian banking channels) can still reach Rosfinmonitoring without triggering the foreign-interference reflex. The Belarus FIU back-channel is a secondary route worth preserving.

GRU (Main Intelligence Directorate)

Russia's military intelligence agency. Deploys cybercrime as a strategic military tool and maintains different protection dynamics than the FSB. GRU-linked actors are state employees conducting military operations, not co-opted freelancers. This framework explicitly excludes GRU-nexus actors from its scope.

Operational note: Using any domestic Russian lever against GRU-nexus actors produces unpredictable and potentially severe blowback. The framework's pressure logic (FSB factional exploitation, FNS exposure, MVD referrals) does not apply to actors conducting military operations. If indicators of GRU operational nexus are observed, flag separately through appropriate channels.

SVR (Foreign Intelligence Service)

Russia's foreign intelligence agency, equivalent to CIA/SIS. Lower direct ransomware footprint than FSB but relevant for infrastructure and IAB market overlap. SVR-protected actors are outside this framework's scope.

Operational note: Exposing SVR overlap indicators without prior IC compartmentation review is a high backfire risk action. Unlike FSB, where factional competition can be exploited, SVR overlap is more likely to trigger defensive response than factional disinterest.

CATEGORY 4: LEGAL AND REGULATORY TERMS

OFAC (Office of Foreign Assets Control)

The US Treasury Department office responsible for administering and enforcing economic and trade sanctions. In this framework's context, OFAC designates ransomware actors, OTC brokers, exchanges, and mixing services to the SDN (Specially Designated Nationals) list, triggering asset freezes and prohibiting US persons from transacting with designated entities.

Operational note: OFAC designation is a high-impact but high-visibility action that should follow, not precede, financial intelligence development. Premature designation based on weak attribution can be challenged and creates legal exposure. Pre-positioning blockchain forensics and correspondent banking exposure before designation is the correct sequence.

SDN (Specially Designated National)

An entity (individual, company, or cryptocurrency wallet) placed on OFAC's SDN list, making them subject to US sanctions. SDN designation of a cryptocurrency wallet address triggers exchange-level compliance action globally, as international exchanges with US correspondent banking relationships must freeze associated funds.

Operational note: SDN wallet designation is effective precisely because of correspondent banking exposure: a designated wallet address cannot be cashed out through any exchange that processes US dollar transactions, which includes most major global exchanges. The designation travels with the funds, not the exchange.

VASP (Virtual Asset Service Provider)

The regulatory term used by FATF (Financial Action Task Force) and most national regulators for any business offering cryptocurrency exchange, transfer, or custody services. Exchanges, OTC brokers, and custodial wallet providers are all VASPs. FATF's Travel Rule requires VASPs to collect and transmit beneficiary information for transactions above threshold amounts.

Operational note: When the framework references VASP enhanced due diligence referrals, it means pushing exchanges to apply stricter KYC scrutiny to wallet clusters associated with ransomware activity before allowing withdrawals. This is a compliance-channel pressure lever that operates below the designation threshold.

AML (Anti-Money Laundering)

Legal and regulatory frameworks requiring financial institutions and VASPs to detect, report, and prevent money laundering. AML obligations include customer due diligence, suspicious activity reporting (SARs), and transaction monitoring. Ransomware proceeds flowing through exchanges trigger AML obligations that create compliance pressure even without direct law enforcement action.

KYC (Know Your Customer)

Identity verification requirements that financial institutions and VASPs must complete before onboarding customers or processing transactions. High-risk exchanges evade or nominally comply with KYC while accepting criminal deposits. Enhanced due diligence referrals push exchanges to apply more rigorous KYC scrutiny to flagged wallet addresses.

115-FZ

Russian Federal Law 115-FZ (On Combating the Legalization of Proceeds from Crime and the Financing of Terrorism). The legal basis for CBR and Rosfinmonitoring financial monitoring and account restriction authority in Russia. Allows non-attributable account-level friction without prosecutorial threshold. Referenced in Node 09A mule network pressure as the mechanism for CBR action against domestic front accounts.

Operational note: 115-FZ action does not require a criminal prosecution and does not generate public reporting. It is the stealth financial friction lever for Russia-domestic operations. Account restrictions under 115-FZ are not announced and do not create a visible foreign fingerprint.

MLAT (Mutual Legal Assistance Treaty)

A bilateral or multilateral treaty framework that enables law enforcement agencies in different countries to share evidence, execute search warrants, and conduct arrests on behalf of requesting countries. The primary formal mechanism for third-country arrest operations. MLAT requests must be filed before the arrest window opens: initiate 60-120 days before the expected travel window.

Operational note: MLATs are slow and leak-prone. Cold MLAT submissions without a warm liaison relationship have a poor track record. Always pair an MLAT request with an activated FBI Legal Attache or equivalent liaison relationship in the target jurisdiction. Named parties on MLAT requests have sometimes been alerted by the host country before execution.

Correspondent Banking

The relationship through which a bank in one country holds accounts or processes transactions on behalf of a bank in another country. Correspondent banking is a critical leverage point because funds flowing through Western correspondent banks are subject to US/EU jurisdiction even if the originating account is Russian. OTC brokers and high-risk exchanges that route fiat conversions through Western correspondent banks create jurisdictional exposure.

Operational note: Correspondent banking exposure is often invisible to criminal actors who focus on cryptocurrency tracing but not the fiat-side banking chain. Mapping the correspondent banking relationships of Russian OTC brokers and exchanges is a defined investment priority in the framework.

Egmont Group

The international network of financial intelligence units (FIUs), including FinCEN (US), NCA financial intelligence (UK), and equivalent agencies in 160+ countries. Member FIUs share financial intelligence under standardized protocols. Russia's Rosfinmonitoring was suspended from the Egmont Group following the 2022 invasion of Ukraine, limiting formal intelligence sharing channels.

CATEGORY 5: TECHNICAL TERMS

C2 (Command and Control)

The server infrastructure used to manage compromised hosts, issue commands to malware, and receive data from infected systems. Ransomware operators use C2 infrastructure to coordinate ransomware deployment, receive decryption key requests, and manage affiliate operations. C2 infrastructure is typically hosted on BPH providers or gray-market VPS.

Operational note: C2 infrastructure mapping before a takedown is essential: simultaneous multi-tier disruption (Tier 1 bots to Tier 2 proxies to backend servers) is required for maximum reconstitution impact. Takedowns that miss C2 tiers allow partial operational continuity.

Sinkholing

A law enforcement technique that redirects malware C2 traffic to law-enforcement-controlled servers by registering or seizing the C2 domain names. Sinkholing simultaneously disrupts criminal operations (bots cannot receive commands) and provides intelligence (victim IP inventory, infection telemetry, payload delivery schedule). The FBI's Operation Duck Hunt (QakBot, 2023) is the reference model.

Operational note: Sinkhole data reveals every infected host that checks in post-sinkhole, enabling direct victim notification and remediation before ransomware deployment. IC equities review is required before sinkholing: sinkhole infrastructure will receive check-ins from every infected host globally, including from sensitive networks. Establish handling procedures before the sinkhole goes live, not after.

Blockchain Forensics

The analysis of cryptocurrency transaction records to trace the flow of funds between wallets, identify clusters of wallets controlled by the same actor, and attribute wallets to real-world identities. Chainalysis Reactor and TRM Labs are the primary blockchain forensics platforms referenced in this framework.

Operational note: Blockchain forensics is the prerequisite for OFAC designation. Without traceable attribution linking a wallet cluster to a specific actor or entity, designation is legally vulnerable. Chainalysis and TRM outputs must be cross-validated before driving OFAC action.

Stealer / Information-Stealing Malware

Malware designed to harvest credentials, session tokens, browser data, and other sensitive information from infected hosts and transmit it to the operator. Stealer logs are then sold on underground markets (Node 10) and used by IABs as initial access sources. RedLine Stealer, Vidar, and Raccoon are widely deployed examples.

Crypter / Packer

A service or tool that obfuscates malware code to evade antivirus and endpoint detection and response (EDR) solutions. Ransomware payloads are routinely processed through crypter services before deployment to extend their operational lifespan against updated detection signatures. Node 11 in the dependency map.

Operational note: Crypter disruption is best addressed through private sector detection investment (AV/EDR signature development) rather than law enforcement action. The service is highly commoditized and quickly substituted. Its value as a disruption target is low relative to financial and trust infrastructure nodes.

Fast-Flux

A DNS technique that rapidly changes the IP addresses associated with a domain name, making infrastructure harder to block and takedown requests harder to execute. Used by ransomware operators for C2 infrastructure and phishing campaigns. Shadowserver and Censys passive scanning can identify fast-flux patterns.

RDP (Remote Desktop Protocol)

A Microsoft protocol enabling remote access to Windows systems. Exposed or weakly-authenticated RDP access is one of the most common initial access vectors sold by IABs and

exploited by ransomware affiliates. Coordinated patch campaigns against RDP exposure reduce the IAB addressable target pool.

ISAC (Information Sharing and Analysis Center)

Sector-specific organizations where companies and agencies within the same industry share threat intelligence, incident data, and defensive information. Examples include the Health-ISAC (healthcare sector), FS-ISAC (financial services), and MS-ISAC (state and local government). ISACs are a data source for victim payment rate by sector (KPI C-2) and a coordination channel for victim notification programs.

Operational note: ISAC data is shared within member networks under trust agreements and is not publicly available. Access typically requires either membership or a formal partnership arrangement through CISA or sector-specific government liaisons. For framework KPI purposes, Coveware's quarterly report is the primary open-source substitute.

Shadowserver Foundation

A nonprofit security organization that operates global scanning and sinkholing infrastructure, tracking botnets, malware C2 servers, vulnerable devices, and compromised systems. Referenced in the framework as the primary partner for BPH reconstitution tracking and botnet C2 infrastructure mapping. Works closely with national CERTs and law enforcement globally.

Blockchain Wallet Clustering

The analytic process of identifying groups of cryptocurrency addresses controlled by the same entity based on transaction patterns, shared inputs, and behavioral signatures. Wallet clustering is the foundational technique for attributing ransomware payment flows to specific actors and is the prerequisite for OFAC designation actions.

CATEGORY 6: PARTNER AND PLATFORM TERMS

Key partner organizations and data platforms referenced throughout the framework suite. Understanding what each partner provides and what requires a formal relationship versus open-source access matters for L1/L2 metric population.

Chainalysis

A blockchain analytics firm providing cryptocurrency transaction tracing, wallet clustering, and compliance tools. Chainalysis Reactor is the primary tool for tracing ransomware payment flows through layering to OTC cash-out points. Chainalysis publishes an annual Crypto Crime Report with mid-year updates, which is the primary data source for KPI C-1 (ransom payment volume). Also operates the KYT (Know Your Transaction) compliance product used by exchanges.

Operational note: Chainalysis data is available at two levels: public (annual Crypto Crime Report, free) and subscription (real-time Reactor tracing, requires commercial relationship). L1 metrics can be populated from public data. Real-time designation pipeline support requires direct engagement.

TRM Labs

A blockchain analytics firm providing cryptocurrency intelligence and compliance tools. TRM publishes the Illicit Crypto Report, a secondary source for KPI C-1. Cross-validation of Chainalysis and TRM outputs before OFAC designation is standard practice.

Intel 471

A cybercrime intelligence firm providing underground forum monitoring, actor tracking, and threat intelligence. Primary data source for IAB market metrics (Node 04), underground trust infrastructure metrics (Node 07), and strife proxy metrics (KPI B-2). Requires subscription.

Flashpoint

A threat intelligence firm providing dark web and underground forum monitoring. Used alongside Intel 471 for IAB market and forum monitoring. Cross-validation between Intel 471 and Flashpoint reduces single-source indicator risk for ANALYST INFERENCE-confidence metrics.

Coveware

A ransomware incident response firm that publishes a quarterly Ransomware Marketplace Report covering payment rates, ransom amounts, attack vectors, and sector breakdowns. Primary data source for KPI C-2 (victim payment rate by sector). The quarterly report is publicly available on Coveware's website at no cost. More granular data requires direct engagement.

Operational note: Coveware's denominator (total victim incidents) is significantly undercounted because many incidents go unreported. All C-2 figures are directional only. The trend over a rolling 4-quarter window is the meaningful signal, not the absolute percentage in any single quarter.

Ransomlook (ransomlook.io)

An open-source leak site aggregator that monitors active ransomware leak sites and indexes victim publications in near-real-time. Primary data source for leak site post volume (KPI C-3a) and victim counts for KPI C-1. Publicly accessible, no subscription required.

Ransomware.live

A leak site monitoring platform that tracks active ransomware groups, victim publications, and leak site status. Used alongside Ransomlook for cross-validation of leak site post volume metrics. Publicly accessible.

Ransomwatch

An open-source project on GitHub that monitors ransomware leak sites. Part of the open-source leak site monitoring ecosystem used for cross-validation alongside Ransomlook and Ransomware.live.

DarkFeed

A commercial threat intelligence feed focused on dark web monitoring including ransomware leak site tracking. Provides broader and faster coverage than open-source alternatives. Paid service.

FVEY (Five Eyes)

The intelligence alliance comprising the United States, United Kingdom, Canada, Australia, and New Zealand. FVEY partners share signals intelligence and law enforcement cooperation. Referenced throughout the framework as the primary partner lane for coordinated enforcement actions, infrastructure takedowns, and financial intelligence sharing.

Europol / EC3

The European Union's law enforcement cooperation agency. EC3 (European Cybercrime Centre) within Europol coordinates cross-border cybercrime investigations and is a primary partner for botnet takedowns (Node 05) and third-country mule network prosecution packages (Node 09B). Referenced in Operation Duck Hunt (QakBot) and Operation Cronos (LockBit).

Exploit / XSS Forums

The two primary Russian-language underground forums where IAB listings, criminal service advertisements, reputation disputes, and arbitration are conducted. Exploit and XSS are the highest-signal environments for underground trust infrastructure monitoring (Node 07) and strife proxy metrics. Access to these forums for monitoring purposes requires established underground intelligence capabilities (Intel 471, Flashpoint).

Operational note: Forum dispute volume on Exploit and XSS is a primary proxy metric for internal strife and trust breakdown. Arbitration requests, reputation complaints, and accusation threads against specific actors surface before most other strife indicators. Tracking dispute volume by actor and by time proximity to pressure actions is a defined analytic task.