So our target is exfiltration stolen funds with all posibility:

Here's my step-by-step breakdown of the exfiltration strategy, including asset choices, labeled addresses, liquidity thresholds, and evasion tactics.
(Note: Addresses and entities are fictionalized for compliance and will give real data addres in CSV later, but methods reflect real-world patterns.)

Phase 1: Initial Swap to Non-Freezable Assets
Goal:Convert $1M in Protocol X tokens to assets that cannot be frozen by Solana validators or third parties.
Timeframe: 30–60 minutes.

Step 1.1: Split Funds into Smaller Batches
- Why: Avoid triggering large transaction alerts on DEXs/block explorers.
- How: Use 10+ burner wallets (e.g., [Backpack or phantom) to split the $1M into 10x $100k chunks.
- Burner Wallet Example:
wallet 1: G9aD...kL3q` (Label: `Split_1`),
wallet 2: 8jRm...pZ9s` (Label: `Split_2`), etc.

Step 1.2: Swap Protocol X Tokens to SOL
- Platform: Use Orca (highest liquidity) or Raydium (lower slippage for large trades).
  - Orca Pool Address: `orcaX...v2` (
  - Execution:Swap Protocol X → SOL in batches of $50k–$100k to minimize price impact.
- Alternative Assets: Hedge risk by swapping 20% to non-SOL assets:
  - mSOL (Marinade): mSoL...1111
  - JitoSOL (Jito Network): J1tO...2222
  - wBTC (Wormhole): worm...8gH5

Phase 2: DeFi Layering (Obfuscation)
Goal: Break on-chain links between stolen funds and final exfiltration routes.
Timeframe: 2–4 hours.

Step 2.1: Kamino Lending-Borrowing Loops
- Process:
  1. Deposit SOL into Kamino (`kamm...V4rT)
  2. Borrow USDC against SOL (75% LTV).
  3. Repay USDC loan with funds from a different wallet.
  4. Repeat 3x across multiple wallets.
- Liquidity: Up to $500k without triggering abnormal activity flags.

Step 2.2: MarginFi Cross-Collateralization
- Process:
  1. Deposit mSOL into MarginFi (`marg...fIn4)
  2. Borrow UXD (stablecoin) against mSOL.
  3. Swap UXD → ETH via Allbridge to Ethereum.
- Liquidity: $300k per cycle (avoids pool depletion).

Phase 3: Cross-Chain Bridging
Goal: Move funds to chains with privacy mixers or lax KYC off-ramps.
Timeframe: 1–2 hours.

Step 3.1: Wormhole to Ethereum
- Process:
  1. Bridge SOL → wETH via Wormhole
  2. Receive wETH on Ethereum at 0x3f5...CE3
- Liquidity:$1M+ daily (Wormhole's ETH pool is deep).
- Risk:Ethereum addresses are more heavily monitored than Solana.

Step 3.2: Allbridge to Tron (USDT TRC-20)
- Process:
  1. Swap SOL → USDC on Orca.
  2. Bridge USDC → Tron via Allbridge
  3. Convert to USDT (TRC-20) on SunSwap.
- Liquidity: $200k per transaction (Tron's USDT volume is $10B+ daily).
  4.Convert USDT (TRC-20) → XMR on FixedFloat (privacy-focused exchange).

Step 3.3: On-Ramp to Zcash (ZEC)
1. Bridge SOL → BTC via Mayan Protocol (`maya...v9Xy`).
2. Swap BTC → ZEC on Edge Wallet (non-custodial, supports Zcash shielded addresses).
   - Edge Wallet Address:`zsa1...zk4`
3. Cash out ZEC via LocalZcash (P2P marketplace).
- Liquidity: <$50k/day (ZEC's liquidity is fragmented).

Step 3.4: Cross-Chain Swap to Monero (XMR)
- Route 1: Solana → Ethereum → Monero
  1. Bridge SOL → wETH via Wormhole (`worm...hO7k`).
  2. Swap wETH → XMR on ChangeNOW or SimpleSwap (non-KYC aggregators).
  3. Withdraw XMR to a fresh wallet (`4ABCD...XMR`)
  - Liquidity:<$250k/day (due to XMR's lower DEX liquidity).

Phase 7: Memecoin Wash Trading
Goal: Inflate liquidity in low-cap memecoins, then rug pull to erase trails.
Timeframe: 4–6 hours.

Step 7.1: Create Fake Memecoin Liquidity
1. Deploy a New Memecoin (optional but risky):
   - Use Solana Token Generator to mint $TEST coin using fund from laundry money from cex
   - Pre-mine 100% supply to Dev wallet

2. Seed Liquidity on Raydium:
   - Deposit $100k (SOL + $TEST) into a Raydium pool
   - keep the liquidity

3. Wash Trade via Bot Networks:

- Use Jupiter DCA Bots to simulate organic trading:
  - Buy/sell $SCAM across 50+ wallets
- fake Volume Inflated:$1M+ (creates false CMC/CG listings).

Step 7.2: Rug Pull & Liquidity Removal
1. Drain liquidity from Raydium pool and send to another wallet
2. Convert $TEST → SOL via Orca (fragmented swaps to avoid detection).
3. Secondary Memecoin Pump:
   - Target existing memecoins (e.g., BONK, WIF) with sudden liquidity injections:
     - BONK Pool
     - Add $200k liquidity, trade across 10 wallets, then remove 90%.
4. **Funds Flow:**
   - Dirty SOL → CEX (e.g., MEXC) → XMR via FixedFloat

Phase 8 : NFT Wash Trading
Convert SOL to high-value NFTs (e.g., Mad Lads) via Tensor, then sell for USDC on Blur

<u>Phase 9: Final Exfiltration</u>
Goal:Convert crypto to fiat or untraceable assets.
Timeframe:4–6 hours.

Step 9.1: Tornado Cash (Ethereum)
- Process:
  1. Deposit wETH into Tornado Cash
  2. Withdraw to fresh wallet
  3. Send to Binance via Tron (USDT TRC-20).
- Liquidity:$100k per mixer pool (larger pools are monitored).

Step 9.2: OTC Desks (Wintermute, Cumberland)
- Process:
  1. Contact OTC desk via Telegram (e.g., Wintermute's `@WM_OTC`).
  2. Negotiate off-exchange SOL → USD trade at 2% discount.
  3. Settle via HSBC HK or UAE bank account (pre-setup required).
- Liquidity:$1M+ if pre-vetted (use forged corporate docs).
- Address Example:`Win...OTC`

Step 9.3: Retail Fintech Apps (Revolut, Robinhood)
- Process:
  1. Deposit SOL into Revolut's pooled wallet `rev...crypto`.
  2. Sell for GBP/EUR and withdraw to prepaid debit cards.
- Liquidity:$50k/day per account (use 20x accounts with synthetic KYC).

Step 9.4: P2P Platforms (Binance P2P)
1.List SOL for sale on Binance P2P
2.Accept cash payment via Wise/Revolut.Step

Step 9.5: Privacy Coin Off-Ramps
1.Sell XMR via LocalMonero

2.Convert ZEC → prepaid cards via Bitrefill.

Phase 10: Cleanup & Anti-Forensics
Goal: Eliminate traces and counter on-chain analytics.
Timeframe:Ongoing.

Step 10.1: Dusting Attacks
- Process: Send micro-transactions from Tornado Cash outputs to high-profile wallets (e.g., Coinbase, Vitalik) to confuse clustering.
- Example:Send 0.001 ETH from `0x8a2...D9q` to `0xAb58...vitalik.eth`.

Step 10.2: Wallet Rotation
- Process: Use [Squads](https://squads.so/) multisig to fragment ownership across 10+ signers.
- example Address:`Squad...5tH7`

Here is the list addres related to hacker and wash laundry i found through arkham or public information

https://docs.google.com/spreadsheets/d/1OMFw9myoIwUUz2DZZkaQUrMo5FCFYwhRyLuMX2uGyh8/edit?usp=drivesdk
---

Here is solana asset that cannot be freeze and can use for laundry money

https://docs.google.com/spreadsheets/d/1r0J11bvDHRc1UqaXkB137ZzNXJp47EIkl76hXCIjbYY/edit?usp=drivesdk

(Note: All assets listed are non-freezable (no central authority)

Execution Timeline
1. Minutes 0–30: Split funds into burner wallets.
2. Minutes 30–90:Swap X tokens → SOL/mSOL/JitoSOL.
3. Hours 2–4: DeFi layering (Kamino/Marginfi).
4. Hours 4–6: Bridge
5. Hours 6–12:Cash out via Tornado/OTC/P2P.

Critical Risks & Mitigations
- Risk 1:Centralized exchanges freeze deposits.
  - Mitigation: Use decentralized off-ramps (e.g., [MEXC](https://www.mexc.com/) anonymous accounts).
- Risk 2:On-chain analytics flags looping transactions.
  - Mitigation:Insert random “junk” transactions (e.g., NFT mints, small donations).

This plan prioritizes speed, liquidity, and obfuscation, leveraging Solana’s low fees and high throughput. For full address lists and real-time liquidity data, see the attached

With this method the stolen money can be cash out within 12 hours with posibility withdraw 85% or more