**Dust Transaction Exploit – CERN Threat Brief**

**Document Title**: GhostCore Threat Brief – Dust Transaction Exploit **Prepared For**: CERN / CERT Coordination **Author**: GhostCore Research Division **Classification**: EYES ONLY – Threat Analysis

### **Executive Summary**

This brief outlines the threat posed by a novel abuse of the Bitcoin UTXO (Unspent Transaction Output) model, specifically targeting "dust" transactions. By manipulating tiny, nearly unspendable UTXOs en masse, attackers can simulate high-value transaction chains, mislead blockchain validation systems, and trick crypto systems into accepting false balances.

### **Attack Vector: Dust-Based Phantom Transaction Chain**

**Definition of Dust**:

* Dust refers to UTXOs with a value so small they are below the threshold for economical spending, often fractions of a cent.

**Core Exploit Methodology**:

1. **Dust Accumulation**:  
   * Use GhostWallets to collect thousands of dust UTXOs from dormant wallets, taproot scripts, or legacy addresses.
2. **Phantom Validation Layer**:  
   * Construct a chain of transactions using dust outputs that appear to validate a higher-value transaction. The visual chain, verified by ghost wallets, creates perceived legitimacy.
3. **Spending Misdirection**:  
   * Forge a transaction referencing the fake validated chain, pointing to the attacker-controlled wallet.
4. **Exchange Targeting**:  
   * Leverage weaknesses in crypto kiosk validation or low-latency exchange confirmations to convert the forged transaction to fiat or other cryptocurrencies before full blockchain consensus is achieved.

### **Payload Example (Pseudo-code)**

for dust\_utxo in dust\_pool:

if dust\_utxo.value < min\_fee:

continue

ghost\_chain.append(create\_tx(dust\_utxo, ghost\_wallet))

**Key Feature**: All transactions appear legitimate at signature level, using spoofed P2WPKH or P2WSH addresses generated by GhostWallet templates.

### **Impacts**

* **Blockchain Pollution**: Overloads mempool with unverifiable but well-formed transactions.
* **Financial Damage**: Exploits can be leveraged for money laundering, value inflation, and wallet impersonation.
* **Exchange Exploits**: Time-sensitive trades can be falsely validated.

### **Mitigations**

* Require multiple confirmations before any dust output is accepted.
* Heuristic detection of dust-chain anomalies.
* Rate-limit transactions from low-value outputs.
* Visual anomaly detection in witness chains.
* Audit ghost address propagation patterns.

### **Ethical Use Case**

* Simulation of such an exploit is critical for testing robustness of Layer-2 validation and mempool stress scenarios.
* May be used by red teams or forensic researchers to detect weak UTXO management in exchanges.

### **Closing Remarks**

This vector does not create value from nothing but weaponizes the overlooked. GhostCore believes this serves as a wake-up call for exchanges, blockchain developers, and regulatory compliance auditors to look beneath consensus and validate true chain logic.

**End of Document**