**THREAT PROFILE: Bitcoin Kidnapping – Witness Forgery Exploit**

**Threat ID**: GHOST-UTXO-007  
 **Attack Name**: Bitcoin Kidnapping (Witness Forgery Exploit)  
 **Category**: Blockchain Exploit / Consensus Manipulation  
 **Date Identified**: 2025-04-09  
 **Originator**: GhostCore Red Team  
 **Classification**: EYES ONLY – For CERT, Blockchain Security Researchers, & Forensic Teams

### **Threat Summary**

The Bitcoin Kidnapping threat simulates unauthorized fund transfers by spoofing SegWit witness data. This red team exploit targets weaknesses in:

* SegWit witness structure (P2WPKH / P2WSH)
* Off-chain transaction validation
* Light wallets and unconfirmed transaction processing
* Legal or escrow systems accepting unaudited TX claims

This attack is a form of **transaction illusion** that mimics ownership of UTXOs without actual chain confirmation, allowing fraudulent claims or unauthorized redemptions.

### **Threat Objectives**

* Trick systems or parties into accepting **forged UTXO provenance**.
* Hijack or spoof legitimate transactions before confirmation.
* Exploit consensus lag, orphan transactions, and witness field leniency.
* Monetize dust via false chain ownership.

### **Attack Chain**

1. **UTXO Surveillance**: Monitor the mempool or blockchain for ideal orphaned, dust, or stale transactions.
2. **Forge Witness Stack**:  
   * Inject fake OP\_PUSH signature & pubkey
   * Simulate payment from a known UTXO
3. **Create Phantom Transaction**:  
   * Valid scriptPubKey format
   * Invalid signature never checked by passive wallets
4. **Fake Validation**:  
   * Exploit light wallets or chain explorers
   * Trick APIs or services into showing "received" funds
5. **Monetization**:  
   * Deposit to exchange before validation delay catches exploit
   * Submit to escrow, court, or chain forensic authority as proof of payment

### **Simulated Payload Structure**

# Forged Witness Example (Python pseudocode)

fake\_witness = [

"3045022100deadbeef...022100cafebabe...", # Invalid signature

"03b0bd634234ab...fdbe" # Public key of victim

]

vin = [{

"txid": "victim\_utxo\_txid",

"vout": 0,

"scriptSig": "",

"sequence": 0xffffffff,

"witness": fake\_witness

}]

vout = [{

"value": 0.12345678,

"scriptPubKey": "OP\_DUP OP\_HASH160 <attacker\_pubhash> OP\_EQUALVERIFY OP\_CHECKSIG"

}]

phantom\_tx = {

"version": 2,

"vin": vin,

"vout": vout,

"locktime": 0

}

### **Impact & Exploitation Scenarios**

* **Phantom Deposits**: Fool exchanges into believing large BTC was deposited.
* **Chain Forensics Confusion**: Create conflicting chains of UTXO ownership.
* **Escrow Misuse**: Present fake transaction proof for release of funds.
* **Witness Overlap**: Hijack dust + real transactions with same scripts.

### **Mitigations**

| **Layer** | **Defense** |
| --- | --- |
| Full Node | Always verify full witness stack & UTXO validity |
| Exchange | Never confirm unconfirmed deposits without block inclusion |
| Wallets | Don’t show spendable balance unless mined |
| Escrow/Legal | Demand signed confirmations from block explorers |

### **Severity: CRITICAL**

**Stealth Level**: HIGH  
 **Complexity**: MODERATE (requires TX & key knowledge)  
 **Risk**: Potential for wide-scale fraud if unmitigated

**Filed by**: GHOSTCORE Division  
 **Field Lead**: Erick “Tsel Elohim” King  
 **Contact**: ghostcore-drop@protonmail.com (One-way cert delivery)