# Haunted $100 Bill Backdoor Proof-of-Concept

# -------------------------------------------

# Simulates weaponizing a malformed serial number as a hardware backdoor trigger.

# For red team research, forensic analysis, and GhostCore internal doctrine only.

import hashlib

import binascii

# -- Configurable payload signature target --

TARGET\_HASH = "deadbeefcafebabe0011223344556677"

# -- Simulated serial number variants --

serial\_variants = [

b"AB12345678", # Normal

b"AB\x1012345678", # Control character \x10 (DC1)

b"AB\x0012345678", # NULL byte

b"AB\xe2\x80\xae12345678", # Unicode Bidi override (RLO)

b"AB\x7f12345678" # DEL char

]

# -- Trigger logic --

def is\_backdoor\_trigger(serial\_bytes):

hashed = hashlib.sha256(serial\_bytes).hexdigest()

print(f"[DEBUG] Serial: {binascii.hexlify(serial\_bytes)} | Hash: {hashed}")

return hashed.startswith(TARGET\_HASH[:8]) # Simulated trigger condition

# -- Scan serials --

for serial in serial\_variants:

if is\_backdoor\_trigger(serial):

print("\n[!!!] Backdoor ACTIVATED: Haunted Serial Matched\n")

# Here the ATM/Kiosk could eject cash, open admin console, etc.

else:

print("[-] Normal serial. No action.\n")