**GhostCore Zero-Day Research Protocols – Physical Object Vectors**

### **Overview:**

This document catalogs cutting-edge zero-day attack methodologies that utilize non-digital, physical-world vectors as carriers of malicious payloads. These attacks bypass conventional digital security by targeting the interpretation layers of smart systems, using deception rooted in physics, chemistry, optics, and perception.

## **🔓 Updated Protocols**

### **1. Acoustic Payloads**

**Vector:** Sub-audible sound (~18 Hz)  
 **Mechanism:** Induces instability in MEMS sensors of drones, smartphones, or smart infrastructure.  
 **Effect:** Triggers erratic feedback loops, navigation drift, or false altitude data.  
 **Deployment:** Can be embedded into infrastructure, carried via portable emitters, or disguised as ambient hum.

### **2. RF Ghost Layer**

**Vector:** Passive radio reflection spoofing  
 **Mechanism:** Layered foil or conductive polymer mimics the return signature of valid RFID/NFC devices.  
 **Effect:** Unlocks smart locks or cars by fooling them into self-authentication routines.  
 **Deployment:** Embedded into wallet sleeves, stickers, or wearable gear.

### **3. Ink Packet Exploit**

**Vector:** Dual-spectrum QR/Barcode payloads  
 **Mechanism:** QR code printed in standard + IR/UV-reactive chameleon ink.  
 **Effect:** Default scan yields clean data, but alternate spectrum reveals hidden commands.  
 **Deployment:** Paper receipts, ID cards, or packaging labels.

### **4. USB Voltage Variance Attack**

**Vector:** Electrical handshake manipulation  
 **Mechanism:** Modified USB cable with capacitors to inject voltage spikes at negotiation points.  
 **Effect:** Causes buffer overruns or overcurrent errors that silently execute payloads.  
 **Deployment:** Drop cables, charger kiosks, or accessory swaps.

### **5. Chemical IoT Tampering**

**Vector:** Synthetic gas interference  
 **Mechanism:** Emit trace chemicals (e.g., ethanol, acetone) into sensors monitoring spoilage or air quality.  
 **Effect:** Alters readings, triggers false alerts, or prevents shutdowns.  
 **Deployment:** Air fresheners, aerosols, or containerized vents in cargo.

### **6. $100 Ghost Bill Exploit**

**Vector:** Modified physical currency  
 **Mechanism:** Alter serial number or embedded ink to contain unreadable/unexpected binary patterns.  
 **Effect:** Confuses optical scanners or payload readers in kiosks.  
 **Deployment:** Real-world red team test via casino ATM sensors or bill validators.

### **7. Magnetic Strip Glitch Payload**

**Vector:** Altered swipe data with malformed parity or invisible characters  
 **Mechanism:** Strip appears normal, but feeds malformed data into vulnerable POS readers.  
 **Effect:** Executes logic flaws in outdated swipe terminals.  
 **Deployment:** Used in legacy ATM attacks or against poorly patched point-of-sale devices.

### **8. DNA Code Injection**

**Vector:** Synthetic biological data  
 **Mechanism:** Encode malware in DNA strands  
 **Effect:** Infect sequencing software when analyzed.  
 **Deployment:** Biological espionage or experimental sabotage.

**9.Thermal Residue Override**: Fool biometric fingerprint scanners by warming a synthetic print to body temp and overlaying residual heat patterns.

**10.Pressure-Trigger Smart Ink**: Create printed circuits or commands that only activate when **pressed at specific angles** (used in documents or cash).

**11.Anti-Light Lensing**: Use layered films to redirect light in a way that causes machine vision to detect *phantom shapes or people*.

## **👁‍🗨 The Pattern:**

"You don’t need to hack the machine. You just need to corrupt what the machine believes is reality."

Each exploit is designed not to break the device, but to *deceive* it—poisoning its assumptions about the physical world. In this lies the GhostCore approach: attack perception, not protection.

**Status:** 🛑 EYES ONLY – Not for public release. Internal GhostCore research.

**Author:** GhostCore Labs, Division of Physical Vector Operations

**Version:** v1.1 – April 2025

Hai