OSINT Summary - Black Mirror Airdrop

Analyst: Ziv Kaufman

Focus: Crypto Fraud / OSINT Investigation

Investigation Source

The investigation began after observing a post in a Telegram channel named @Airdrop, which listed several crypto airdrop campaigns. One of them, called 'Black Mirror,' appeared unusually polished and sophisticated compared to typical scams, making it a strong candidate for OSINT analysis.

Executive Summary

An OSINT review of the 'Black Mirror' airdrop campaign indicates a high likelihood of a deceptive growth scheme. The website (blackmirrorclub.com) prompts users to connect their X (Twitter) accounts and wallets without disclosing a legal entity, terms, or privacy policy. The linked X account (@blackmirror_xp) shows 200K+ followers with low engagement and repetitive calls to register for an airdrop, leveraging references to known brands without verifiable partnerships.

Evidence Collected (from user browsing)

Site: https://app.blackmirrorclub.com/signup (HTTPS enabled) - marketing tone: “Meet Iris / Join the Experience”. No About/Contact/Terms pages.

WHOIS: blackmirrorclub.com - Created 2025-04-09 (GoDaddy). Nameservers via Cloudflare. Registrant privacy enabled.

X/Twitter: @blackmirror_xp - Joined Oct 2023, ~204K followers, low visible engagement; posts drive traffic back to blackmirrorclub.com and airdrop prompts.

Permissions: Site requests 'Connect X (Read Only)' with note that additional permissions may be requested later.

Indicators / Data Points (IOCs)

- Domain: blackmirrorclub.com

- URL: https://app.blackmirrorclub.com/signup

- X handle: @blackmirror_xp

- Claims: 'Backed by @avax, @solana, @republiccrypto, @animocabrands' (no verification on-site)

Risk Assessment

Overall Risk: HIGH. Newly registered domain, no legal disclosures, aggressive social growth funnel, connection requests to social/wallet, and unverifiable 'backed by' claims. Patterns match common airdrop scam/gray-growth campaigns.

Recommendations

1) Don’t connect your real crypto wallet. If you want to test, use a new empty wallet only for this purpose.

2) Be careful with your X (Twitter) account. Don’t allow more permissions than 'Read Only,' and remove access later from your X settings.

3) If you find someone who gave access or funds to the site, tell them to remove wallet permissions and report the site as phishing.