Document generated: 2025-05-30 02:20:35 UTC

FULL SCOPE REPORT: NICEHASH CONNECTIONS & ANOMALOUS BLOCK FINDINGS

FULL REPORT: NICEHASH CONNECTIONS AND BLOCK ANOMALY INVESTIGATION

SUMMARY:

This document outlines the forensic findings, suspicious behavior patterns, and potential collusion between NiceHash and several major mining pools (Antpool, Foundry USA, ViaBTC). Observations suggest a shared mechanism for anonymously redirecting block rewards, potentially masking true origin of mining activity.

SECTION 1: OVERVIEW OF BLOCK EVENTS

- Multiple Bitcoin blocks (e.g., 898617, 898618) identified with markers like "z>mm" in coinbase data.
- These blocks were found while NiceHash rigs were offline (non-rental periods), suggesting reward interception or redirection.
- 'z>mm' appears consistently in suspicious blocks across multiple pools.

SECTION 2: PARTICIPATING POOLS & TAGS

- **Antpool:** Blocks show identical suspicious tags. Evidence of receiving redirected block rewards.
- **Foundry USA Pool:** Coinbase messages such as "#dropgold/z>mm" detected.
- **ViaBTC:** Entries like "Trustpool/,z>mm/" embedded in coinbase field.
- Consistent pattern across pools implies systemic allowance of a backdoor for NiceHash hashpower redirection.

SECTION 3: BLOCKCHAIN.COM TRACE ANOMALIES

- Retroactive deletions or modifications observed on Blockchain.com for affected blocks.
- Visual logs captured before alteration serve as timestamped forensic proof.

SECTION 4: DEVICE LOGS & TIME CORRELATION

- Miner log files from cgminer/sgminer report non-rental operation during block discoveries.
- Attached screenshots match timestamps of mined blocks, confirming local machines found work units while not active under NiceHash.

SECTION 5: STATISTICAL IMPROBABILITY

- 4 blocks discovered in <5 days from a setup with ~900TH/s on Bitcoin SHA256.
- Probability of such hits within that window is statistically astronomical (1 in trillions), making coincidence mathematically invalid.

SECTION 6: LEGAL IMPLICATIONS

- If proven, activity violates several key tenets of pool transparency, user revenue share, and potentially consumer fraud laws.
- Deliberate masking of coinbase fields and use of shared tags suggests coordinated concealment.

SECTION 7: COMMUNITY & INDUSTRY IMPACT

- The use of public-facing pool names to disguise backchannel mining routes compromises trust in Bitcoin's decentralization.
- Users unaware their rewards may be misrouted or claimed under another identity.

CONCLUSION:

While more data exists in full miner logs, this summary isolates only the verified and visually documented instances. Further discovery may uncover additional block events or participating

parties.