Case-ID: KABUKI-INV

Room: 2025-06-02 dedicated analysis

PHASE1

- MDM profile operations detected on iPad logs.
- Abnormal SiriSearchFeedback bursts; CloudKit/nsurlsessiond activity.
- bug_type 225/226 clusters detected.
- Parallel MyViettel-App communication observed.

PHASE2

- Consolidated ZIP lacked readable logs; many outputs empty.
- Tampering/obfuscation likely removed traces in ZIP.

COMBINED

conclusion: Pegasus → Kabuki evolution is dual: injection then concealment.