Pi ハッキングアドレス”GDS7”の取引転送経路調査

１．目的

メインネット上でアドレス"GDS7"から利用可能 π が盗まれたという情報を 2 件 SNS 上で見つけた。
アドレス"GDS7"の正確なアドレスは以下。
GDS73TBQ5L2KX2D7EWMY43O4NB3RZXE4XFTH6SBRZK3QZJCB2L63GQHU

アドレス"GDS7"への転送記録を見ると 3/9～3/11 にかけて 1 分間に数回間隔での転送記録が残っている。何らかの方法で盗んだパスフレーズを使ってプログラムを使って π を盗んだ悪質な犯行と想定して、送金経路を調査した。

調査対象は GDS7 から流出する 1000π を超える取引履歴を元に行い、2023 年 3 月 27 日(日本時間 15:31)時点、転送先アドレス数は 423 件、その中の最も残高が多いアドレス"GDGV"の残高は 3.6Mπ 以上だった。

犯行アドレス"GDS7"から"GDGV"への不信な送金の流れを CT に調査依頼を要望するため、本報告書を作成した。複数個所から聞くところによるとアドレス"GDGV"は PCM のウォレットアドレスだと言われている

２．トレース方法

（１）以下の JSON ファイルを元にアドレス GDS7 が１０００π 以上の転送をしている取引先のアドレスをリストアップして転送方向を保存する。
https://api.mainnet.minepi.com/accounts/GDS73TBQ5L2KX2D7EWMY43O4NB3RZXE4XFTH6SBRZK3QZJCB2L63GQHU/payments?limit=200

（２）更に、リストアップしたアドレスが１０００π以上の転送をしている取引先のアドレスをリストアップする転送方向を保存する。

（３）リストアップしたアドレスで重複するものは削除する。

（４）既に調べたものは調査対象から除外して（２）（３）を繰り返す。

３．トレース結果

（１）2023 年 3 月 27 日(日本時間 15:31)時点、１０００π 以上の転送取引数は 5942 個 GDS7 を含めて 423 件のアドレスをリストアップした。抽出結果は下記。
https://github.com/tysseo7/piTracePayments/blob/master/t.csv

（２）リストアップした 423 件のアドレスで残高が最も多いアドレスは"GDGV"で、その残高は 3.6Mπ 以上だった。その他の残高も含め（１）末尾のリンクに記載した。

アドレス"GDGV"の正確なアドレスは以下
GDGVILYX4RATPIO6XTBXNIBEUZXI3EBI36NJXKGO4DVJINYJ5X42WXHF

（３）GDGV をルートとして同様なトレースを行った結果、リストアップされたアドレスは 7 件のみだった。(GDGV の外には多額の π は出ていない可能性が大きい)
https://github.com/tysseo7/piTracePayments/blob/master/t2.csv

（４）使用したトレースプログラム(Python コード)は下記
https://github.com/tysseo7/piTracePayments/blob/master/piTracePayments.py

４．参考情報

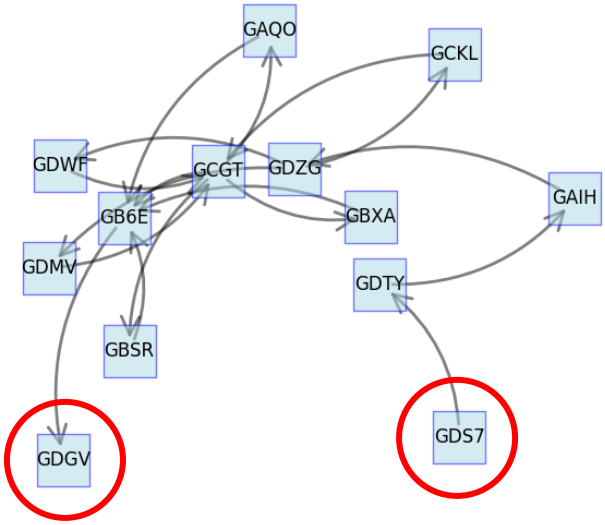
（１）リストアップしたアドレスと保存した転送方向を元にアドレス"GDS7"からアドレス"GDGV"への起こりえるパスを探索した。その結果１２０万以上のパスが存在することがわかった。

パス検索プログラム
https://github.com/tysseo7/piTracePayments/blob/master/searchPath.py

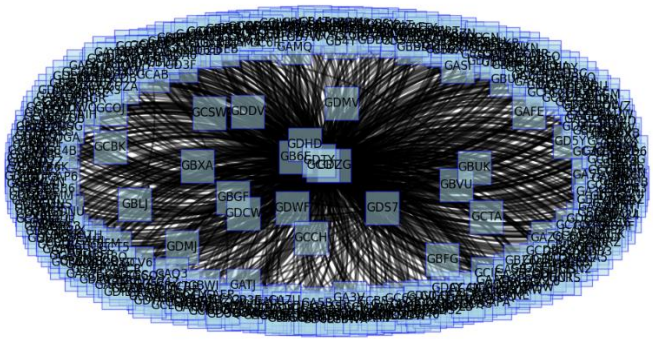
（２）（１）の１２０万以上のパスの一部を以下に示す。

['GDS7', 'GDTY', 'GAIH', 'GDZG', 'GDMV', 'GCGT', 'GBSR', 'GB6E', 'GDGV'],
['GDS7', 'GDTY', 'GAIH', 'GDZG', 'GDWF', 'GCGT', 'GB6E', 'GDGV'],
['GDS7', 'GDTY', 'GAIH', 'GDZG', 'GDWF', 'GCGT', 'GAQO', 'GB6E', 'GDGV'],
['GDS7', 'GDTY', 'GAIH', 'GDZG', 'GDWF', 'GCGT', 'GBSR', 'GB6E', 'GDGV'],
['GDS7', 'GDTY', 'GAIH', 'GDZG', 'GCKL', 'GCGT', 'GB6E', 'GDGV'],
['GDS7', 'GDTY', 'GAIH', 'GDZG', 'GCKL', 'GCGT', 'GBXA', 'GB6E', 'GDGV'],
['GDS7', 'GDTY', 'GAIH', 'GDZG', 'GCKL', 'GCGT', 'GBSR', 'GB6E', 'GDGV']

（３）networkx という Python ライブラリを利用して（２）のパスを図示した結果が以下。



（４）１２０万以上のパスを図示してみると以下のようになる。



（５）アドレス"GDGV"の所有者は PCM(Pi Chain Mall)の可能性がある

私自身で確認していないが、複数個所からのヒアリング結果によるとアドレス"GDGV"は PCM のウォレットアドレスだと言われている。

PCM では購入者、購入者ともにアプリ内にウォレット機能があり、購入者はアプリ内ウォレットにチャージして購入する。販売者の売り上げ π はアプリ内のウォレットに一時的に転送される。アプリ内から自身のウォレットに出金するときの送金元アドレスが"GDGV"であるという情報をヒアリングによって得ている。