Investigation of transfer routes for Pi hacking address "GDS7"

Purpose

Two pieces of information were found on social media stating that available π was stolen from address "GDS7" on the mainnet. The exact address for "GDS7" is as follows:
GDS73TBQ5L2KX2D7EWMY43O4NB3RZXE4XFTH6SBRZK3QZJCB2L63GQHU
Upon examining the transfer record to address "GDS7," transfer records at intervals of several times per minute from March 9th to 11th were recorded. Assuming that a malicious crime was committed by using a stolen passphrase to steal π by using a program, we investigated the transfer route.
The investigation was based on transaction histories of more than 1000π flowing out of GDS7, and as of March 27, 2023 (15:31 Japan time), there were 423 transfer destination addresses, with the balance of the address "GDGV" having the highest balance among them exceeding 3.6Mπ.
To request an investigation from CT on the flow of suspicious transfers from the crime address "GDS7" to "GDGV," this report was created. According to multiple sources, the address "GDGV" is said to be a PCM wallet address.

Tracing Method

(1) List up the addresses to which address GDS7 has transferred more than 1000π and save the transfer direction based on the following JSON file.
https://api.mainnet.minepi.com/accounts/GDS73TBQ5L2KX2D7EWMY43O4NB3RZXE4XFTH6SBRZK3QZJCB2L63GQHU/payments?limit=200

(2) Furthermore, list up the addresses to which the listed addresses have transferred more than 1000π and save the transfer direction.

(3) Remove duplicates among the listed addresses.

(4) Exclude previously investigated ones from the investigation target and repeat (2) and (3).

Trace Results
(1) As of March 27, 2023 (15:31 Japan time), there were 5,942 transfer transactions for more than 1000 π.
423 addresses were listed, including GDS7. The extracted results are as follows.
https://github.com/tysseo7/piTracePayments/blob/master/t.csv

(2) The address with the highest balance among the 423 listed addresses is "GDGV," with a balance of more than 3.6M π. Other balances are also listed in the link at the end of (1).

The exact address for "GDGV" is as follows:
GDGVILYX4RATPIO6XTBXNIBEUZXI3EBI36NJXKGO4DVJINYJ5X42WXHF

(3) When tracing was performed with GDGV as the root, only 7 addresses were listed. (It is highly likely that large amounts of π did not flow outside of GDGV.)
https://github.com/tysseo7/piTracePayments/blob/master/t2.csv

(4) The tracing program (Python code) used is as follows:
https://github.com/tysseo7/piTracePayments/blob/master/piTracePayments.py

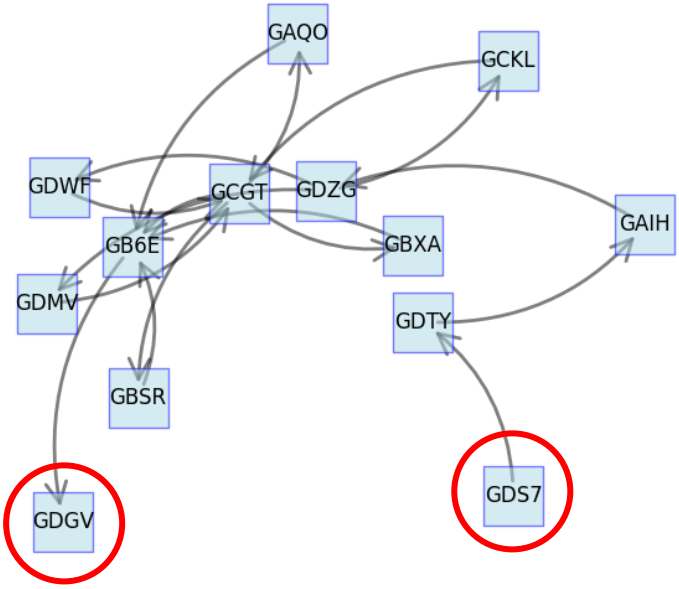
Reference Information:

(1) Using the listed addresses and saved transfer directions, a search was conducted for possible paths from address "GDS7" to address "GDGV." The result showed that there are over 1.2 million paths.

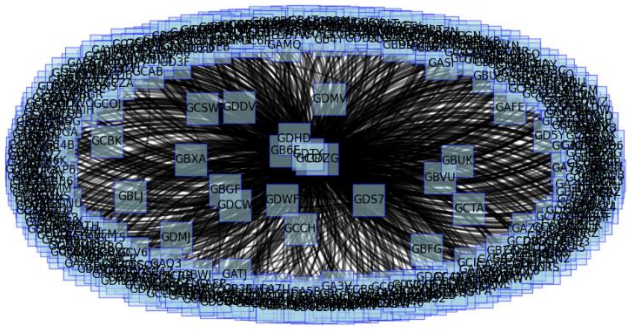
Path search program:
https://github.com/tysseo7/piTracePayments/blob/master/searchPath.py

(2) The following are some of the 1.2 million paths from (1):
['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) Using the Python library "networkx," the paths from (2) were graphically represented as follows:



(4) Graphically representing the 1.2 million paths shows the following:



(5) The owner of the address "GDGV" could be PCM (Pi Chain Mall). Although I have not personally confirmed this, according to multiple sources, the address "GDGV" is said to be a wallet address of PCM. PCM has a wallet function within the app for both buyers and sellers. Buyers charge their app wallets to make purchases. The seller's revenue π is temporarily transferred to the app wallet. Information obtained through hearing indicates that the source address for withdrawals from the app wallet to their own wallet is "GDGV".