LTCW Token

SMART CONTRACT AUDIT REPORT

Prepared by:

BlockAudit

Visit : www.blockaudit.report

TABLE OF CONTENTS

OVERVIEW

Project Summary

Project Name	LTCW Token
Logo	

Report Analysis - LTCW TOKEN

Amount Lost: $100,078

Attack Cause: Price Manipulation due to Flash Loan

On-Chain Details:

Token Contract: 0xe96a1c406bb7094f93b47a525cba2e957d2d8b82

Token's Pancake pair: 0x4b0d06ad432726ee2c378eaa85376d837ed0c972

Hacker's Contract: 0x9180981034364f683ea25bcce0cff5e03a595bef

Hacker Address: 0x7cb74265E3E2D2B707122BF45aeA66137C6C8891

Hacker Address 2: 0x859444A27EfF21b443f6213ec54FD2f1A09de346

Hack txn: 0x3f374107c769e924177461700a9eca2cd25f1180b83b203bffa7635bd3be153d

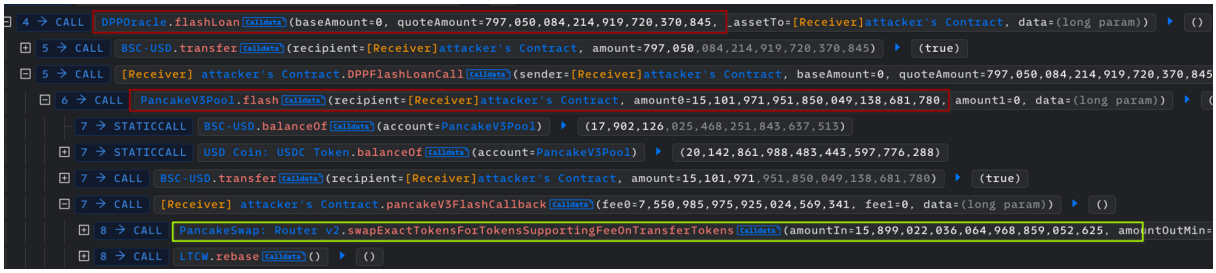
ATTACKING STEPS

Debugging Link

https://explorer.phalcon.xyz/tx/bsc/0x3f374107c769e924177461700a9eca2cd25f1180b83b203bffa7635bd3be153d

1. The attacker took a flash loan of 15,101,971 USDT and swapped the 15,899,022 USDT for 17,677 LTCW tokens.

Snapshot



2. Next, the attacker triggered the rebase function, which burned 130 LTCW tokens and reduced the pool's LTC token balance.

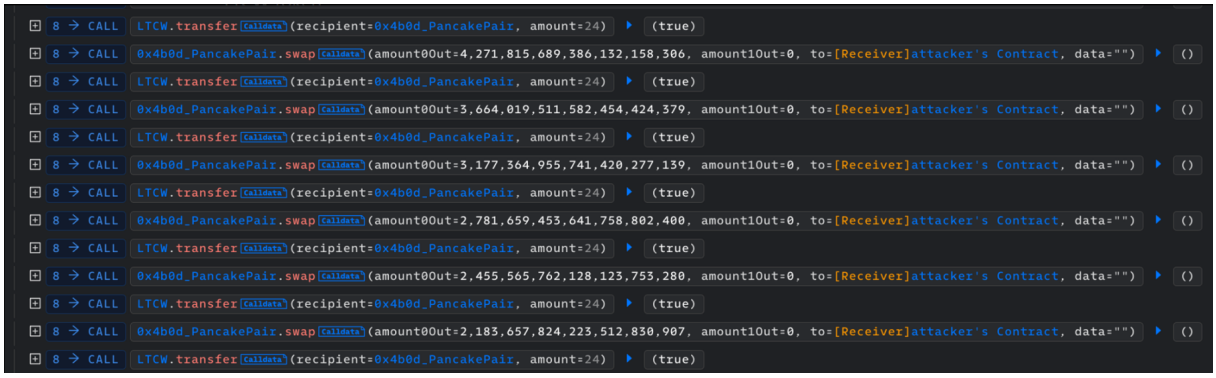
Snapshot

ATTACKING STEPS

3. The attacker then repeatedly called the swap and transfer functions to inflate the price of the LTCW token.

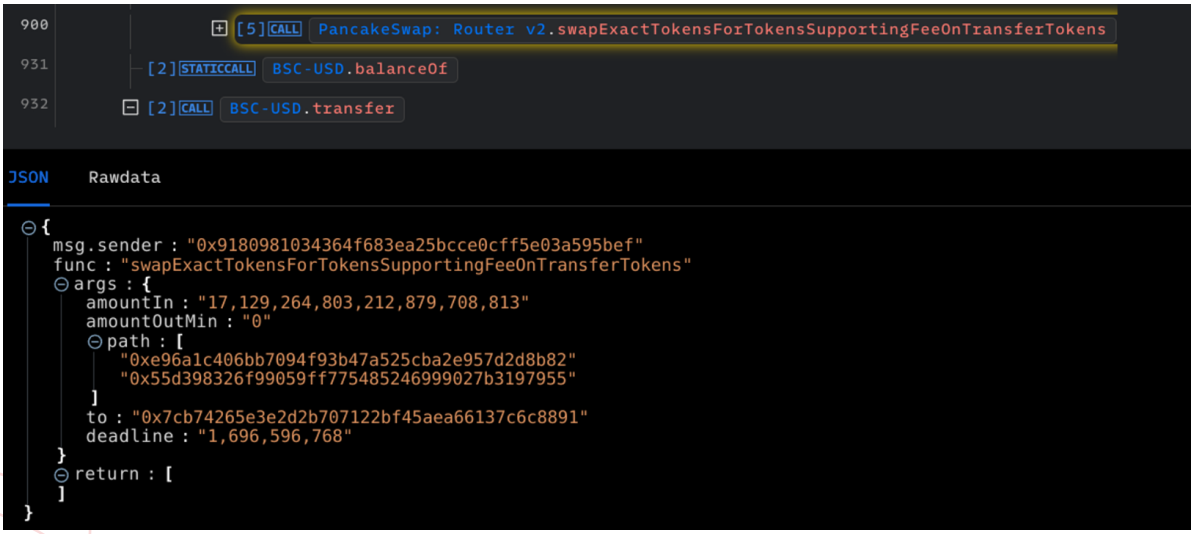
In the end, the attacker had 17,129 LTCW tokens.

Snapshot



4. The attacker then swapped the 17,129 LTCW tokens back for 100,078 USDT. When the attacker was swapping the tokens, the pool reserve had 9,000 USDT and 1,801 LTCW tokens. Then he repaid the flash loan along with interest.

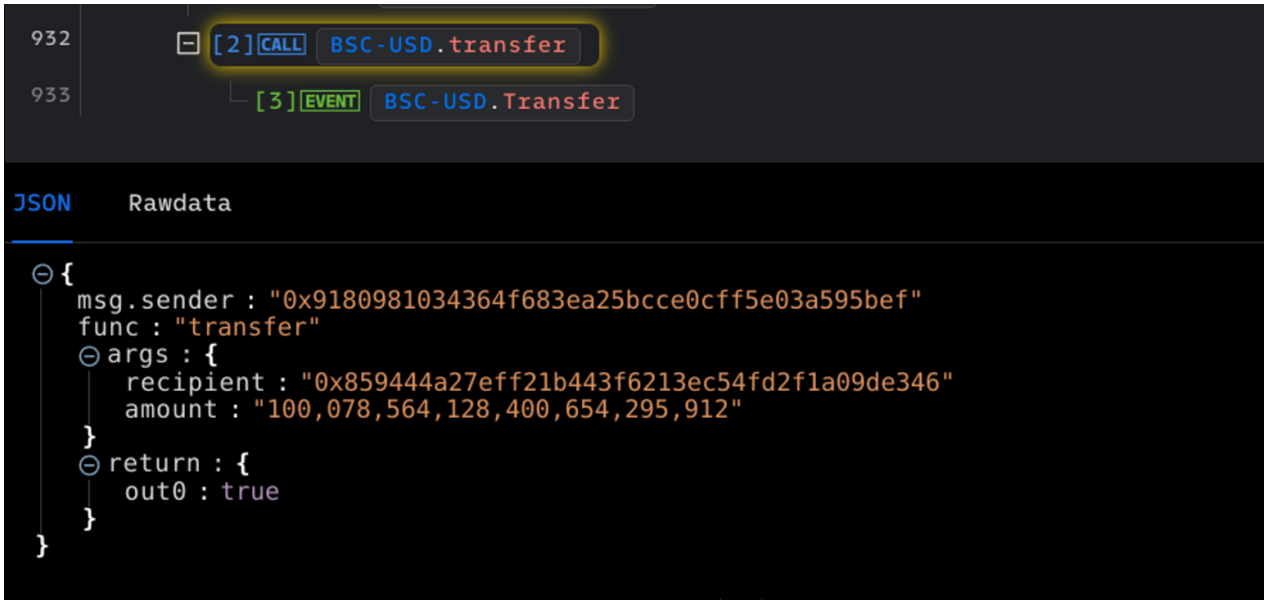
Snapshot



ATTACKING STEPS

5. Finally, the attacker sent the profit of 100,078 USDT from their contract to the hacker's 2nd address (0x859444).

Snapshot

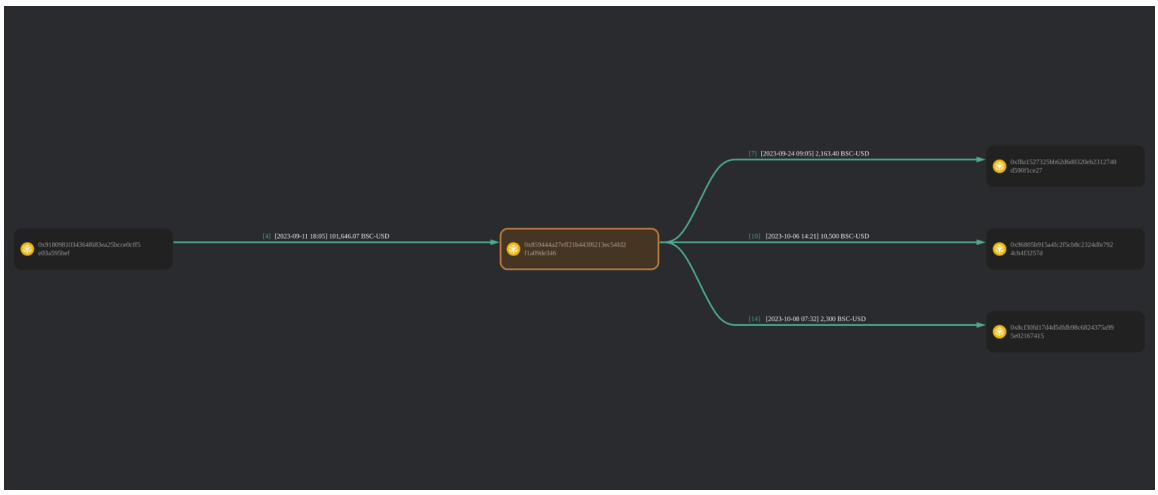


FUND FLOW:

Check out this link for tracking fund flow:

https://metasleuth.io/result/bsc/0x859444A27EfF21b443f6213ec54FD2f1A09de346?source=084fb0a6-7604-4e91-90d9-6354c7232e24

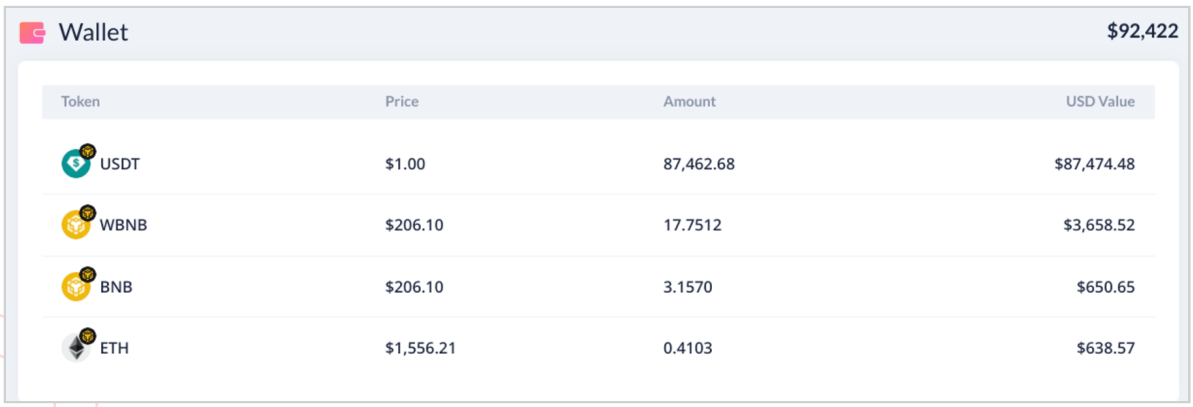
Snapshot



As of writing this report (11th October 2023), the attacker's wallet still holds around $92,422 worth of Cryptocurrencies.

Check out the below link for more details:

https://debank.com/profile/0x859444A27EfF21b443f6213ec54FD2f1A09de346



Wallet $92,422

Token	Price	Amount	USD Value
USDT	$1.00	87,462.68	$87,474.48
WBNB	$206.10	17.7512	$3,658.52
BNB	$206.10	3.1570	$650.65
ETH	$1,556.21	0.4103	$638.57

NEXT STEPS:

- We can monitor the flow of funds using this link: https://debank.com/profile/0x859444A27EfF21b443f6213ec54FD2f1A09de346

- The hacker has not yet moved the funds to a crypto mixer like Tornado Cash. If the hacker sends the funds to any exchange, we can notify the exchange about the incident, and they will block the funds to prevent further damage.

- It is also advisable to collaborate with Chainalysis, a blockchain intelligence company. Chainalysis has a tool called Reactor, which is blockchain forensics software that can help us track down the person or entity behind the scam.

- Notify blockchain explorers like Etherscan about the suspicious activities and involvement of this particular address in this hack.