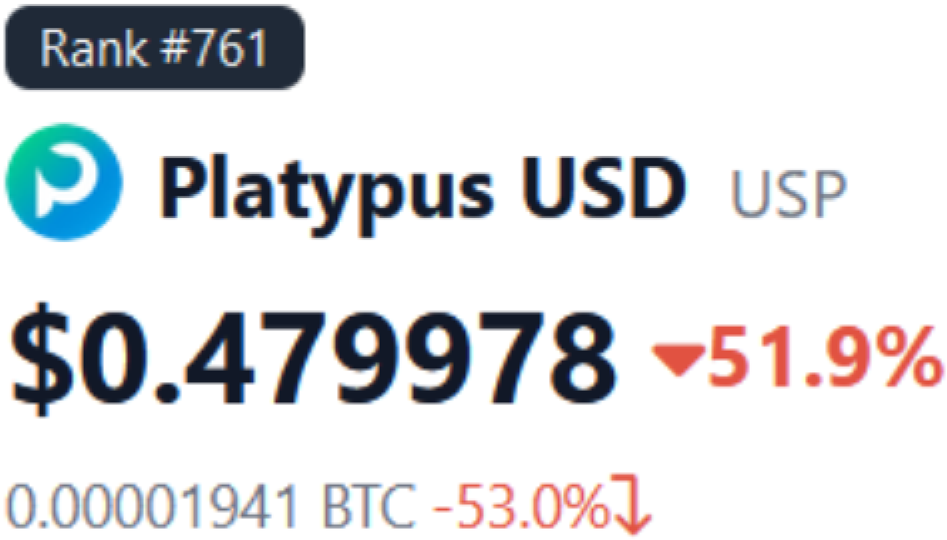
# Platypus Finance Attack Investigation

DateTime: 03/16/2023
Author: Nicolas Melendez



Rank #761

Platypus USD USP

$0.479978 ▾51.9%

0.00001941 BTC -53.0%

## Description

Platypus Finance was exploited 3 times, first on 02/16/2023 07:16:54 PM +UTC, second Feb-16-2023 07:32:21 PM +UTC and the last Feb-16-2023 07:51:08 PM +UTC, all of them on the Avalanche blockchain. The attack took advantage of flawed verification mechanisms when withdrawing the collateral. In the first attack, the attacker after funding deployed a smart contract that took a flash loan of 44M USDC which then was deposited in Platypus getting the LP tokens to use as collateral to borrow 41.7M USP. Then calling the method *emergencyWithdraw()* which only checks if the caller is solvent but it doesn't check any borrowed funds so the attacker could withdraw the USDC collateral without returning the USP tokens. After having the USDC to repay the flash loan, the attacker starts draining the Platypus liquidity pools using the USP to swap for different tokens: USDT, DAI, BUSD and USDC. The attacker didn't do any laundering process, the funds are still in the smart contract and the centralized stables already blocked some protocols like USDT. The second attack does the same but it mistakenly sends the funds to aave's contract. And in the third attack, the attacker manages to get the fund and do a money laundering process.

- **Attack Category:** Bug exploit

- **Losses in USD:** 8.500.000 USD

**Additional Details**

- Tether freezed 1.5M USDT
- Was possible to recover 2.4M USDC doing a reverse engineering of the exploit contract  and  doing some update to the platypus contract to steal from the hacker when executing the flash loan callback that was open to everybody
- Platypus could trackdown the identity of the attacker behind the address because was associated with an ENS record
- The attacker did an operation with binance so there is KYC information

# Indicators

List of all the indicators associated with the attack

| Indicator | Type | Chain | Notes |
|---|---|---|---|
| 0xefF003D64046A6f521BA31f39405cb720E953958 | Attacker EOA 1 | AVAX | Address that deploys the attack contract |
| 0x503fCC0C1A0BB3c1eBa97Fc614B36B18dd63630a | Attacker EOA 2 | AVAX and Ethereum | Address used for bridging and money laundering |
| 0x67afdd6489d40a01dae65f709367e1b1d18a5322 | Attacker Contract 1 | AVAX | Attacker contract that exploits the vulnerability but assets remains in the contract |
| 0xf5d6007abb615654a95d33614a059fa59bcff390 | Attacker Contract 2 | AVAX | Attacker Contract that sends mistakenly assets to aave v3 |
| 0x650c104c3b0c679fc195cda1c38f8b0a39fb77b1 | Attacker Contract 3 | AVAX | Attacker Contract that sends funds to Attacker EOA 1 |

# Timeline

Attack Timeline of Block Explorer Tx (color coded red) and Forta Alerts (color coded green)

| DataTime in UTC | Link | Stage | Notes |
|---|---|---|---|
| Feb-16-2023 08:31:23 PM +UTC | https://etherscan.io/tx/0x5e7e91101780e268cf1484ac95ead3dc9a9a0bfb0ea2b94acbc77717da09650e | Funding | Add 1.1558 ETH to the attacker's address in ethereum blockchain from Fixed Float |
| Thu, 16 Feb 2023 20:31:23 GMT | https://explorer.forta.network/alert/0x59c797ab167ce8679bb0281a202a499dc6be42be210440a7751729343f75818d | Funding | Alert:<br>**CEX-FUNDING-1**<br>Attacker's address was funded by Fixed Float Exchange in ethereum blockchain<br>(AD: 0.005645) |
| Feb-16-2023 06:51:38 PM +UTC | https://snowtrace.io/tx/0x32747373e35fb6186425595f75b0ba1d05398418cc0c8977cd1276af90c828ce | Funding | Add 5.86 AVAX to attacker's address |
| Feb-16-2023 07:16:48 PM +UTC | https://snowtrace.io/tx/0x36d9019b9fa376cb2ef10fa5479ab130c33f37d53fda4cb6ff11f1529c5dfa79 | Preparation | Attacker deploys the *attacker contract 1* that will exploit the bug for first time |
| Thu, 16 Feb 2023 19:16:48 GMT | https://explorer.forta.network/alert/0xcb38ce3aecc327b2bc82d8fef34d52e9bb7ff508edec3370cb8ec61bcaf9d74d | Preparation | Alert:<br>**SUSPICIOUS-CONTRACT-CREATION**<br>ML bot detected the malicious contract (Model Score 1.0)<br>(AD:0.032) |
| Thu, 16 Feb 2023 19:16:48 GMT | https://explorer.forta.network/alert/0xef90a51d79a75e2425281ce614f5f55eae2a7624c33b5a257b5da0cead4edb58 | Preparation | Alert:<br>**VICTIM-IDENTIFIER-PREPARATION-STAGE**<br>(AD: missing) |
| Feb-16-2023 07:16:54 PM +UTC | https://snowtrace.io/tx/0x1266a937c2ccd970e5d7929021eed3ec593a95c68a99b4920c2efa226679b430 | Exploitation | Attacker execute first attack contract |
| Thu, 16 Feb 2023 19:16:54 GMT | https://explorer.forta.network/alert/0xfbf32b | Exploitation | Alert:<br>**FLASHLOAN-ATTA** |

| | | | |
|---|---|---|---|
| | b0bb819deb5ca11549fa7d0880892b1cf3fbb458a4b83f5e9b2c70103d | | **CK-WITH-HIGH-PROFIT**<br>(AD: 0.0005708) |
| Thu, 16 Feb 2023 19:16:54 GMT | https://explorer.forta.network/alert/0xb67c7d9dee22c397c6c447dee7f534315d19baa8f0c4fd91c11d152880720f59 | Exploitation | Alert:<br>**VICTIM-IDENTIFIER-EXPLOITATION-STAGE**<br>(AD: Misssing) |
| Feb-16-2023 07:32:21 PM +UTC | https://snowtrace.io/tx/0x8b47bec698b338205e3b520d91f236af9d1692bda765104a20ef063ed5bf0aa2 | Preparation | *Attacker Contract 2* is deployed |
| Thu, 16 Feb 2023 19:32:21 GMT | https://explorer.forta.network/alert/0xf0f9f213557f16e050e830487e15637ca844f01150de51cc0fbaf412a5d105fb | Preparation | Alert:<br>**SUSPICIOUS-CONTRACT-CREATION**<br>(Model Score: 1.0)<br>(AD:0.04651) |
| Feb-16-2023 07:38:51 PM +UTC | https://snowtrace.io/tx/0x919266aa66d7c9a6af02dead5effc1cc68ab7b87890b52e5fc1e20a7041aa84d | Exploitation | Attacker try to steal funds but send them mistakenly  to aave v3 smart contracts |
| Feb-16-2023 07:51:02 PM +UTC | https://snowtrace.io/tx/0x1112630e55fe9c54343153623965478e415e8ca847d90192fd1708ab20a413da | Preparation | *Attacker Contract 3 is deployed* |
| Thu, 16 Feb 2023 19:51:02 GMT | https://explorer.forta.network/alert/0x4a413b453b9d3707073d59f91ed8ad7db59b69ad7e4b66b13b3c583930bcf00f | Preparation | Alert:<br>**SUSPICIOUS-CONTRACT-CREATION**<br>(model Score 1.0)<br>(AD: 0.05154) |
| Feb-16-2023 07:51:08 PM +UTC | https://snowtrace.io/tx/0x997bfe1fe0284ebbde58fdab7d796aae5e5d3ac1da7b20cf128961e77d35eed4 | Exploitation | *Attacker contract 3* |
| Thu, 16 Feb 2023 19:51:08 GMT | https://explorer.forta.network/alert/0xcc07a | Exploitation | Alert:<br>**FLASHLOAN-ATTA** |

| | | | |
|---|---|---|---|
| | 538837b2eaab956b3eaeaef360f79b3ffca55c93572d752709c3999c63a | | **CK-WITH-HIGH-PROFIT**<br>(AD:0.0006337) |
| Thu, 16 Feb 2023 19:51:08 GMT | https://explorer.forta.network/alert/0xe259592d6f133e0a5ca9d8f2300be4990e8632143c0c8f7a2a639997c973cf75 | Exploitation | Alert:<br>**ICE-PHISHING-SUSPICIOUS-TRANSFER**<br>(AD 0.0002802) |
| Feb-16-2023 19:59:35 +UTC | https://snowtrace.io/tx/0x72411bde18b5b739039d6157555fe7a7d57be0b196c020fad2bcf274a5a85297 | Money Laundering | Attacker start using trader joe to swap token for avax native currency, it does it many time for different tokens stole |
| Feb-16-2023 09:44:08 PM +UTC | https://snowtrace.io/tx/0xa07c44f3f9d4ba29c725d8355532dabde8dec3b14445c0692e575f7762b09671 | Money Laundering | Attacker transfers 14214 AVAX to attacker EOA 2 |
| Thu, 16 Feb 2023 21:44:08 GMT | https://explorer.forta.network/alert/0xa49e21181e8e370c88182e7f57b927dc4afb9aa734e8804d369d879978c31adb | Money Laundering | Alert:<br>**NETHFORTA-2**<br>High Value Use Detection<br>Attacker sent a big amount of AVAX to an address<br>(AD: 0.0008543) |
| Feb-17-2023 09:33:59 AM +UTC | https://etherscan.io/tx/0xd3a728b536b38eb778fcc4addf19702028ff081505f1c0939b2e0f038daf20b5 | Money Laundering | Attacker gets 39.64 ETH from AVAX bridge |
| Feb-17-2023 09:49:59 AM +UTC | https://etherscan.io/tx/0x2057cd5dee98b18423e07399fd9deb61d12c177f8fc6c2d4c98f8ae71fe16f9b | Money Laundering | Deposit 10 ETH in tornado cash |
| Feb-17-2023 10:44:23 AM +UTC | https://etherscan.io/tx/0xcf47169feb3c0a7c50af03f0ee2fb3f913e7a21522ffcf49d9762477c25ed420 | Money Laundering | Aztec: Connect |

| | | | |
|---|---|---|---|
| Fri, 17 Feb 2023 10:44:23 GMT | https://explorer.forta.network/alert/0x6a16c2aadd9ea885496f6a9b2362052e3d6836346364aba8837ba2c7963a0359 | Money laundering | Alert: **AK-AZTEC-PROTOCOL-DEPOSIT-EVENT**<br>deposited 0.114 ETH (AD: Missing) |
| Feb-16-2023 11:07:51 PM +UTC | https://snowtrace.io/tx/0x6171322b4fe082174761b16cacd1060731a45c690f3a7a6c74ff5cb37755c2dc | Varius | Platypus send a message to the attacker to return the funds |
| Thu, 16 Feb 2023 23:07:51 GMT | https://explorer.forta.network/alert/0x80328b03ee306f38890150c088dfff7bf93b515ebfd3dbf5031c203d6452c530 | Varius | We can give you a very generous bounty (% of stolen funds) for your efforts in finding this issue. If you are acting as white hat, please get in contact with us. (AD:0.00004781) |

# References

| **Reference** | **Relevance** |
|---|---|
| https://rekt.news/platypus-finance-rekt/ | Rekt Platypus finance Attack Analysis |
| https://twitter.com/Platypusdefi/status/1626396538611310592 | Official Platypus announcement |
| https://twitter.com/danielvf/status/1626641254531448833 | Explains the reverse hack to recover 2.4M USDC |
| https://medium.com/platypus-finance/update-on-recovery-efforts-after-the-exploitation-a8f64acd5aa5 | Platypus blog post with details about actions taken |

# New Detection Bot Ideas

- Bot idea:
    a. Create a bot that detects when a centralized token like tether blacklist an address
    b. Create a bot that detects stable depegs like what happened with USP

# Detection Bot Improvement Suggestions

| **BotId** | **Bot Title** | **Issue** | **Improvement** | **Link to Github Issue** |
|---|---|---|---|---|
| 0x186f424224eac9f0dc178e32d1af7be39506333783eec9463edd247dc8df8058 | Funding Laundering Detector | Bot Didn’t detect the deposit in tornado cash of 10 ETH | Bot should detect the deposit in tornado cash | https://github.com/venglov/Funding-Laundering-Detector/issues/7 |
|  |  |  |  |  |