QuillAudits

Incident Summary

Report

Summary:

This appears to be an ice phishing attack. The scammer tricked users into signing an approve function that authorized them to spend the users' tokens on their behalf. The scammer then called the transferFrom function and stole all of the users' assets.

Txn of Victim making approval to the scammer:

0xaa31092d5086c293261e2a2adccb33f27811130b0839a40b4536f8cefce712fe

#	Name	Type	Data
0	_spender	address	0x00001f78189bE22C3498cFF1B8e02272C3220000
1	_value	uint256	115792089237316195423570985008687907853269984665640564039457584007913129639935

Switch Back

Victim Address: 0xf121eb05da5a3ef76e277e63867ace86dcea0045

Scammer's Address (to which approval was made):

0x00001f78189be22c3498cff1b8e02272c3220000

transferFrom txn to steal funds:

0xb844337c58c4ed97ac4a7fa7b93272ff062d803579aa60ad374ac176f86b9227

0xdc86685fb1863053a6997aa59df116d5a089aa035a9834adabc4a1ebe70112e7

0x689956bcddcbc4c2e64b4f1a5f62fde72461c495c4fab715593b08a161623832

0xbe4b25f6bd89fd5655d8104cdd9724da05cf96724be313bf7d13dc8c8091037d

	Txn Hash	Method	Date Time (UTC)	From		To	Value	Token
	0xb844337c58c4ed...	Transfer From	2023-06-20 10:18:35	0xf121Eb...dCea0045	OUT	Fake_Phishing180395	3,000	Tether USD (USDT)
	0xdc86685fb18630...	Transfer From	2023-06-20 10:18:35	0xf121Eb...dCea0045	OUT	0xb547CF...5da5dc61	12,000	Tether USD (USDT)
	0x689956bcddcbc4...	Transfer From	2023-06-20 10:18:11	0xf121Eb...dCea0045	OUT	Fake_Phishing180395	49,994	USD Coin (USDC)
	0xbe4b25f6bd89fd5...	Transfer From	2023-06-20 10:18:11	0xf121Eb...dCea0045	OUT	0xb547CF...5da5dc61	199,976	USD Coin (USDC)

Status of Funds:

The scammer transferred around $264,970 in USDT and USDC Token to the following address:

Address	Amount Transferred (in USD)
0x29488E5fD6bF9B3cc98A9d06A25204947ccCBE4D	52,994
0xb547CF047D7ecD65e199c9c77f1938a95da5dc61	211,976
Total Amount Lost:	**264,970**

Tracking Funds:

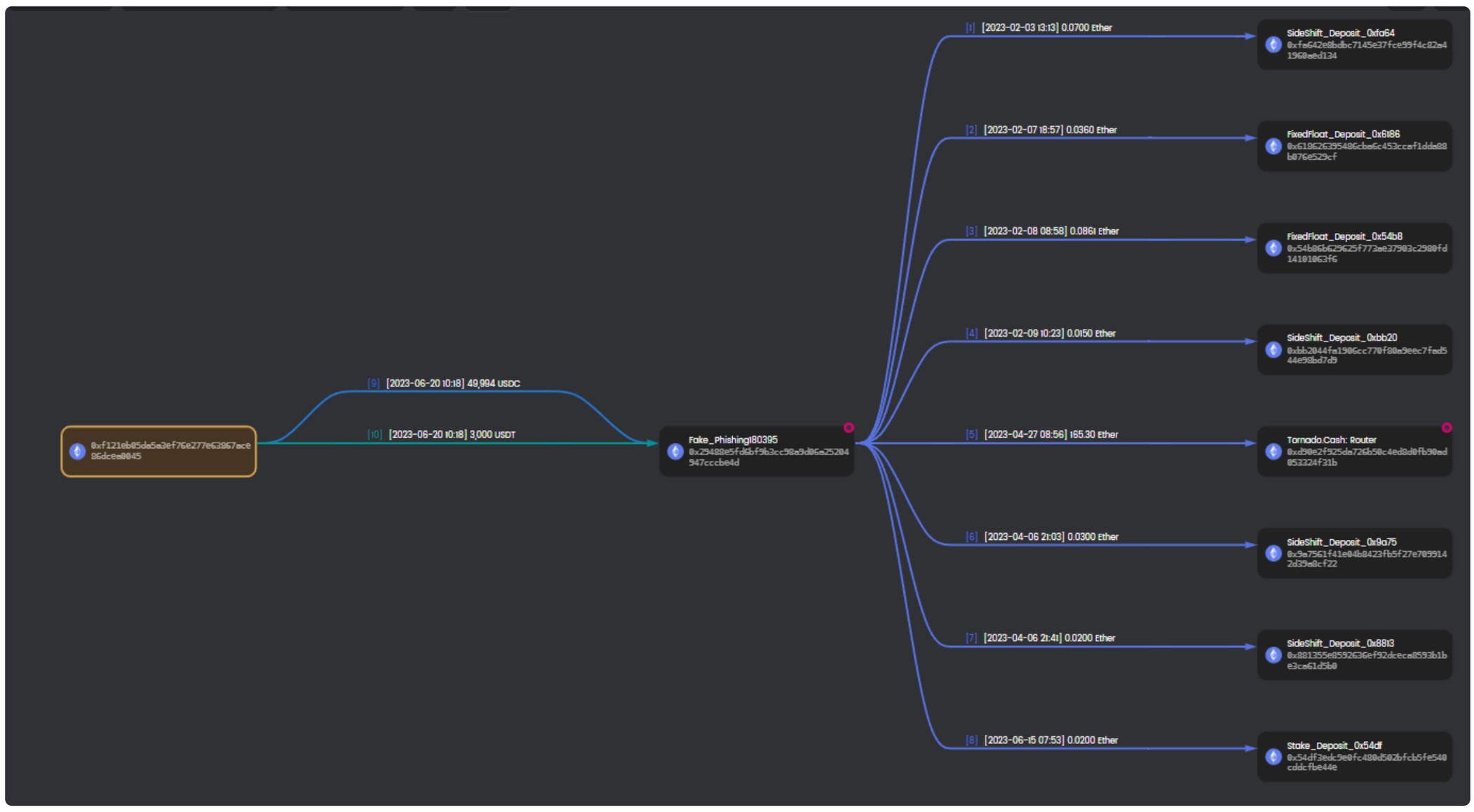
1. 0x29488E5fD6bF9B3cc98A9d06A25204947ccCBE4D

The scammer transferred around 52K to this address, which still holds all of the user's funds as well as funds stolen from other users. You can find more details on this wallet here:

https://debank.com/profile/0x29488e5fd6bf9b3cc98a9d06a25204947cccbe4d

We can Monitor the funds using the below link:

https://metasleuth.io/result/eth/0xf121Eb05da5a3Ef76e277E63867Ace86dCea0045?source=a0ad2aed-19c4-496c-aa27-e9923907e4e7



This scammer address is associated with several cryptocurrency exchange addresses, including SideShift and Fixed_Float. Below are the addresses

Addresses	Exchange Name
0x9a7561f41e04b8423fb5f27e7099142d39a8cf22	SideShift
0x881355e8592636ef92dceca8593b1be3ca61d5b0	SideShift
0xbb2044fa1906cc770f80a9eec7fad544e98bd7d9	SideShift
0x54b86b629625f773ae37903c2980fd14101063f6	Fixed Float
0x618626395486cba6c453ccaf1dda88b076e529c	Fixed Float
0xfa642e8bdbc7145e37fce99f4c82a41960aed134	SideShift

Next Actions:

We can notify SideShift and Fixed Float Exchanges about the incident, providing them with the on-chain transaction details. Once they have this information, they will be able to block the address, preventing further damage.

---

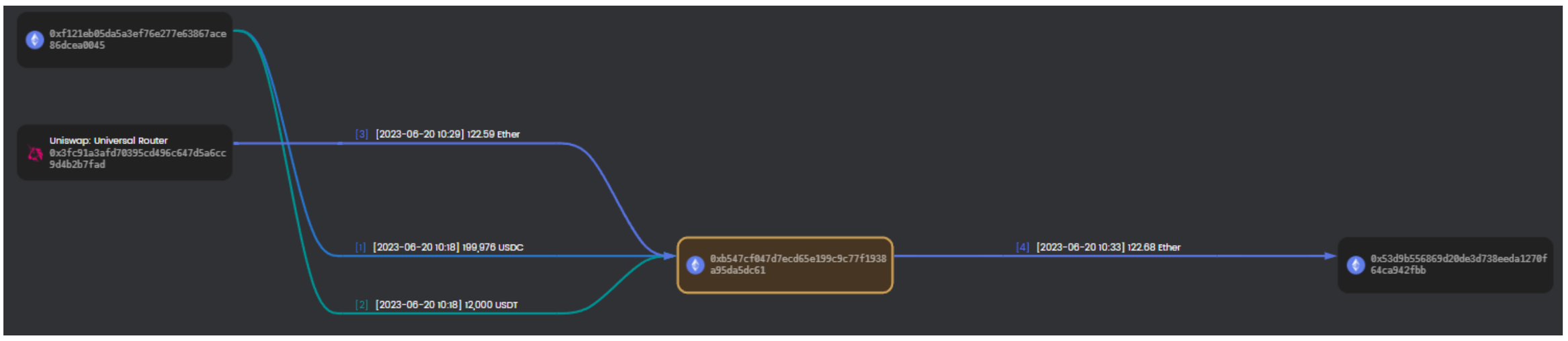
2. 0xb547CF047D7ecD65e199c9c77f1938a95da5dc61:

The attacker had transferred $211K to this address. Then he swapped the funds (12K USDT and 200K USDC) into 122.68 Ether (115.6 and 6.9 ETH) from UniswapV3 and transferred it to 0x53d9b556869d20de3d738eeda1270f64ca942fbb

Currently, the funds (122 Eth) sits at 0x53d9b556869d20de3d738eeda1270f64ca942fbb

We can Monitor the funds using the below link:

https://metasleuth.io/result/eth/0xb547CF047D7ecD65e199c9c77f1938a95da5dc61?source=fab3d7cd-3405-4cc9-916d-9d304c1d281c



Next Actions:

For this address, We can monitor the flow of funds using the above link. If the scammer send the funds to any exchange we can notify the particular exchange about the incident and they will block the funds, preventing further damages.

It is also advisable to collaborate with Chainalysis. They have a tool called Chainalysis Reactor, which is blockchain forensics software that connects cryptocurrency transactions to real-world entities. This tool maybe helpful to track down the person/entity behind the scam.More details here: https://www.chainalysis.com/chainalysis-reactor/

Notify blockchain explorers like Etherscan and web3 user defense platforms such as Web3Antivirus, revoke.cash, WalletGuard, etc. about the suspicious activities and involvement of this particular address in a scam. By flagging the address as malicious, the community will be able to identify and protect themselves from potential fraudulent activities associated with it

QuillAudits