

# Easyfi疑似私钥被盗事件

## 分析

本次攻击是以区块链上以窃取私钥为基础，以窃取用户资产为目的的攻击手段。

## 流程

EasyFi官方地址：0xbf126c7aab8aee364d1b74e37def83e80d75b303

中间地址：0x222def1dfeeaed8202491cdf534e4efff3268666

受害者1地址：0x0c08d0fe35515f191fc8f0811cadcf6b2615b74

受害者2地址：0xf59c2e9d4ab5736a1813738e5aa5c3f5eaf94d9e

1. 最初EasyFi项目的官方中间地址发送了8, 800, 000 EASY

<https://etherscan.io/tx/0x6141b4dfb3df85684329aaaf2d335bc1c1ede4c68c2054582f487825c5aa561e>

Transaction Details

Sponsored: Bybit: Trade \$100 & stand to Win 1 BTC!

Overview Logs (1) State Comments

Transaction Hash: 0x6141b4dfb3df85684329aaaf2d335bc1c1ede4c68c2054582f487825c5aa561e

Status: Success

Block: 10963363 3059552 Block Confirmations

Timestamp: 474 days 1 hr ago (Sep-30-2020 11:02:53 AM +UTC)

From: 0xbf126c7aab8aee364d1b74e37def83e80d75b303 (EasyFi: Deployer)

Interacted With (To): Contract 0x913d8ad7ce6986a8cbfee5a54725d9eea4f0729 (EasyFi: Old EASY Token)

Tokens Transferred: From EasyFi: Deplo... To 0x222def1dfeeaed... For 8,800,000 EASY (EASY)

2. 该中间地址分别向两个受害者地址发送2700000和2000000个EASY

<https://etherscan.io/tx/0x9375d202197e26c8de9e0ee76a3ec990111dbfd552f2224dce9dae40624d4ee6>

Overview Logs (1) State Comments

Transaction Hash: 0x9375d202197e26c8de9e0ee76a3ec990111dbfd552f2224dce9dae40624d4ee6

Status: Success

Block: 11014021 3008919 Block Confirmations

Timestamp: 466 days 3 hrs ago (Oct-08-2020 09:03:59 AM +UTC)

From: 0x222def1dfeeaed8202491cdf534e4efff3268666

Interacted With (To): Contract 0x913d8ad7ce6986a8cbfee5a54725d9eea4f0729 (EasyFi: Old EASY Token)

Tokens Transferred: From 0x222def1dfeeaed... To 0x0c08d0fe35515f... For 2,700,000 EASY (EASY)

Value: 0 Ether (\$0.00)

Transaction Fee: 0.003956712 Ether (\$12.85)

Gas Price: 0 nnnnnnnn76 Ether (76 Gwei)

Ether Price: This website uses cookies to improve your experience and has an updated Privacy Policy. Got It

<https://etherscan.io/tx/0xfeab6cdf637c0f40dbcb9d2f58a78b42cb6dd83d1a02d6a3362cd4b8fe2dcd8f>

Transaction Details

Sponsored: Decentar - Tory Lanez Just dropped his NFT! Mint a 3NITY! [Mint a 3NITY now!](#)

Overview

Logs (1)

State

Comments

Transaction Hash:

0xfeab6cdf637c0f40dbcb9d2f58a78b42cb6dd83d1a02d6a3362cd4b8fe2dcd8f

Status:

Success

Block:

110139883008954 Block Confirmations

Timestamp:

466 days 3 hrs ago (Oct-08-2020 08:57:11 AM +UTC)

From:

0x222def1dfeeaed8202491cdf534e4efff3268666

Interacted With (To):

Contract 0x913d8adf7ce6986a8cbfee5a54725d9eea4f0729 (EasyFi: Old EASY Token)

Tokens Transferred:

From 0x222def1dfeeaed...

To 0xf59c2e9d4ab57...

For 2,000,000

EASY (EASY)

Value:

0 Ether (\$0.00)

Transaction Fee:

This website uses cookies to improve your experience and has an updated Privacy Policy.

3. 在2021年4月19日，攻击者0x83a2eb63b6cc296529468afa85dbde4a469d8b37利用两个受害者账户向攻击者账户分别转了1,035,555.826203866010956193和1,799,990个EASY，通过检测合约，发现合约中的执行逻辑没有可以利用的漏洞，因此可以判定，这是一次因用户私钥或助记词泄露从而窃取用户虚拟资产的攻击。在完成攻击获取到大量EASY数字资产后，该攻击者接着在Uniswap中将EASY置换为USDC。

Transaction Action:

Swap 243.331404843552172077 EASY For 912.195765 USDC On Uniswap V2

Swap 756.668595156447827923 EASY For 0.905285101478328407 Ether On Uniswap V2

Swap 0.905285101478328407 Ether For 1,940.62645 USDC On Uniswap V2

From:

0x83a2eb63b6cc296529468afa85dbde4a469d8b37 (Easyfi Hacker)

Interacted With (To):

Contract 0xdef1c0ded9bec7f1a167081983240f027b25eff (0x: Exchange Proxy)

Tokens Transferred:

From Easyfi Hacker To Uniswap V2: EAS... For 243.331404843552172077 EASY (EASY)

From Uniswap V2: EAS... To Easyfi Hacker For 912.195765 USD Coin (USDC)

From Easyfi Hacker To Uniswap V2: EASY For 756.668595156447827923 EASY (EASY)

From Uniswap V2: EASY To Uniswap V2: USDC For 0.905285101478328407 (\$2,963.63) Wrapped Eth... (WETH)

From Uniswap V2: USDC To Easyfi Hacker For 1,940.62645 (\$1,940.63) USD Coin (USDC)

Value:

0 Ether (\$0.00)

结论

根据整个攻击过程的分析，根本原因在于攻击者可以利用被攻击者的账户地址调用合约，窃取受害者私钥授权合约执行并向攻击者地址进行大额数字资产的转账。

参考链接

<https://new.qq.com/omn/20210423/20210423A0B6HC00.html>