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

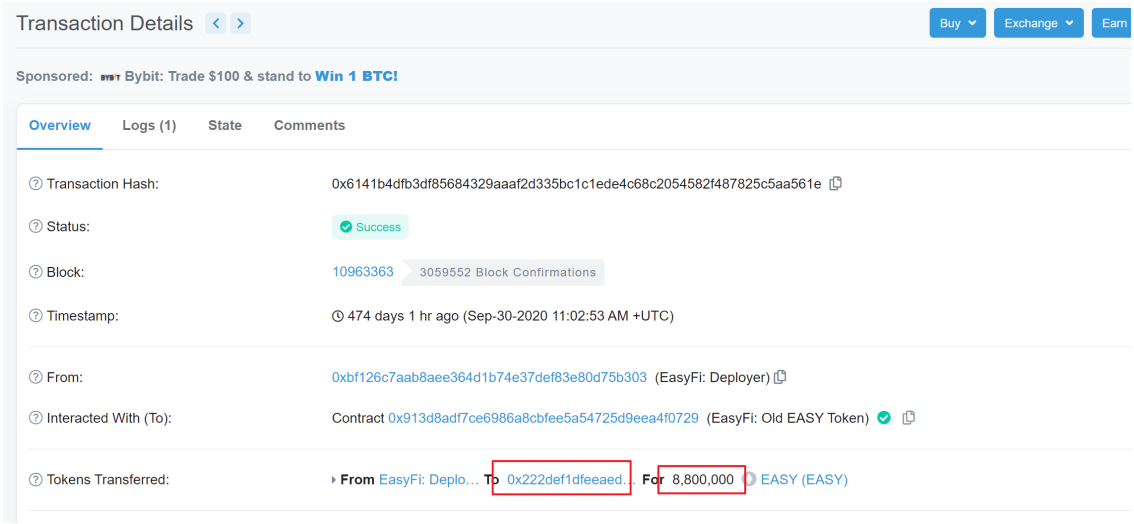
中间地址：0x222def1dfeeaed8202491cdf534e4efff3268666

受害者1地址：0x0c08d0fe35515f191fc8f0811cadcfc6b2615b74

受害者2地址：0xf59c2e9d4ab5736a1813738e5aa5c3f5eaf94d9e

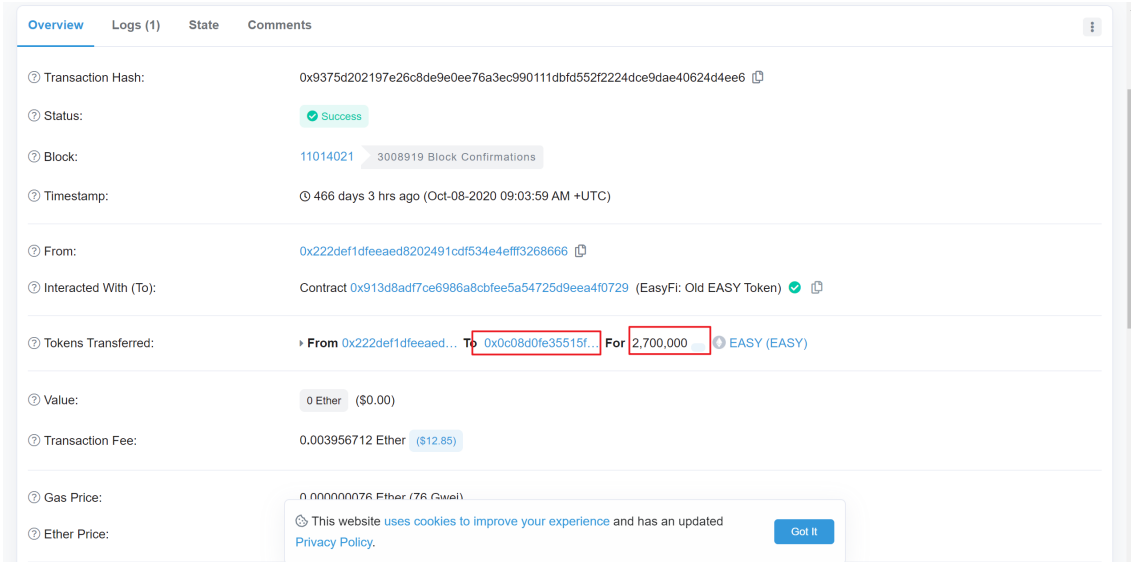
1. 最初EasyFi项目的官方向中间地址发送了8，800，000 EASY

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

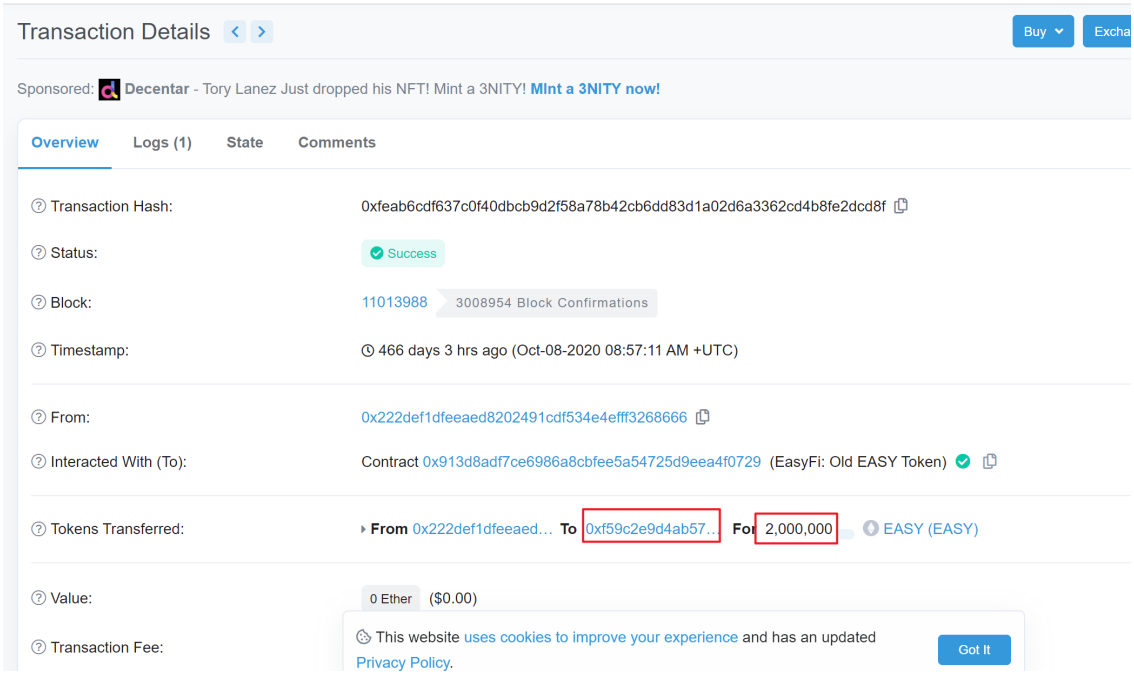


2. 该中间地址分别向两个受害者地址发送2700000和2000000个EASY

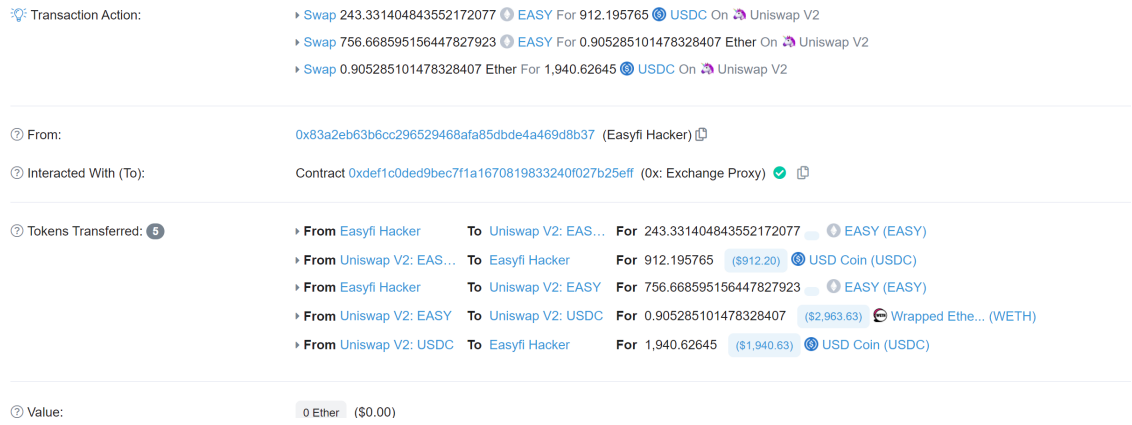
   https://etherscan.io/tx/0x9375d202197e26c8de9e0ee76a3ec990111dbfd552f2224dce9dae40624d4ee6



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



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。



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