BlockSec
Follow
Jan 2, 2021 · 4 min read · Listen

Security incident on Seal Finance

The BlockSec Team, Zhejiang University, China

On 30th Nov, our security incident monitoring system **ThunderForecast** discovered an attack on Loopring protocol (Blog in EN, CN) through scanning history transactions among the Ethereum. As a conclusion, the root cause of this attack is the lack of access control on the `sellTokenForLRC` function. The attacker took advantage of 80.97 ETH, which is equivalent to 48,849.2 USD based on the price at that time.

On 11th Dec 2020, our monitoring system **ThunderForecast** reported a series of transactions trading with an abnormal trade rate. Then, we used the EthScope system developed by our research team to analyze these transactions and discovered that this is an attack leveraging a vulnerability of Seal Finance Protocol for the arbitrage purpose.

What is Seal?

Mentioned at the Seal whitepaper: “SEAL — An experimental protocol that serves as an intermediary between major DeFi protocol tokens, creating deeper liquidity in between”. Up to now, there exist over 10 liquidity pools which hook Seal with other different well-known tokens(such as UNI, YFI, USDT, SNX and etc.). To earn the bonus, the investor needs to deposit LP tokens into the SEAL reward contract and trigger the `breed()` function in the contract `Farm` to produce new SEAL tokens. The `Farm` contract is deployed in every Seal pool and the function `breed()` in the contract is used to issue new Seal tokens. As the setting of `breed()`, it issues an additional 1.6% of Seal Token. Furthermore, 0.8% of issued Seal tokens are exchanged to another token which is deposited into the pool with the other 0.8% of issued Seal tokens as liquidity. However, since there is no access control designed for the `breed()` function, anyone can trigger this function and this primitive design becomes the root cause of this reported attack.

The following is the confirmed source code of function `breed()`:

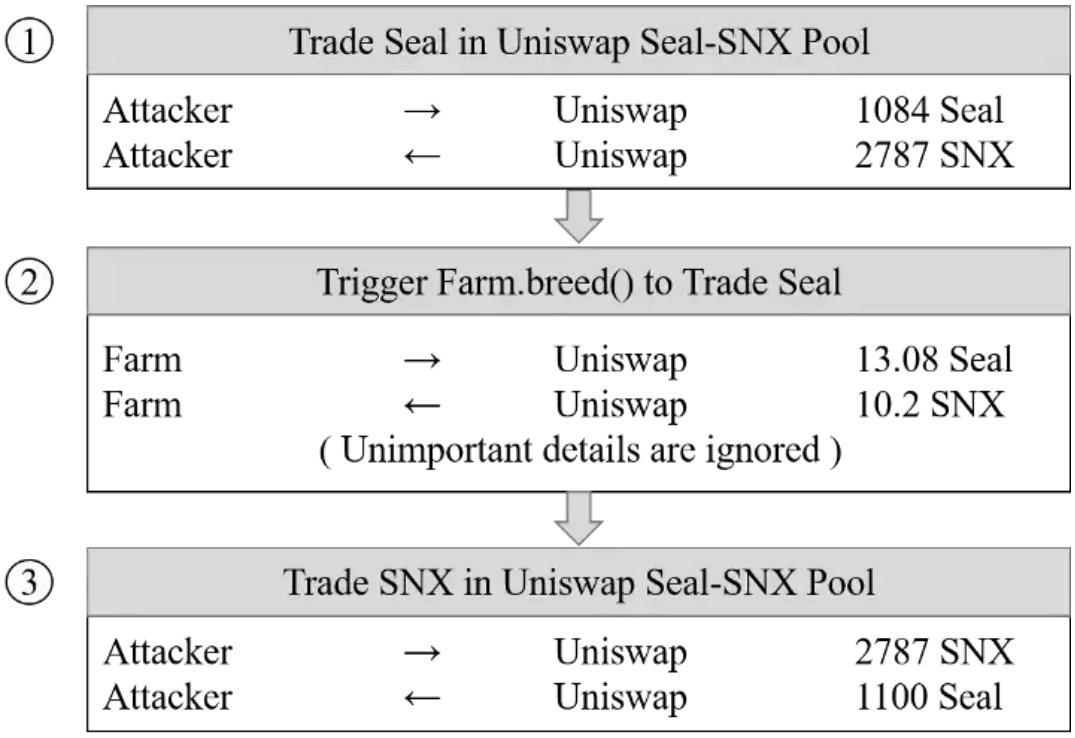
```
function breed() external {
    require(now / 1 days > today);
    today += 1;

    uint256 sealPairAmount = seal.balanceOf(address(cSeal));
    uint256 tokenPairAmount = token.balanceOf(address(cSeal));
    uint256 newSeal = sealPairAmount.mul(spawnRate).div(1e18);
    uint256 amount = UniswapV2Library.getAmountOut(newSeal, sealPairAmount, tokenPairAmount);

    seal.mint(address(cSeal), newSeal);
    if(address(seal) < address(token))
        cSeal.swap(0, amount, address(this), "");
    else
        cSeal.swap(amount, 0, address(this), "");
    token.transfer(address(cSeal), amount);
    seal.mint(address(cSeal), newSeal);
    cSeal.mint(address(this));
}
```

Details

We now start revealing more details of this attack with one attacking transaction. In this transaction, the attacker repeats the attacking logic for 10 Seal pools to maximize their profit. For the following analysis, we focus on the attack launched in the Seal-SNX pool.



There are three steps involved:

- Step 1: Swap **1,084 Seal** to **2,787 SNX** in the Seal-SNX pool. The trade rate is: **1 Seal = 2.57 SNX**.
- Step 2: Trigger `breed()` function in `Farm` contract. This function issues **13.08 Seal** and swaps it to **10.20 SNX**. The trade rate now is: **1 SNX = 0.78 Seal**. The reason is that most of the SNX in the pool is swapped to Seal and causes a huge difference between SNX and Seal in terms of the amount. Then, based on the price calculation algorithm of Uniswap, SNX becomes extremely valuable(price increases over 3 times) in the pool.
- Step 3: Swap **2787 SNX** to **1100 Seal** in the Seal-SNX pool. Since the exchange further increases the price of SNX, the attacker arb out more Seal tokens (extra **16 Seal**).

To further measure and confirm the loss, we replayed `breed()` function under the block status, which is before the attack, by using our system **EthScope**. As a result, `Farm` issued 18 additional Seal tokens compared to normal invocation. The attacker grabs out 16 Seal and only 2 Seal are left in the pool.

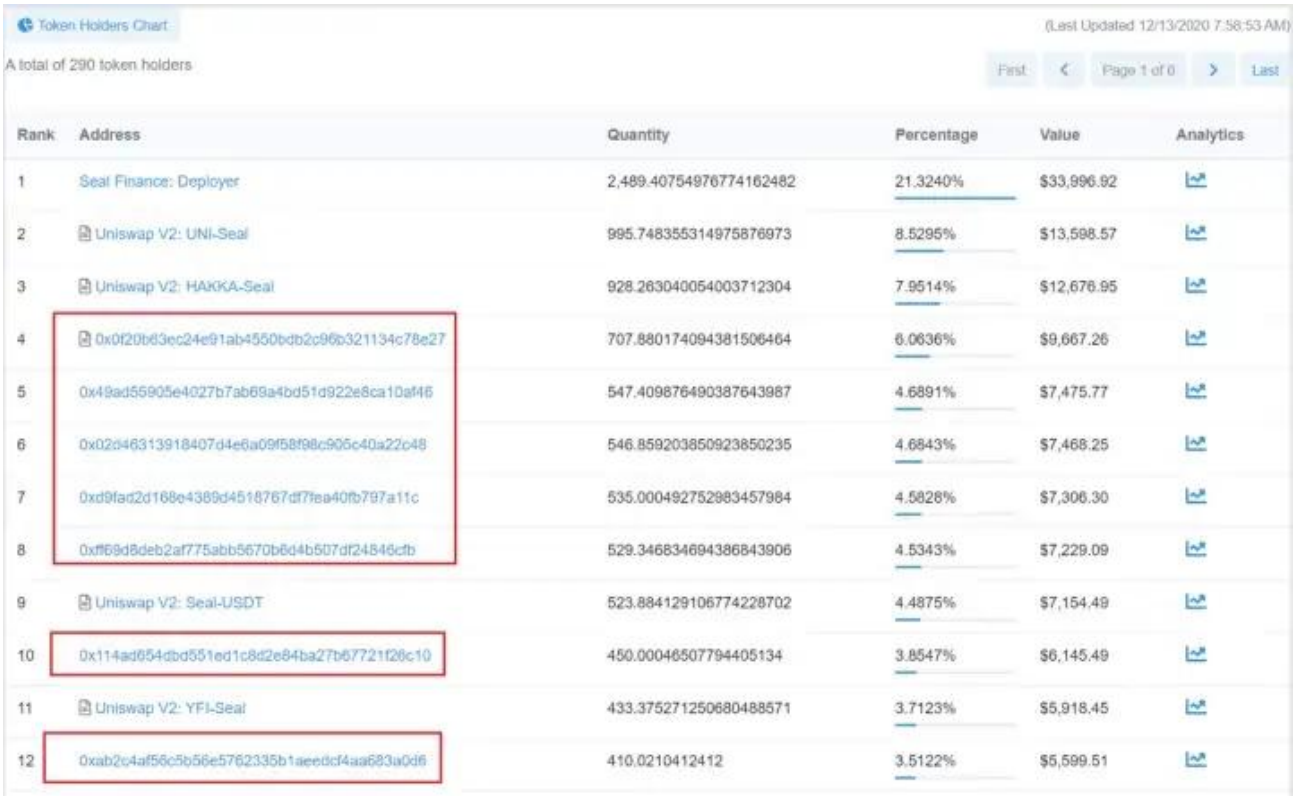
Gain & Loss

In this transaction, the attacker gains total of **175 Seal**.

The scale of the attack

Up to 13th December 2020, there are 3 malicious contracts(0x49f93e, 0x8b3710, 0x0f20b6) deployed on-chain and 22 transactions are successfully launched to rap **4,247** Seal tokens. Based on the price at the moment, the attacker earns about **58,467** USD through leveraging the vulnerability of Seal protocol. It is worth to mention that **the vulnerability of Seal protocol is still under the attack!!!**

Furthermore, through analysing the flow of gained Seal tokens, we discover that around 900 Seal tokens are deposited into DEX and the rest is distributed into 6 different addresses. As shown in the following figure, those addresses are all top holders of Seal tokens apart from Seal Finance and the liquidity pool in the Uniswap V2.



Token Holders Chart (Last Updated 12/13/2020 7:58:53 AM)

A total of 290 token holders

First < Page 1 of 0 > Last

Rank	Address	Quantity	Percentage	Value	Analytics
1	Seal Finance: Deployer	2,489.40754976774162482	21.3240%	$33,996.92	
2	Uniswap V2: UNI-Seal	995.74835531497587697 3	8.5295%	$13,598.57	
3	Uniswap V2: HAKKA-Seal	928.263040054003712304	7.9514%	$12,676.95	
4	0x0f20b6d3cc24e91ab4550bdb2c96b321134c78e27	707.880174094381506464	6.0636%	$9,667.26	
5	0x49ad55905e4027b7ab69a4bd51d922e8ca10af46	547.409876490387643987	4.6891%	$7,475.77	
6	0x02d46313918407d4e6a09f58f98c905c40a22c48	546.859203850923850235	4.6843%	$7,468.25	
7	0xd9fad2d168e4389d4518767df7fea40fb797a11c	535.000492752983457984	4.5828%	$7,306.30	
8	0xff69d8deb2af775abb5670b6d4b507df24846cfb	529.346834694386843906	4.5343%	$7,229.09	
9	Uniswap V2: Seal-USDT	523.884129106774228702	4.4875%	$7,154.49	
10	0x114ad654dbd551ed1c8d2e84ba27b67721f26c10	450.00046507794405134	3.8547%	$6,145.49	
11	Uniswap V2: YFI-Seal	433.375271250680488571	3.7123%	$5,918.45	
12	0xab2c4af56c5b56e5762335b1aeedcf4aa683a0d6	410.0210412412	3.5122%	$5,599.51	

The End

With the development of the DeFi eco-system in Ethereum, various security problems are gradually popping out. In fact, the root cause, which is **access control**, behind the attack causes a considerable loss (58,467USD) on Seal through launching 22 transactions up to 13th December 2020.

Update (2021/01/04)

After the first attack on 11/30, 2020, the attacker has deployed a third attack contract and launched five attacks. The last attack was on 12/24, 2020 and transferred the obtained Seal tokens to this address . During this process, the attacker obtained 6,021 Seal Tokens.

Timeline:

- 2020/12/11: Suspicious transactions were found
- 2020/12/12: Complete the analysis
- 2020/12/13: Reported to Seal Finance
- 2021/01/03: This blog is released
- 2021/01/03: CVE-2021–3006 is assigned

Defi Defiattack Security Blockchain Security Smart Contract Security