Case Study

- Formation.Fi flash loan security incident analysis

- Another flash loan price manipulation attack? : Welnance. finance Event Analysis

공유

- https://www.blockthreat.io/
  - 다양한 블록체인 보안 정보 요약
- https://cryptozombies.io/
  - Solidity를 이용한 좀비게임 개발 튜토리얼
- https://medium.com/coinmonks/programming-defi-uniswap-part-1-839ebe796c7b
  - Defi 개발(추후)

Crime

- DailyMail profile of Yevgeniy Polyanin, a wanted affiliate of the REvil ransomware group.
- FBI seized $2.3M in Bitcoin from affiliate of REvil, Gandcrab ransomware gangs.
- Italian couple arrested for installing cryptomining software on department store computers.

Hacks

- On November 30, 2021 MonoX lost $31M after a price calculation bug was exploited to manipulate the MONO token exchange rate.
- On November 30, 2021 0xHabitat team's Gnosis safe was compromised in a sophisticated phishing attack which led to a covert backdoor. $275K were lost in WETH, DAI, and HBT tokens.
- On December 2, 2021 BadgerDAO's Cloudflare account was compromise allowed attackers to inject malicious JavaScript snippet requesting token approvals. As a result, more than $120M in users' funds were stolen after visiting the compromised website with one account losing $50M in a single transaction.
- On December 4, 2021 Bitmart hot wallet was compromised which resulted in the loss of $200M worth of various crypto assets across multiple chains. Following the compromise attackers exchanged stolen tokens on 1inch exchange and mixed them using Tornado.Cash.

Vulnerabilities

- Bitclout fixed a double spending bug after it was responsibly disclosed by

공유

- Gmail/Github
  - bears.team.kr@gmail.com
  - 잠실!@34
- github + jekyll : Blog

Formation.Fi flash loan security incident analysis

개요

- 21년 11월 21일 Knownsec Blockchain Lab이 이더리움 상 DeFi 프로토콜인 Formation.Fi 에서 Flash Loan 공격 탐지
- 10만불 가량의 손해 발생

공격과정(1/3)

1. 0xd02c 로 시작하는 Contract로 200 USDT 예치

from UniswapV2Pair to 0xd02c260f54...4c20a6 200 Tether USD (USDT)

2. 100 USDT를 Vault에 맡기고(Deposit) 99 Formation USD 확보


```
"[FUNCTION]" : "deposit"
"[OPCODE]" : "CALL"
"from" : {
  "address" : "0xd02c260f54997146c9028b2ac7144b11ce4c20a6"
  "balance" : "88982805035852433758"
}
"to" : {
  "address" : "0xcb6afdc84e8949ddf49ab00b5b351a5b0f65a723"
  "balance" : "0"
}
"value" : "0"
"input" : {
  "_amount" : "100000000"
  "_recipient" : "0xd02c260f54997146c9028b2ac7144b11ce4c20a6"
}
"output" : {
  "0" : "99997695605728505820"
```

공격과정(2/3)

3. Vault Contract의 swapIn 함수를 큰 Fee로 호출


```
"[FUNCTION]" : "swapIn"
"[OPCODE]" : "CALL"
"from" : {
    "address" : "0xd02c260f54997146c9028b2ac7144b11ce4c20a6"
    "balance" : "88982805035852433758"
}
"to" : {
    "address" : "0xcb6afdc84e8949ddf49ab00b5b351a5b0f65a723"
    "balance" : "0"
}
"value" : "0"
"input" : {
    "account" : "0xd02c260f54997146c9028b2ac7144b11ce4c20a6"
    "amount" : "100000000"
    "fee" : "201402163916316"
}
```

공격과정(3/3)

4. Vault Contract의 withdraw 함수로 99 Formation USD에서 99999 USDT 확보!


```
"[FUNCTION]" : "withdraw"
"[OPCODE]" : "CALL"
"from" : {
    "address" : "0xd02c260f54997146c902
    "balance" : "0"
}
"value" : "0"
"input" : {
    "_amount" : "99997695605728505820"
    "_recipient" : "0xd02c260f54997146c
}
"output" : {
    "0" : "99997695605728505820"
```

```
"[FUNCTION]" : "transfer"
"[OPCODE]" : "CALL"
"from" : {
    "address" : "0xcb6afdc84e8949ddf49ab00b5b351a5b0f65a723"
    "balance" : "0"
}
"to" : {
    "address" : "0xdac17f958d2ee523a2206206994597c13d831ec7"
    "balance" : "1"
}
"value" : "0"
"input" : {
    "_to" : "0xd02c260f54997146c9028b2ac7144b11ce4c20a6"
    "_value" : "99999999652"
```

취약점 분석(1/2)

swapIn

```
function swapIn(
        address account,
        uint256 amount,
        uint256 fee
) external notLocked {
        require(amount >= _minAmountForSwap, "Should be bigger than minimum amount");
        require(fee >= txFee, "Fee should be greater than tx fee");
        token.safeTransferFrom(msg.sender, address(this), amount);
        uint256 redistribution = ((fee - txFee) * lpFee) / BASIS_POINT;

        totalTokens += (redistribution * (10**decimals)) / 10**token.decimals();
        treasuryAmount += fee - redistribution;

        emit SwapInProcessed(account, amount, fee);
}
```

* fee 값이 totalTokens 값에 영향을 줌

취약점 분석(2/2)

withdraw

```
function withdraw(uint256 _amount, address _recipient) external nonReentrant notLocked returns (uint256)
        // If _shares not specified, transfer full share balance
        uint256 shares = _amount;
        if (_amount == type(uint256).max) {
                shares = _balances[msg.sender];
        }

        // Limit to only the shares they own
        require(shares <= _balances[msg.sender], "Amount exceeds balance");

        // Ensure we are withdrawing something
        require(shares > 0, "Nothing to withdraw");

        uint256 tokensToTransfer = (shares * totalTokens) / totalSupply;
        totalSupply -= shares;
        _balances[msg.sender] -= shares;
        totalTokens -= tokensToTransfer;
        emit Transfer(msg.sender, address(0), shares);
        token.safeTransfer(_recipient, (tokensToTransfer * 10**token.decimals()) / (10**decimals));

        return shares;
```

* totalTokens 값이 실제 전송할 값에 영향을 줌

* USDT 의 decimals 값과 Formation USD decimal 값의 차이가 큼(6 vs 18)

Welnance. finance Event Analysis

개요

- 21년 11월 13일 Knownsec Blockchain Lab이 BSC(Binance Chain) 상 DeFi 프로토콜인 Welnance.Finance 에서 Flash Loan 공격 탐지

공격과정(1/2)

- 1,000,000 BUSD를 wbnB-bus로 부터 대출
- pancakeSwap에서 1,000,000 BUSD로 169,882 WEL로 구매

From	0x16b9a82891338…	To	0x96e28c2ffa1bbf…	For	1,000,000 ($1,010,000.00)		Binance-Peg ... (BSC-US...)
From	0x96e28c2ffa1bbf…	To	PancakeSwap V2:…	For	1,000,000 ($1,010,000.00)		Binance-Peg ... (BSC-US...)
From	PancakeSwap V2:…	To	0x96e28c2ffa1bbf…	For	169,882.169378306740578468		Welnance Coi... (WEL)

- 80 WEL로 4,056 wlWEL 변환
- wlUSDT로 부터 8,651BUSD, wlBTC로 부터 0.06BTC, wlETH로 부터 0.7 ETH 대출

From	0x723dca315dcea…	To	0x96e28c2ffa1bbf…	For	4,056.67574453		WEL Pack coi... (wlWEL)
From	0x781d0d50ae368…	To	0x96e28c2ffa1bbf…	For	8,651 ($8,737.51)		Binance-Peg ... (BSC-US...)
From	0xadbbcad6d68a5…	To	0x96e28c2ffa1bbf…	For	0.06 ($2,912.19)		Binance-Peg ... (BTCB)
From	0x3e18d5d225c25…	To	0x96e28c2ffa1bbf…	For	0.7 ($2,772.52)		Binance-Peg ... (ETH)

공격과정(2/2)

- 남은 169,802 WEL로 999,893 BUSD로 변환, 대출한 8,651 BUSD와 합쳐 1,000,000 BUSD를 상환

From 0x96e28c2ffa1bbf…	To PancakeSwap V2:…	For 169,802.169378306740578468	Welnance Coi... (WEL)
From PancakeSwap V2:…	To 0x96e28c2ffa1bbf…	For 999,893.35774469076614121 ($1,009,892.29)	Binance-Peg ... (BSC-US...)
From 0x96e28c2ffa1bbf…	To 0x16b9a82891338…	For 1,002,550 ($1,012,575.50)	Binance-Peg ... (BSC-US...)

- 남은 5,994 BUSD, 0.7 ETH, 0.06 BTC를 공격자 주소로 전송

From 0x96e28c2ffa1bbf…	To 0xa6516b0fc4e98…	For 5,994.35774469076614121 ($6,054.30)	Binance-Peg ... (BSC-US...)
From 0x96e28c2ffa1bbf…	To 0xa6516b0fc4e98…	For 0.7 ($2,772.52)	Binance-Peg ... (ETH)
From 0x96e28c2ffa1bbf…	To 0xa6516b0fc4e98…	For 0.06 ($2,912.19)	Binance-Peg ... (BTCB)

취약점 분석(1/2)

- wlXXX pool에서 대출시 borrowAllowed 함수를 호출
  - 대출 조건이 valid한지 확인
  - wlWEL 값을 담보로 지정
- borrowAllowed 함수 내부적으로 getHypothetical~ 함수 호출
  - 사용자 담보물이 대출 금액보다 큰 지 확인

취약점 분석(2/2)

- 처음 단계에서 매우 큰 금액의 BUSD로 WEL 구매 -> WEL 가격 상승 -> wlWEL 가격 급등
- 이를 담보로 wlBTC, wlETH, wlUSDT를 대출
- 남은 WEL로 다시 BUSD 상환

- 담보의 가치를 쉽게 조작할 수 있는 문제!

Reference

- https://medium.com/@Knownsec_Blockchain_Lab/knownsec-blockchain-lab-formation-fi-flash-loan-security-incident-analysis-8a24555f8356
- https://medium.com/@Knownsec_Blockchain_Lab/knownsec-blockchain-lab-another-flash-loan-price-manipulation-attack-65620364f5f9
- https://bscscan.com/tx/0xf7a9c59953763a57f412b2e45455e70192b44356c602f7c79ddbfa9cb05f440b
-