

# DeFi 보안 취약점 최신 사례 연구

위험에 빠진 DeFi, 우리가 구해보자!

# Who am I?



**Juno Im**

Security Researcher / Engineer



Theori, Security Researcher





- 2018 ~
- Currently, leading Web3 security



Bounty Hunter 

- Ethereum, Pancake Swap, Google ...

Ethereum Project  
Bug Bounty Leaderboard

1		Sam Sun 35000 points
2		Martin Holst Swende 33500 points
3		ChainSecurity 21000 points
4		Juno Im 20500 points



New postmortem!

Whitehat [@junorouse](#) found a critical bug in [@PancakeSwap](#)'s lottery contract, which also affected [@PantherSwap](#), [@ape\\_swap](#), and [@KnightsBsc](#).

PancakeSwap paid out a big \$70,000 bug bounty.

Immunefi led the disclosure process. Funds safu.

# Agenda

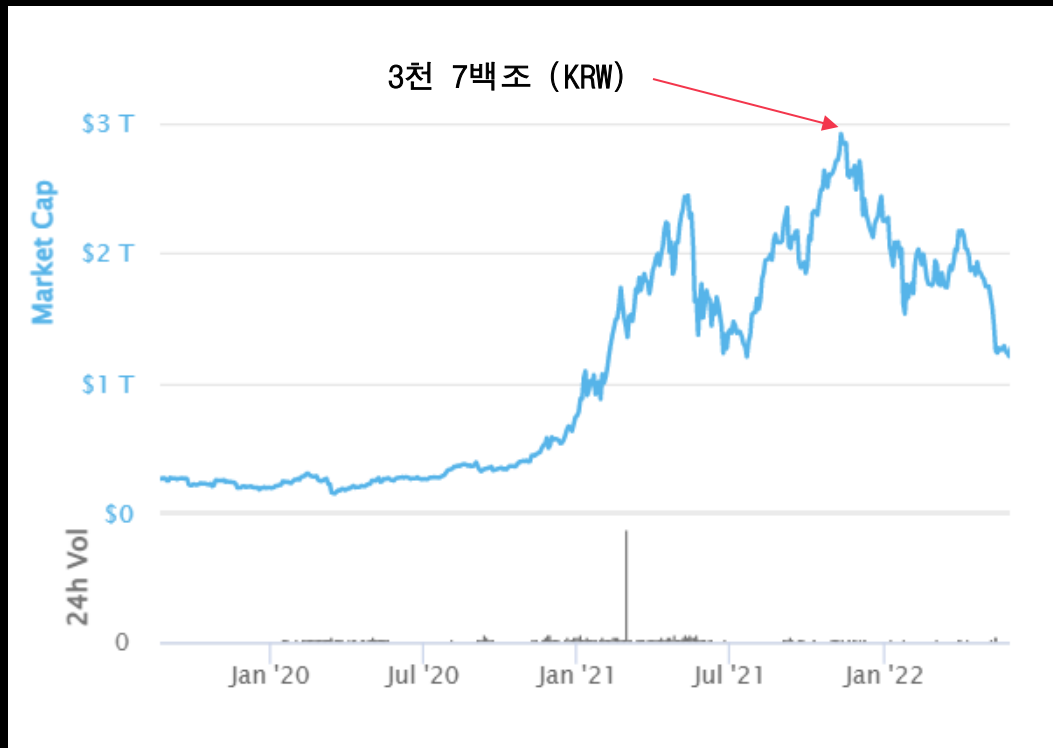
- 1 DeFi and Cybersecurity
- 2 Case Studies
- 3 What should we do, then?
- 4 Conclusion

# 1. DeFi and Cybersecurity

- DeFi 보안 왜 중요할까?
- 해커들의 타깃이 되는 이유
- DeFi 보안 사고 동향

## 1. DeFi and Cybersecurity

# DeFi 보안 왜 중요할까?



- Simple Answer:
  - To protect customer's asset from an adversary
- 한 번 사고가 발생하면 DeFi가 구동되고 있는, 탈중앙화 블록체인 특성상 "Roll-back"이 힘들 (불가능하진 않음, e.g., Ethereum Classic)
- 금전적 피해 → 보상이 가능한 규모여도, Trust Issue로 인해 사람들이 해당 프로젝트를 기피하게 됨. (경쟁력 상실)
  - But... Who cares?

## 1. DeFi and Cybersecurity

# 해커들의 타깃이 되는 이유

- DeFi 시장 규모 성장 \$\$\$
- 코드 변경이 활발하게 이루어져서 취약점이 발생할 가능성이 많음
- 공격에 쓰이는 cost 대비 return 매우 높음
- DeFi 특성상 해킹 사고 발생 이후 사고조사가 어려움
- 현금화가 매우 간편, 기존은 각종 규제에 의해 막힐 가능성이 높음 (Centralized)
- Dark coin 세탁 (Tornado cash / monero / zcash 등)

### U.S. officials link North Korean hackers to \$615 million cryptocurrency heist

PUBLISHED FRI, APR 15 2022 7:10 AM EDT

<https://www.cnn.com/2022/04/15/ronin-hack-north-korea-linked-to-615-million-crypto-heist-us-says.html>

According to researchers, the identified wallet contains funds related to an attack on the Ronin Network, in which more than \$600 million in digital assets was stolen.

## 1. DeFi and Cybersecurity

# DeFi 보안 사고 동향

1. **Ronin Network** - REKT *Unaudited*

\$624,000,000 | 03/23/2022

2. **Poly Network** - REKT *Unaudited*

\$611,000,000 | 08/10/2021

3. **Wormhole** - REKT *Neodyme*

\$326,000,000 | 02/02/2022

4. **BitMart** - REKT *N/A*

\$196,000,000 | 12/04/2021

5. **Beanstalk** - REKT *Unaudited*

\$181,000,000 | 04/17/2022

6. **Compound** - REKT *Unaudited*

\$147,000,000 | 09/29/2021

- Rekt.news가 제공하는 리더보드
  - Wrecked, 공격당한 Web3 Product를 모아 둔 매거진
- 1~3 위: **Cross-chain bridge** 해킹
- 4위: 거래소 해킹
- 5~6 위: 막대한 자금이 필요한 공격을, **Flash-loan** 기능을 통해 수행
- **모두 2021 하반기 - 2022 상반기에 발생**

## 2. Case Studies

- Smart contract 해킹
- Cross-chain bridge 해킹
- 전통적 Web2 취약점으로 인한 공격



## 2. Case Studies

# Smart contract 해킹 – Cream Finance

› Swap 1,873.933802532388653625 Ether For 7,453,002.766252 USDC On Uniswap V3

› Flash Loan 524,102.159298234706604104 Ether From Aave Protocol V2

› Swap 6,360,562.839915 USDC For 6,356,534.901208345789354257 DAI On Uniswap V3

0x24354d31bc9d90f62fe5f2454709c32049cf866b (Cream Finance Flash Loan Exploiter)

Contract 0x961d2b694d9097f35cfff363ef98823928a330d (Cream Finance Exploiter 3)

TRANSFER 518,102.159298234706604104 Ether From Wrapped Ether To 0xf701426b8126bc60530574ce...

TRANSFER 518,102.159298234706604104 Ether From 0xf701426b8126bc60530574ce... To Cream.Finance: crETH ...

TRANSFER 523,208.004849938820371764 Ether From Cream.Finance: crETH ... To Cream Finance Exploite...

TRANSFER 523,208.004849938820371764 Ether From Cream Finance Exploite... To Wrapped Ether

TRANSFER 2,760.219805803313878092 Ether From Wrapped Ether To Cream Finance Exploite...

TRANSFER 2,760.219805803313878092 Ether From Cream Finance Exploite... To Cream Finance Flash L...

› From Null Address: 0x00... To Cream Finance Ex... For 500,000,000 (\$499,083,000.00) Dai Stableco... (DAI)

› From Cream Finance Ex... To yearn: yDAI Token For 500,000,000 (\$499,083,000.00) Dai Stableco... (DAI)

› From Null Address: 0x00... To Cream Finance Ex... For 451,065,927.891934141488397224 learn DAI (yDAI)

› From Cream Finance Ex... To Curve.fi: y Swap For 451,065,927.891934141488397224 learn DAI (yDAI)

› From Cream Finance Ex... To Curve.fi: y Swap For 0 learn USDC (yUSDC)

› From Cream Finance Ex... To Curve.fi: y Swap For 0 learn USDT (yUSDT)

› From Cream Finance Ex... To Curve.fi: y Swap For 0 learn TUSD (yTUSD)

› From Null Address: 0x00... To Cream Finance Ex... For 447,202,022.713276945512955672 (\$509,810,305.89) Cu

› From Null Address: 0x00... To Cream Finance Ex... For 446,756,774.416766306389278551 Curve Y Pool... (yUSD

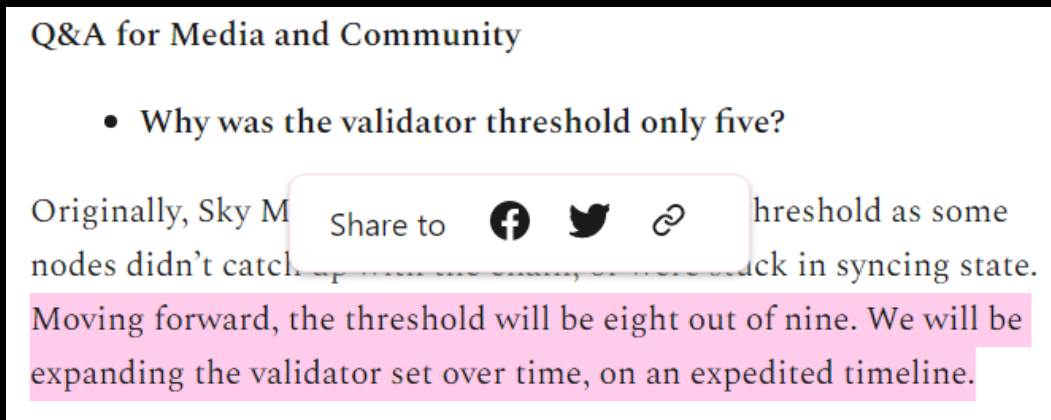
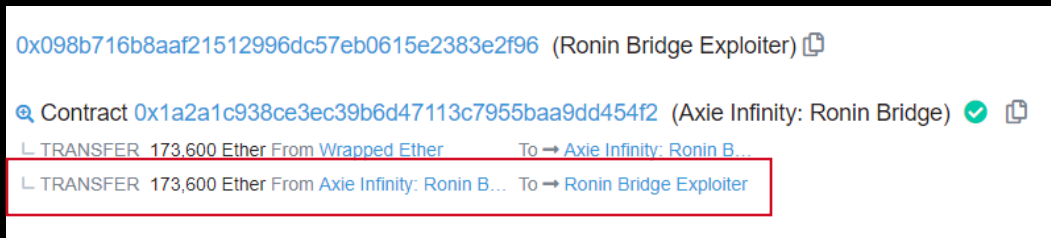
› From Cream Finance Ex... To 0x4b5bfd5212478... For 447,202,022.713276945512955672 (\$509,810,305.89) Cu

- 2021년 10월, 렌딩 프로토콜 Cream Finance가 두번째 공격을 받음
- \$130M (~= 1천6백억 원) 피해
- Flash-loan을 이용해 큰 자금이 있어야만 수행 가능한 로직을 실행 함
- 담보물의 가격을 조작해, 실제 담보금의 가치를 1.5배 부풀림
- 부풀려진 담보금을 바탕으로 Cream Finance의 모든 자산을 대출

<https://rekt.news/cream-rekt-2/>

## 2. Case Studies

# Cross-chain bridge 해킹 – Ronin Network Bridge



- 2022년 03월 23일, 사상 최대의 Web3 해킹. P2E side-chain Ronin Bridge가 공격 당함
- \$624M (~= 7천억 원) 피해
- Ronin: "We discovered the attack this morning after a report from a user being unable to withdraw 5k ETH from the bridge."
- Ronin의 대처 수준이 모두를 놀라게 함
  1. 6일 동안 해당 공격을 인지하지 못함.
  2. Threshold: 5 of 9을 8 of 9으로 변경.
  3. 추후 오픈한 버그바운티의 상금이 자산 규모에 비해 소규모 (~ N만 달러)

<https://roninblockchain.substack.com/p/community-alert-ronin-validators?s=r>

## 2. Case Studies

# 전통적 Web2 취약점으로 인한 공격 - BadgerDAO

At this time, Badger believes that, as publicly reported, the phishing incident that occurred on 2 Dec, 2021 was the result of a maliciously injected snippet provided by **Cloudflare Workers**. Cloudflare Workers is an interface to run scripts that operate on and alter web traffic as it flows through Cloudflare proxies. The attacker deployed the worker script via a compromised API key that was created without the knowledge or authorization of Badger engineers. The attacker(s) used this API access to periodically inject malicious code into the Badger application such that it only affected a subset of the user base.

🕒 129 days 13 hrs ago (Dec-02-2021 12:00:23 AM +UTC) | ⏱ Confirmed within 5 secs

0x1fcd04d0c5364fbd92c73ca8af9baa72c269107 (BadgerDAO Exploiter) 📄

Contract 0x4b92d19c11435614cd49af1b589001b7c08cd4d5 ✅ 📄

▶ From 0x53461e4fddcc1... To BadgerDAO Exploi... For 896.85987522 ⚙ Badger WBTC ... (byvWBT...)

- 2021년 12월 말, Bitcoin을 Ethereum 체인에 유동화해주는, BadgerDAO가 공격 당함
- \$120M (1천5백억 원) 피해
- 공격자는 탈취된 Cloudflare API키를 사용해 악성 스크립트를 삽입 함
- BadgerDAO 방문자가 공격자가 의도한 행위 (공격자 주소에 토큰을 Infinity Approve)를 요청
- 교묘한 수법으로 탐지를 우회, 충분한 자금이 모인 후 transferFrom 함수 호출

<https://badger.com/technical-post-mortem>

### 3. What should we do, then?

- 존재하는 취약점 사전 제거
- 빠른 공격 시도 탐지
- 지속적 보안 기법 연구

3. What should we do, then?

## 존재하는 취약점 사전 제거

- 공격자보다 앞서서, 존재하는 취약점 제거
- **Security Audit**
  - 대상 프로젝트에 존재하는 위협 식별, 취약점 탐지, 대책 수립 (패치 및 Defense-in-Depth 관점의 권고 사항 제공)
  - 대부분 Manual Audit 방식으로 진행 (시간이 오래 걸림)
  - Smart Contract, Node, DApp, Tokenomics, Infrastructure ...
  - Audit Firms: Trail of Bits, OpenZeppelin, Theori

3. What should we do, then?

## 존재하는 취약점 사전 제거

- **Static Analysis / Formal Verification**

- Manual Audit 방식으로 인한 시간 한계점을 극복하기 위해 자동화 취약점 분석 기술 등장
- 인간 대신 기계가 자동으로 취약점을 찾음
- 기존 Web2에서 Complexity 문제로 Practical하지 못했던 기술을 사용하기 시작함
- Companies: CertiK, Certora

- **Bug Bounty**

- 취약점을 찾아오는 WhiteHat 해커에게 포상금을 지급하는 방식
- 불분명한 신원에게 프로젝트를 공개해야 하는 위험성 존재 (보통 Security Audit이 선행되어야 함)
- Platforms: Immunefi, Code4rena, PatchDay

3. What should we do, then?

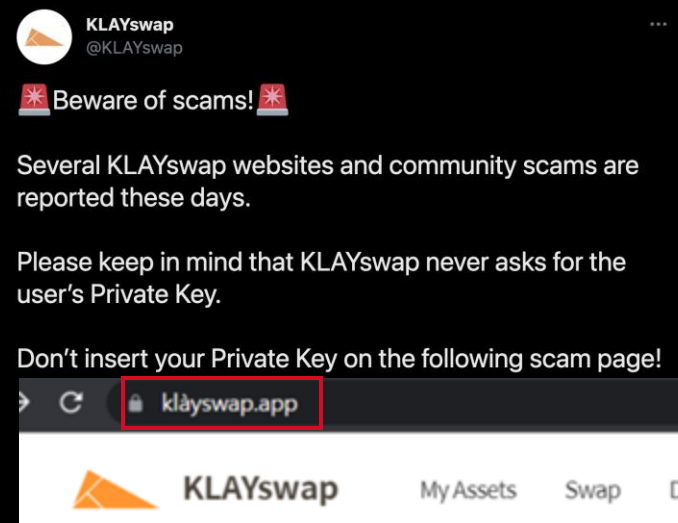
## 빠른 공격 시도 탐지

- 공격을 사전에 예방할 수 없다면, 빠르게 탐지해서 방어라도 해야함.
- 지속적인 On-chain monitoring을 통해 공격 시도 탐지
- i.e., 공격자들의 공격 패턴 학습
  1. 공격자들은, 실제 공격을 진행하기 전, 공격을 수행하는 스마트 컨트랙트를 메인넷에 배포
  2. 배포된 버전을 fork한 로컬 노드에서 테스트
  3. 실제 공격 수행
- 공격 시도 탐지 Idea:
  - 컨트랙트 배포시, EVM 바이트코드를 분석
  - 분석 결과 공격 시도 컨트랙트라면, 빠르게 서비스 운영자에게 고지 후 일시 정지

3. What should we do, then?

## 지속적 보안 기법 연구

- **Phishing detection** 방법 연구
  - 유사 도메인 탐지, 검색 엔진 크롤링 → 노티
- **Exploit mitigation** 적용
  - Sub Resource Integrity, Content-Security-Policy
    - To mitigate: Front-end asset hack, Client-side exploit (XSS, CSRF, ...)
  - Certification Authority Authorization (CAA) record
    - To mitigate: BGP Hijack
  - Control-flow-integrity, Sandboxing, ...
    - To mitigate: Exploit the node or webserver itself.





## 4. Conclusion

- Talk recap

## 4. Conclusion

# Talk recap

- 공격은 계속 증가하고 있고, 더욱 복잡하고 규모도 커질 것
- 과거 공격 사례에서 배우고 적극적으로 적용하고 있음
- 더 많은 Web3 프로젝트들이 효과적으로 audit 받을 수 있는 방법 필요
  - Web3의 폭발적 성장에 비해 블록체인 보안/audit 회사가 부족
- 일단, 할 수 있는 활동을 통해 보안 강화 필요
  - 취약점 제거 (Security audit, **Static Analysis / Formal Verification, Bug bounty**)
  - 공격 탐지 (On-chain monitoring, etc.)
  - 보안 연구 내용 활용 (**Phishing detection 연구, Exploit mitigation 적용**)

# Questions?

- **Interested in Web3 Cybersecurity? We are hiring!**
  - **<https://theori.team/>**
- **juno@theori.io // fb.com/imjuno99**