

Course IV:

DeFi Risks and Opportunities

1. Smart Contract Risk

(iii) Dforce, Yearn.finance

Risks: Smart contract risk

Risk events

Hackers just tapped China's dForce for \$25 million in Ethereum exploit

A known ERC777 vulnerability led to an attack that drained a huge chunk of coin from dForce. The same attack also drained around \$300,000 from a Uniswap pool.

By Andrew Hayward and Robert Stevens

3 min read • Apr 19, 2020 ★

Risks: Smart contract risk

Risk events: DForce

- [“DForce](#), a Chinese decentralized finance protocol, today lost \$25 million worth of its customers’ cryptocurrency due to a well-known exploit of an Ethereum token.
- The money was drained this morning from the contracts of Lendf.Me, a lending protocol that’s part of dForce, a collection of DeFi protocols.
- The site for Lendf.Me is now offline and its smart contracts have been paused. The funds were sent to DeFi lending protocols Compound and Aave. [Stani Kulechov](#), founder and CEO of Aave, told *Decrypt* that around \$10 million of the funds were sent to his protocol.”

Risks: Smart contract risk

Risk events: DForce

- The hack is linked to a well-known Ethereum exploit that was yesterday used to drain more than \$300,000 from decentralized exchange Uniswap.
- Uniswap smart contracts containing [imBTC](#)—an Ethereum-based, tokenized version of Bitcoin that's run by Tokenlon—were drained. Lendf.Me integrated imBTC in January.

Risks: Smart contract risk

Risk events: DForce

- The Uniswap attack took advantage of a known vulnerability that concerns the ERC777 token standard.
- Due to the way Uniswap smart contracts are set up, a hacker could continually withdraw ERC777 funds from Uniswap before the balance updated, gradually draining the contracts of imBTC.
- The dForce hack, though entirely separate from the Uniswap hack, is suspected to use the same exploit.

Risks: Smart contract risk

Risk events: DForce

- In a bizarre twist, the hackers returned \$126,014 back to Lendf.Me with a note saying, "Better luck next time," [according](#) to *Chain News*.



The smart contract for dForce was drained. (Source: DeFiPulse)

Risks: Smart contract risk

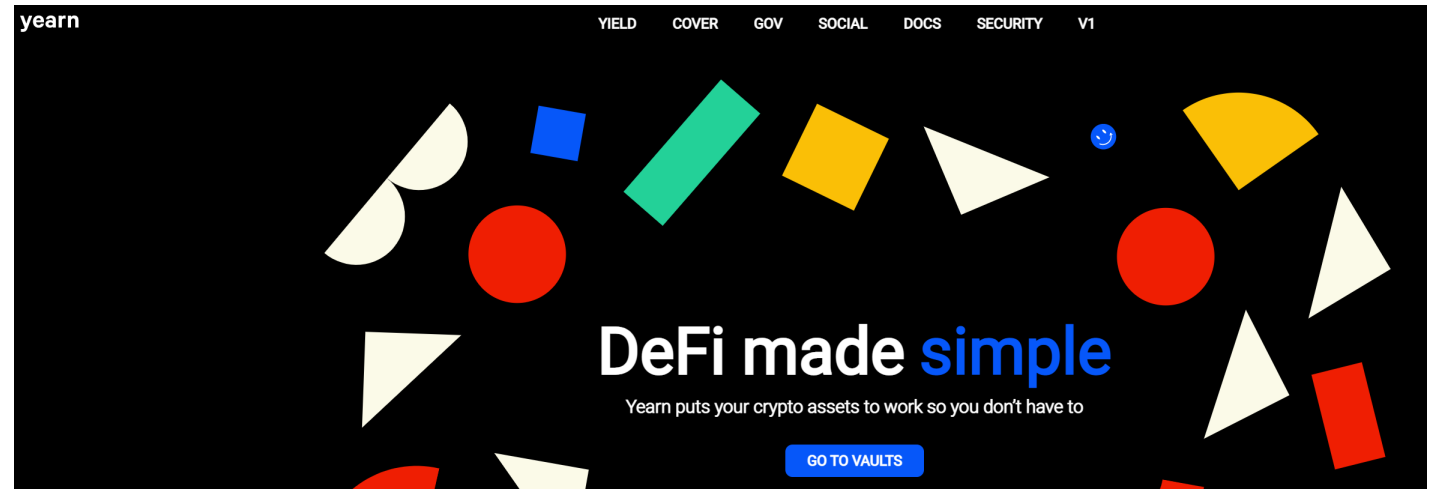
Risk events: DForce

- “Robert Leshner, the CEO of Compound, claims that Lendf.Me had appropriated its code, which was open-source.
- A [report](#) from *The Block* in January found that the term “Compound” appeared four times in dForce's contract.
- “If a project doesn't have the expertise to develop its own smart contracts, and instead steals and redeploys somebody else's copyrighted code, it's a sign that they don't have the capacity or intention to consider security,” tweeted Leshner.”

Risks: Smart contract risk

Yearn.finance

- “Yearn.Finance is a so-called yield aggregator, through which users can deposit funds in pools — or vaults — which are then deployed to other DeFi protocols in an effort to generate yields for those depositors.



Yearn Finance suffers exploit, says \$2.8 million stolen by attacker out of \$11 million loss



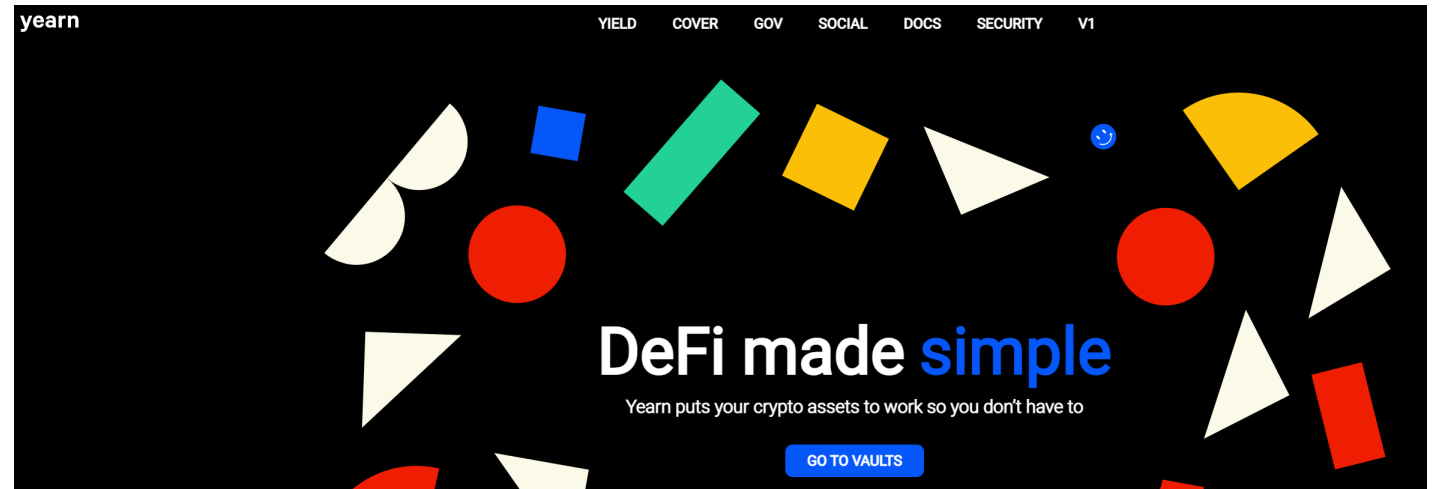
by Michael McSweeney

February 4, 2021, 5:38PM EST · 1 min read

Risks: Smart contract risk

Yearn.finance

- “Stani Kulechov, the founder of DeFi platform Aave, later tweeted out [the transaction](#) at the heart of the exploit, involving numerous DeFi protocols and more than \$5,000 worth of ETH-denominated gas fees.”
- Complex exploit with over 160 nested transactions



Yearn Finance suffers exploit, says \$2.8 million stolen by attacker out of \$11 million loss



by Michael McSweeney

February 4, 2021, 5:38PM EST · 1 min read

Risks: Smart contract risk



Eth: \$1,709.17 (+5.00%) | 168 Gwei

All Filters ▾


Search by Address / Txn Hash

Home

Blockchain ▾

Tokens ▾

Transaction Details

Sponsored:  - AAX - Predict the BTC Price and earn up to 1000 USDT Free. Visit [AAX.com](https://aax.com) now!

Overview

Internal Txns

Logs (254)

State

Comments

Transaction Hash: 0x6dc268706818d1e6503739950abc5ba2211fc6b451e54244da7b1e226b12e027 

Status: ✓ Success

Block: 11792334 6666 Block Confirmations

Timestamp: 1 day 49 mins ago (Feb-04-2021 09:49:07 PM +UTC) | Confirmed within 31 secs

From: 0x14ec0cd2acee4ce37260b925f74648127a889a28 (Yearn (yDai) Exploiter) 

Risks: Smart contract risk

\$200m Flash loan – with no collateral

🔍 Interacted With (To):

🔍 Contract [0x62494b3ed9663334e57f23532155ea0575c487c5](#) ✓

↳ TRANSFER 215,035.171940600397346616 Ether From [Wrapped Ether](#) To → [0x62494b3ed9663334e57f23...](#)

↳ TRANSFER 215,035.171940600397346616 Ether From [0x62494b3ed9663334e57f23...](#) To → [Compound Ether](#)

↳ TRANSFER 215,035.171940600397346616 Ether From [Compound Ether](#) To → [0x62494b3ed9663334e57f23...](#)

↳ TRANSFER 215,030.171940600397346616 Ether From [0x62494b3ed9663334e57f23...](#) To → [Wrapped Ether](#)

↳ TRANSFER 5 Ether From [0x62494b3ed9663334e57f23...](#) To → [Yearn \(yDai\) Exploiter](#)

💡 Transaction Action:

- ▶ Borrow 116,920.396944223800915079 Ether From dYdX
- ▶ Supply 215,035.171940600397346616 Ether To Compound
- ▶ Borrow 126,945,116.6393679705276416 DAI From Compound
- ▶ Borrow 134,000,000 USDC From Compound
- ▶ Repay 126,945,116.6393679705276416 DAI To Compound
- ▶ Repay 134,000,000 USDC To Compound
- ▶ Withdraw 215,035.171940600397346616 Ether From Compound
- ▶ Swap 153,258.252632 USDT For 93.30329749673893679 Ether On Uniswap
- ▶ Flash Loan 98,114.774996376596431537 Ether From Aave Protocol V2
- ▶ Repay 116,920.396944223800915081 Ether To dYdX

Risks: Smart contract risk

🔍 Tokens Transferred: 161

161 token transfers. Just displaying the first 10.

▶ From dYdX: Solo Margin	To 0x62494b3ed96633...	For 116,920.396944223800915079 (\$202,217,334.13)	🌐 Wrapped Ethe... (WETH)
▶ From Aave: aWETH Toke...	To 0x62494b3ed96633...	For 98,114.774996376596431537 (\$169,692,446.80)	🌐 Wrapped Ethe... (WETH)
▶ From Compound Ether	To 0x62494b3ed96633...	For 10,733,973.29750223 (\$368,389,963.57)	🌐 Compound Eth... (cETH)
▶ From Compound Dai	To 0x62494b3ed96633...	For 126,945,116.6393679705276416 (\$126,945,116.64)	🌐 Dai Stableco... (DAI)
▶ From Compound USD Coin	To 0x62494b3ed96633...	For 134,000,000 (\$134,000,000.00)	🌐 USD Coin (USDC)
▶ From 0x62494b3ed96633...	To Curve.fi: DAI/USDC/...	For 33,930,282.286591266737094656 (\$33,930,282.29)	🌐 Dai Stableco... (DAI)
▶ From 0x62494b3ed96633...	To Curve.fi: DAI/USDC/...	For 134,000,000 (\$134,000,000.00)	🌐 USD Coin (USDC)
▶ From 0x0000000000000000...	To 0x62494b3ed96633...	For 165,737,119.612224186410140871	🌐 Curve.fi DAI... (3Crv)
▶ From 0x62494b3ed96633...	To 0x0000000000000000...	For 164,762,431.868951093225613357	🌐 Curve.fi DAI... (3Crv)
▶ From Curve.fi: DAI/USDC/...	To 0x62494b3ed96633...	For 163,753,457.777563 (\$163,753,457.78)	🌐 Tether USD (USDT)
▶ From 0x62494b3ed96633...	To 0xacd43e627e6435...	For 93,014,834.352776703790546945 (\$93,014,834.35)	🌐 Dai Stableco... (DAI)

Scroll for more ▼

Risks: Smart contract risk: Rug pull

Mechanics

- A new token, TKN, is launched on a DEX
- It comes with a very high reward for offering liquidity (high interest rate)
- Retail investors are attracted and offer liquidity (contribute ETH and TKN to the liquidity pool)
- Once the pool is large enough, the original developers (who hold a lot of TKN, sell everything on the DEX causing price of TKN to drop to near zero). That is a rug pull.

Risks: Smart contract risk

Summary

- Not all smart contracts are smart
- Once contract is deployed, it cannot be “fixed”

Other attacks

- Origin (reentrancy) November 2020:

<https://www.theblockcrypto.com/post/84804/defi-protocol-origin-attack-7-million-lost>

<https://hacken.io/researches-and-investigations/biggest-defi-hacks-of-2020-report/>

<https://www.cybavo.com/blog/defi-hacks-2021/>