SharkTeam

Reentrancy Attack: Analysis of Visor Finance's Uniswap V3 Liquidity Protocol Hack

Dec 23, 2021

SharkTeam, a leading blockchain security service team, offers smart contract audit services for developers. To satisfy the demands of different clients, thesmart contract audit services provide both manual auditing and automated auditing.

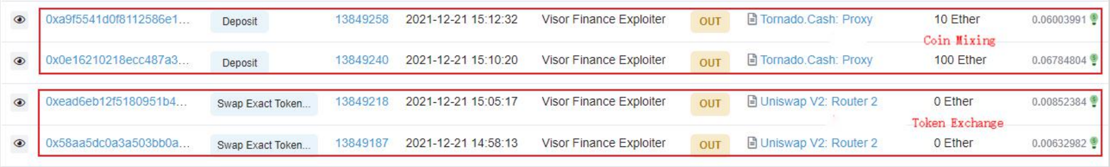
We implement almost 200 auditing contents that cover four aspects: high-level language layer, virtual machine layer, blockchain layer, and business logiclayer, ensuring that smart contracts are completely guaranteed and Safe.

Reentrancy Attack: Analysis of Visor Finance's Uniswap V3 Liquidity Protocol Hack

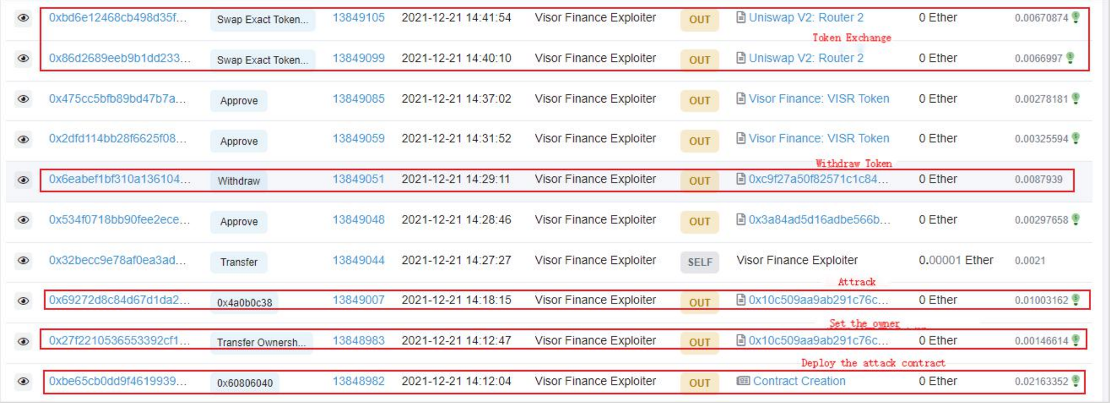
The Uniswap V3 liquidity management protocol, Visor Finance, was attacked with a total loss of about $8.2 million on December 21 at 10:18 p.m.(BJT). SharkTeam conducted attack analysis and technical analysis on this incident for the first time,and summarized the security prevention measures. It is hoped that subsequent blockchain projects can learn from it and build a security defense line in the blockchain industry.

1. Incident analysis

The attack record is as follows:



👁	0xa9f5541d0f8112586e1...	Deposit	13849258	2021-12-21 15:12:32	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	10 Ether	0.06003991
👁	0x0e16210218ecc487a3...	Deposit	13849240	2021-12-21 15:10:20	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	100 Ether	0.06784804
👁	0xead6eb12f5180951b4...	Swap Exact Token...	13849218	2021-12-21 15:05:17	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.00852384
👁	0x58aa5dc0a3a503bb0a...	Swap Exact Token...	13849187	2021-12-21 14:58:13	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.00632982



👁	0xbd6e12468cb498d35f...	Swap Exact Token...	13849105	2021-12-21 14:41:54	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.00670874
👁	0x86d2689eeb9b1dd233...	Swap Exact Token...	13849099	2021-12-21 14:40:10	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.0066997
👁	0x475cc5bfb89bd47b7a...	Approve	13849085	2021-12-21 14:37:02	Visor Finance Exploiter	OUT	Visor Finance: VISR Token	0 Ether	0.00278181
👁	0x2dfd114bb28f6625f08...	Approve	13849059	2021-12-21 14:31:52	Visor Finance Exploiter	OUT	Visor Finance: VISR Token	0 Ether	0.00325594
👁	0x6eabef1bf310a136104...	Withdraw	13849051	2021-12-21 14:29:11	Visor Finance Exploiter	OUT	0xc9f27a50f82571c1c84...	0 Ether	0.0087939
👁	0x534f0718bb90fee2ece...	Approve	13849048	2021-12-21 14:28:46	Visor Finance Exploiter	OUT	0x3a84ad5d16adbe566b...	0 Ether	0.00297658
👁	0x32becc9e78af0ea3ad...	Transfer	13849044	2021-12-21 14:27:27	Visor Finance Exploiter	SELF	Visor Finance Exploiter	0.00001 Ether	0.0021
👁	0x69272d8c84d67d1da2...	0x4a0b0c38	13849007	2021-12-21 14:18:15	Visor Finance Exploiter	OUT	0x10c509aa9ab291c76c...	0 Ether	0.01003162
👁	0x27f2210536553392cf1...	Transfer Ownersh...	13848983	2021-12-21 14:12:47	Visor Finance Exploiter	OUT	0x10c509aa9ab291c76c...	0 Ether	0.00146614
👁	0xbe65cb0dd9f4619939...	0x60806040	13848982	2021-12-21 14:12:04	Visor Finance Exploiter	OUT	Contract Creation	0 Ether	0.02163352

(1) Deploy the attack contract

Transaction： 0xbe65cb0dd9f4619939cfeb56b3ef3a996e2b028b93fd66443abfa06d6df8e58d

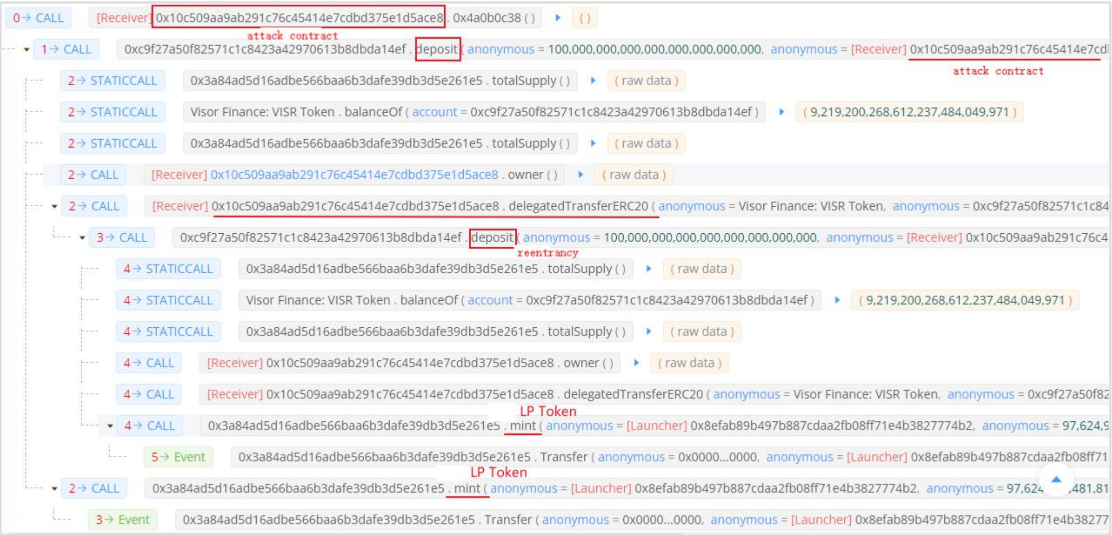
Attack contract: 0x10C509AA9ab291C76c45414e7CdBd375e1D5AcE8

(2) Attack

The attack transaction is:

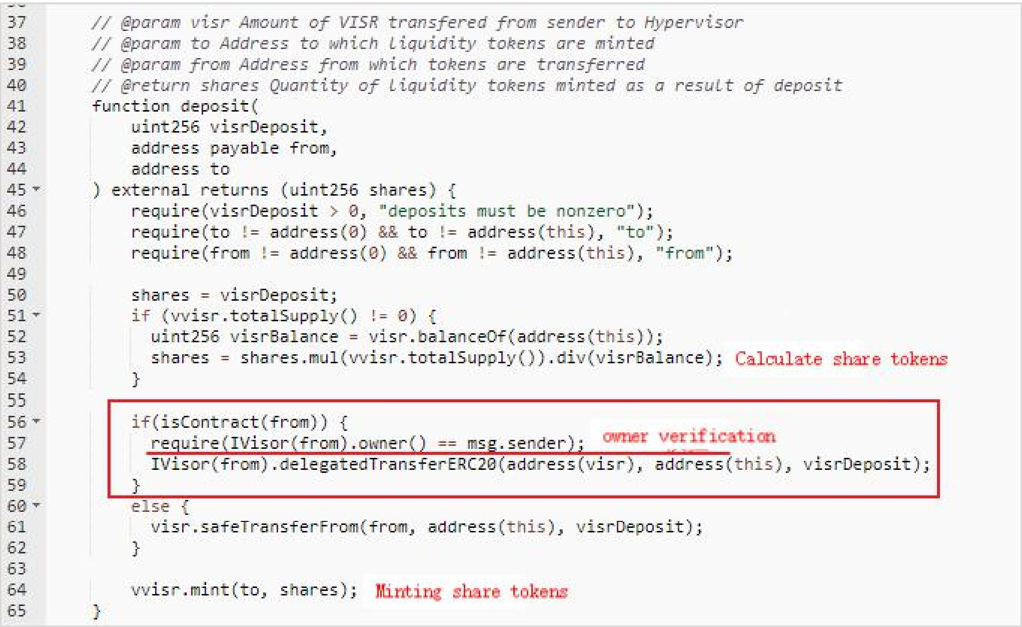
0x69272d8c84d67d1da2f6425b339192fa472898dce936f24818fda415c1c1ff3f

The attack detail is as follows:



```
0→ CALL        [Receiver] 0x10c509aa9ab291c76c45414e7cdbd375e1d5ace8 . 0x4a0b0c38 ( )  ▸  ( )
1→ CALL        0xc9f27a50f82571c1c8423a42970613b8dbda14ef . deposit ( anonymous = 100,000,000,000,000,000,000,000,000,  anonymous = [Receiver] 0x10c509aa9ab291c76c45414e7cd
  2→ STATICCALL  0x3a84ad5d16adbe566baa6b3dafe39db3d5e261e5 . totalSupply ( )  ▸  ( raw data )
  2→ STATICCALL  Visor Finance: VISR Token . balanceOf ( account = 0xc9f27a50f82571c1c8423a42970613b8dbda14ef )  ▸  ( 9,219,200,268,612,237,484,049,971 )
  2→ STATICCALL  0x3a84ad5d16adbe566baa6b3dafe39db3d5e261e5 . totalSupply ( )  ▸  ( raw data )
  2→ CALL        [Receiver] 0x10c509aa9ab291c76c45414e7cdbd375e1d5ace8 . owner ( )  ▸  ( raw data )
  2→ CALL        [Receiver] 0x10c509aa9ab291c76c45414e7cdbd375e1d5ace8 . delegatedTransferERC20 ( anonymous = Visor Finance: VISR Token,  anonymous = 0xc9f27a50f82571c1c84
    3→ CALL        0xc9f27a50f82571c1c8423a42970613b8dbda14ef . deposit ( anonymous = 100,000,000,000,000,000,000,000,000,  anonymous = [Receiver] 0x10c509aa9ab291c76c4
      4→ STATICCALL  0x3a84ad5d16adbe566baa6b3dafe39db3d5e261e5 . totalSupply ( )  ▸  ( raw data )
      4→ STATICCALL  Visor Finance: VISR Token . balanceOf ( account = 0xc9f27a50f82571c1c8423a42970613b8dbda14ef )  ▸  ( 9,219,200,268,612,237,484,049,971 )
      4→ STATICCALL  0x3a84ad5d16adbe566baa6b3dafe39db3d5e261e5 . totalSupply ( )  ▸  ( raw data )
      4→ CALL        [Receiver] 0x10c509aa9ab291c76c45414e7cdbd375e1d5ace8 . owner ( )  ▸  ( raw data )
      4→ CALL        [Receiver] 0x10c509aa9ab291c76c45414e7cdbd375e1d5ace8 . delegatedTransferERC20 ( anonymous = Visor Finance: VISR Token,  anonymous = 0xc9f27a50f82
      4→ CALL        0x3a84ad5d16adbe566baa6b3dafe39db3d5e261e5 . mint ( anonymous = [Launcher] 0x8efab89b497b887cdaa2fb08ff71e4b3827774b2,  anonymous = 97,624,9
        5→ Event       0x3a84ad5d16adbe566baa6b3dafe39db3d5e261e5 . Transfer ( anonymous = 0x0000...0000,  anonymous = [Launcher] 0x8efab89b497b887cdaa2fb08ff71
  2→ CALL        0x3a84ad5d16adbe566baa6b3dafe39db3d5e261e5 . mint ( anonymous = [Launcher] 0x8efab89b497b887cdaa2fb08ff71e4b3827774b2,  anonymous = 97,624  ,481,81
    3→ Event       0x3a84ad5d16adbe566baa6b3dafe39db3d5e261e5 . Transfer ( anonymous = 0x0000...0000,  anonymous = [Launcher] 0x8efab89b497b887cdaa2fb08ff71e4b38277
```

A reentrancy attack occurred in the deposit function during the attack. The deposit function is as follows:



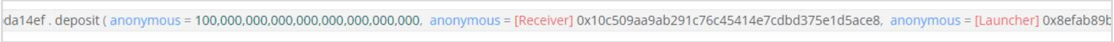
```
    // @param visr Amount of VISR transfered from sender to Hypervisor
    // @param to Address to which liquidity tokens are minted
    // @param from Address from which tokens are transferred
    // @return shares Quantity of liquidity tokens minted as a result of deposit
    function deposit(
        uint256 visrDeposit,
        address payable from,
        address to
    ) external returns (uint256 shares) {
        require(visrDeposit > 0, "deposits must be nonzero");
        require(to != address(0) && to != address(this), "to");
        require(from != address(0) && from != address(this), "from");

        shares = visrDeposit;
        if (vvisr.totalSupply() != 0) {
          uint256 visrBalance = visr.balanceOf(address(this));
          shares = shares.mul(vvisr.totalSupply()).div(visrBalance);
        }

        if(isContract(from)) {
          require(IVisor(from).owner() == msg.sender);
          IVisor(from).delegatedTransferERC20(address(visr), address(this), visrDeposit);
        }
        else {
          visr.safeTransferFrom(from, address(this), visrDeposit);
        }

        vvisr.mint(to, shares);
    }
```

The contract invokes the deposit function，the parameters are as follows:

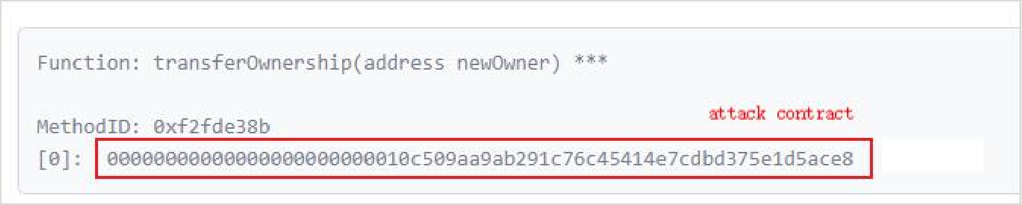


```
da14ef . deposit ( anonymous = 100,000,000,000,000,000,000,000,000,  anonymous = [Receiver] 0x10c509aa9ab291c76c45414e7cdbd375e1d5ace8,  anonymous = [Launcher] 0x8efab89b
```

The volume of specified tokens deposited is visrDeposit, the attack contract is from, and the attacker's account address is to.

Transaction ： 0x27f2210536553392cf180c0b37055b3dc92094a5d585d7d2a51f790c9145e47c

Change the contract's owner to the attack contract.

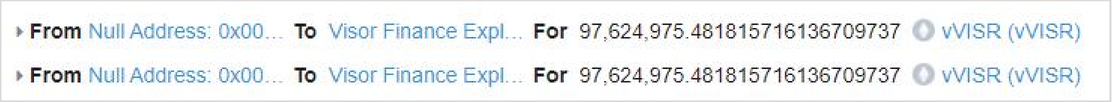


```
Function: transferOwnership(address newOwner) ***

MethodID: 0xf2fde38b
[0]:  00000000000000000000000010c509aa9ab291c76c45414e7cdbd375e1d5ace8
```

attack contract

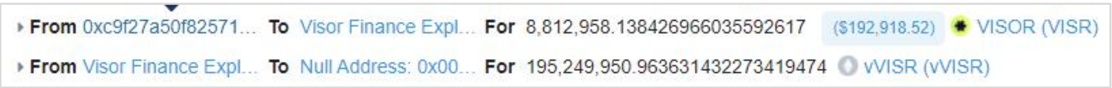
Therefore, it can pass the verification of the owner address, Then, when the attack contract's delegatedTransferERC20 function is invoked, a reentrancy attack occurs, and the deposit function is performed again with the same parameters, thereby repeatedly minting 97624975 vVISR share tokens.



- From Null Address: 0x00... To Visor Finance Expl... For 97,624,975.481815716136709737 vVISR (vVISR)
- From Null Address: 0x00... To Visor Finance Expl... For 97,624,975.481815716136709737 vVISR (vVISR)

(3) Withdraw Token

Transaction：0x6eabef1bf310a1361041d97897c192581cd9870f6a39040cd24d7de2335b4546

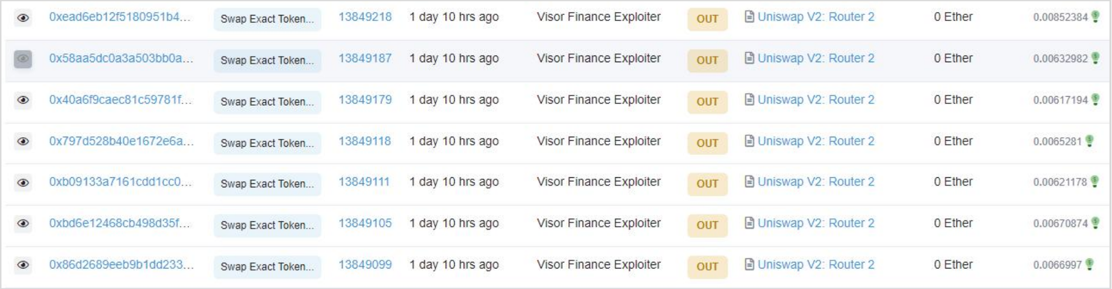


- From 0xc9f27a50f82571... To Visor Finance Expl... For 8,812,958.138426966035592617 ($192,918.52) VISOR (VISR)
- From Visor Finance Expl... To Null Address: 0x00... For 195,249,950.963631432273419474 vVISR (vVISR)

195249950 vVISR share tokens were withdrawn by 8812958 VISR.

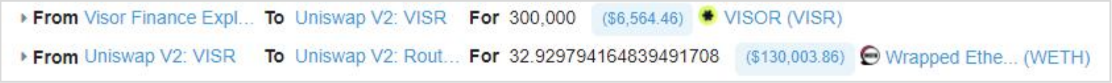
(4)Token Exchange

Convert VISR to ETH with UniswapV2.



0xead6eb12f5180951b4...	Swap Exact Token...	13849218	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.00852384
0x58aa5dc0a3a503bb0a...	Swap Exact Token...	13849187	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.00632982
0x40a6f9caec81c59781f...	Swap Exact Token...	13849179	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.00617194
0x797d528b40e1672e6a...	Swap Exact Token...	13849118	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.0065281
0xb09133a7161cdd1cc0...	Swap Exact Token...	13849111	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.00621178
0xbd6e12468cb498d35f...	Swap Exact Token...	13849105	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.00670874
0x86d2689eeb9b1dd233...	Swap Exact Token...	13849099	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Uniswap V2: Router 2	0 Ether	0.0066997

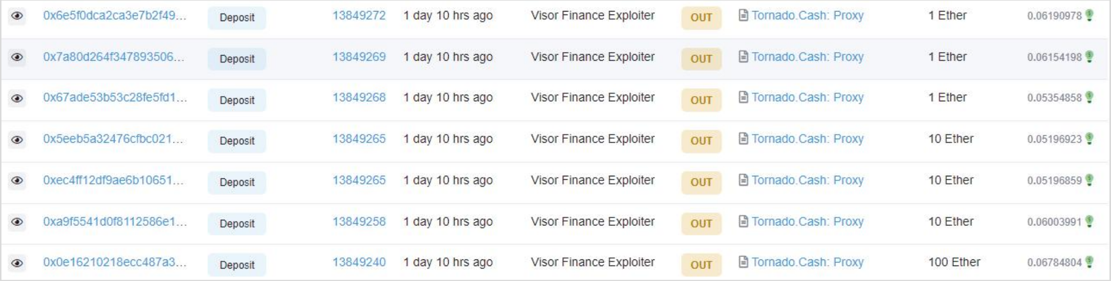
As an example, in the transaction : 0x86d2689eeb9b1dd233e6a9ab62ffa16ecdedff55ea5f6f10571432cf9830d907, 300000 VISR is exchanged for 32.93 WETH.



- From Visor Finance Expl... To Uniswap V2: VISR For 300,000 ($6,564.46) VISOR (VISR)
- From Uniswap V2: VISR To Uniswap V2: Rout... For 32.929794164839491708 ($130,003.86) Wrapped Ethe... (WETH)

(5)Coin Mixing

The Tornado platform is used for coin mixing.



👁	0x6e5f0dca2ca3e7b2f49…	Deposit	13849272	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	1 Ether	0.06190978
👁	0x7a80d264f347893506…	Deposit	13849269	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	1 Ether	0.06154198
👁	0x67ade53b53c28fe5fd1…	Deposit	13849268	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	1 Ether	0.05354858
👁	0x5eeb5a32476cfbc021…	Deposit	13849265	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	10 Ether	0.05196923
👁	0xec4ff12df9ae6b10651…	Deposit	13849265	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	10 Ether	0.05196859
👁	0xa9f5541d0f8112586e1…	Deposit	13849258	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	10 Ether	0.06003991
👁	0x0e16210218ecc487a3…	Deposit	13849240	1 day 10 hrs ago	Visor Finance Exploiter	OUT	Tornado.Cash: Proxy	100 Ether	0.06784804

The loophole in the deposit function called contract verification logic is the main reason for this attack. To limit the contract calling address, SharkTeam advises utilizing a whitelist mechanism in the contract.

Reentrancy locks should also be added to key functions in deposit, such as utilizing openzeppelin's ReentrancyGuard to avoid reentrancy attacks.

2. Safety suggestion

SharkTeam reminds you that please be vigilant when setting foot in blockchain projects. Try to choose more stable, More secure, public chains, and projects that have been audited for several rounds, In initiating a transaction. Never put your assets at risk and become a hacker's ATM.

SharkTeam

In Math, We Trust !

https://sharkteam.org

https://t.me/sharkteamorg

https://twitter.com/sharkteamorg