



成都链安



Footprint
Analytics

2022年上半年 Web3安全态势深度研报

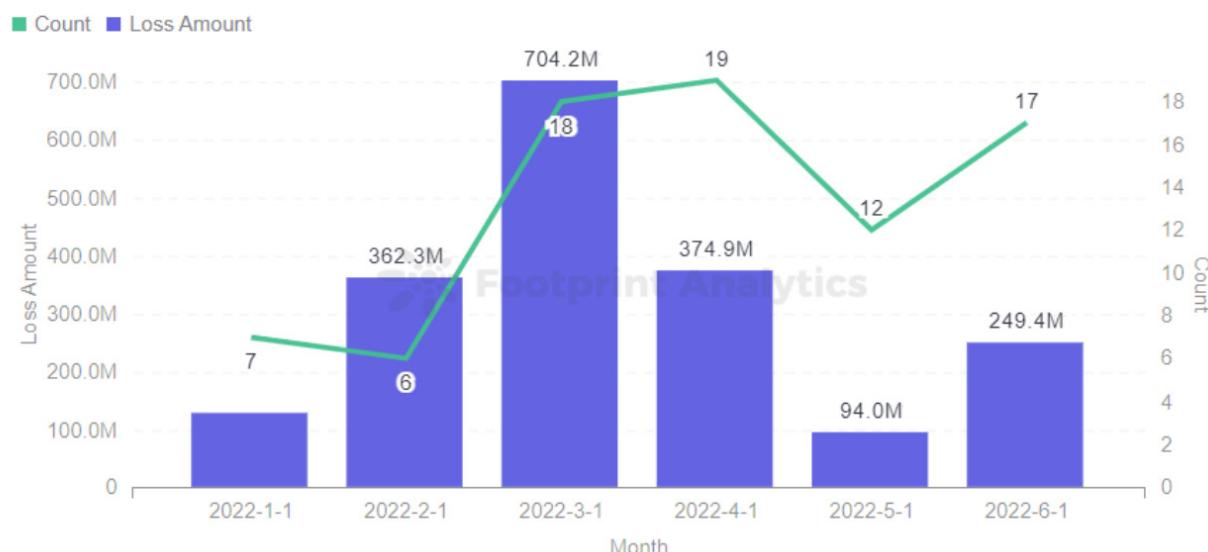
CONTENTS 目录

2022上半年Web3安全态势综述	01
数据一 2022上半年共发生7起跨链桥攻击事件，共损失11亿3599万美元	02
数据二 53%的攻击方式为合约漏洞利用	06
数据三 约26.6%的攻击方式为闪电贷	09
数据四 上半年共发生5起损失过亿的安全事件	13
数据五 整个DeFi TVL从1月初的2798亿美元跌到了6月末的824亿美元，下跌70.5%	16
数据六 黑客通过Tornado Cash共洗钱11亿4070万美元	18
数据七 约71%的攻击发生在DeFi领域	19
数据八 NFT领域主要安全事件10起，损失约为6490万美元；NFT钓鱼事件频发	22
结语	28
成都链安介绍	29
声明	29

2022上半年Web3安全态势综述

2022年上半年，Web3领域共监测到主要安全事件约**79**起，因各类攻击造成的损失达到了**19亿1287万美元**。

H1 Total Losses Amount & Count



上半年安全事件数量及损失金额

我们可以从以下这组数据看到上半年的Web3安全领域的整体概况：

- ◆ 上半年发生**7**起跨链桥攻击事件，共损失**11亿3599万美元**；
- ◆ **53%**的攻击方式为合约漏洞利用；
- ◆ 约**26.6%**的攻击方式为闪电贷；
- ◆ 上半年共发生**5**起损失过亿的安全事件；
- ◆ 整个DeFi市场TVL从1月初的**2760亿美元**跌到了6月末的**800亿美元**，下跌**71%**；
- ◆ 黑客通过Tornado Cash共洗钱**11亿4070万美元**；
- ◆ 约**71%**的攻击发生在DeFi领域。

在第一季度和第二季度的安全报告中，我们已经从各个维度展示和分析了区块链安全领域的总体态势，包括总损失金额、被攻击项目类型、各链平台损失金额、攻击手法、资金流向、项目审计情况等。

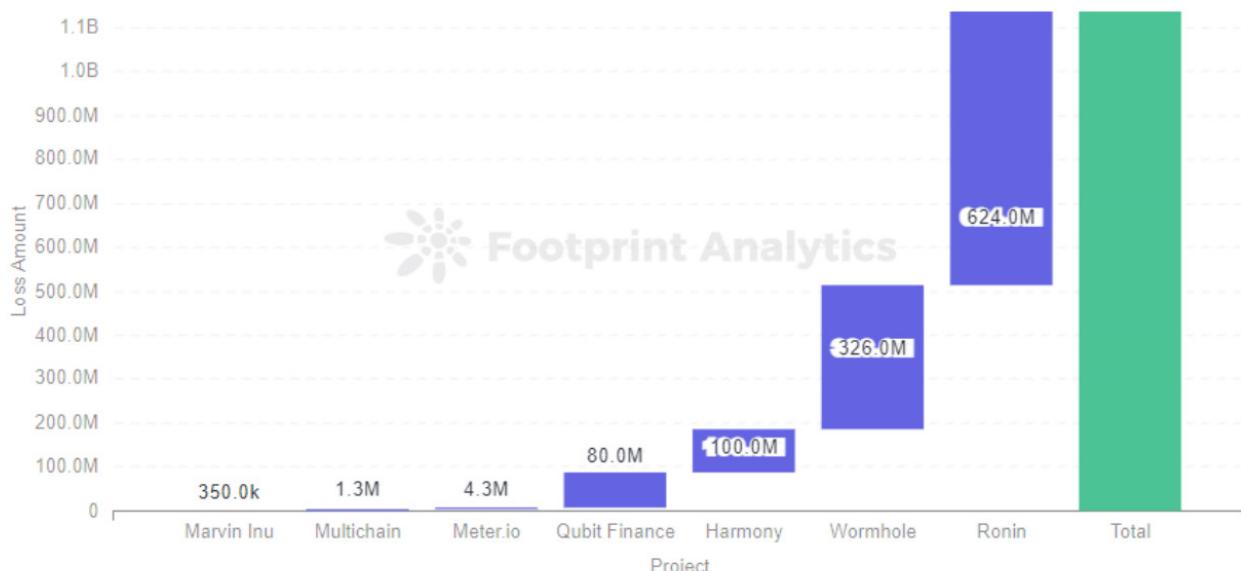
在这份半年报里，我们将这些发生在上半年的典型的安全数据提取出来，从安全事件出发，结合成都链安安全团队多年在实战中的审计经验、资金追踪经验和研究经验，为大家还原这些数据背后的深层次原因和安全事件的来龙去脉。

数据一

2022上半年共发生7起跨链桥攻击事件，共损失11亿3599万美元

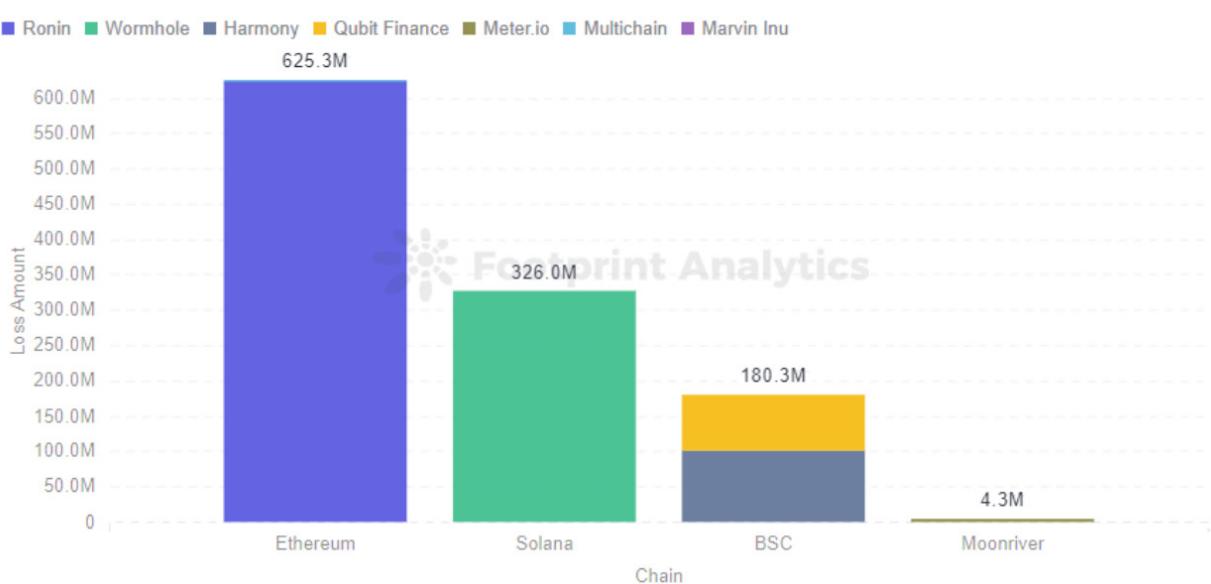
2022年上半年，共发生了7起跨链桥攻击事件，共计损失金额约11亿3599万美元，占了上半年总损失金额的59%。为什么黑客钟爱跨链桥？为什么跨链桥攻击损失金额如此巨大？跨链桥安全性该如何保障？

H1 Attacked Bridges by Loss Amount



上半年跨链桥损失金额（按项目）

H1 Attacked Bridges



上半年跨链桥损失金额（按链平台）

◆ 1 什么是跨链桥？

当前区块链行业发展迅猛，出现了各种各样的公有链，但是不同链上有着不同类型的资产、协议等，使得它们之间无法直接通信，这给用户带来了诸多不便，比如：某用户持有比特币资产，但是想在以太坊生态中进行投资或消费，那么最直接的方式就是通过中心化的交易所进行兑换，但是整个过程非常繁琐，耗时很长并且需要多次支付手续费。

跨链技术的发展使得用户对于不同区块链之间的互操作（如：资产交易和信息交互）成为可能，其中应用范围最广的实现就是跨链桥。

◆ 2 目前跨链桥类型

- 两条链之间转移一项资产：存在将特定加密货币转移到另一条链的桥梁。例如wBTC（由BitGo管理）和tBTC（由Keep Network管理），两者都允许用户将BTC从比特币区块链转移到以太坊。
- 两条链之间转移许多资产：一些桥允许用户移动多个令牌，但只能在两条链之间移动。例如，Rainbow Bridge可以将ETH和多个ERC-20代币从以太坊发送到NEAR协议。同样，Gravity和ZeroSwap分别允许以太坊与Cosmos和Binance Smart Chain (BSC)之间的多资产转移。
- 资产从一条链转移到多条链：某些跨链桥使用户能够将一条链连接到多个区块链。一个例子是 Wormhole，它将资产从Solana连接到Ethereum、Fantom、Avalanche、Terra和Polygon。
- 不同链之间转移多种资产：Ren Bridge就是一个典型例子，它促进代币在独立区块链之间的移动来提高互操作性。

◆ 3 跨链桥如何工作？

- (一) Alice将Token A发送到源链（例如以太坊）上的特定地址并支付交易费用。
- (二) Alice的Token A由受信任的验证者锁定在智能合约中或由受信任的托管人持有。
- (三) 线下程序在源链上获取到了Alice锁定Token A触发的事件，线下程序将在目标链(例如Polygon)上面铸造等量价值的Token B.

◆ 4 跨链桥几起安全事件金额为何如此巨大？

首先跨链桥需要持有大量的资金，以确保所有的发送者都能得到支付，所以每次攻击都会造成大量的资金损失，最后黑客也比较专注于资金更多的跨链桥。

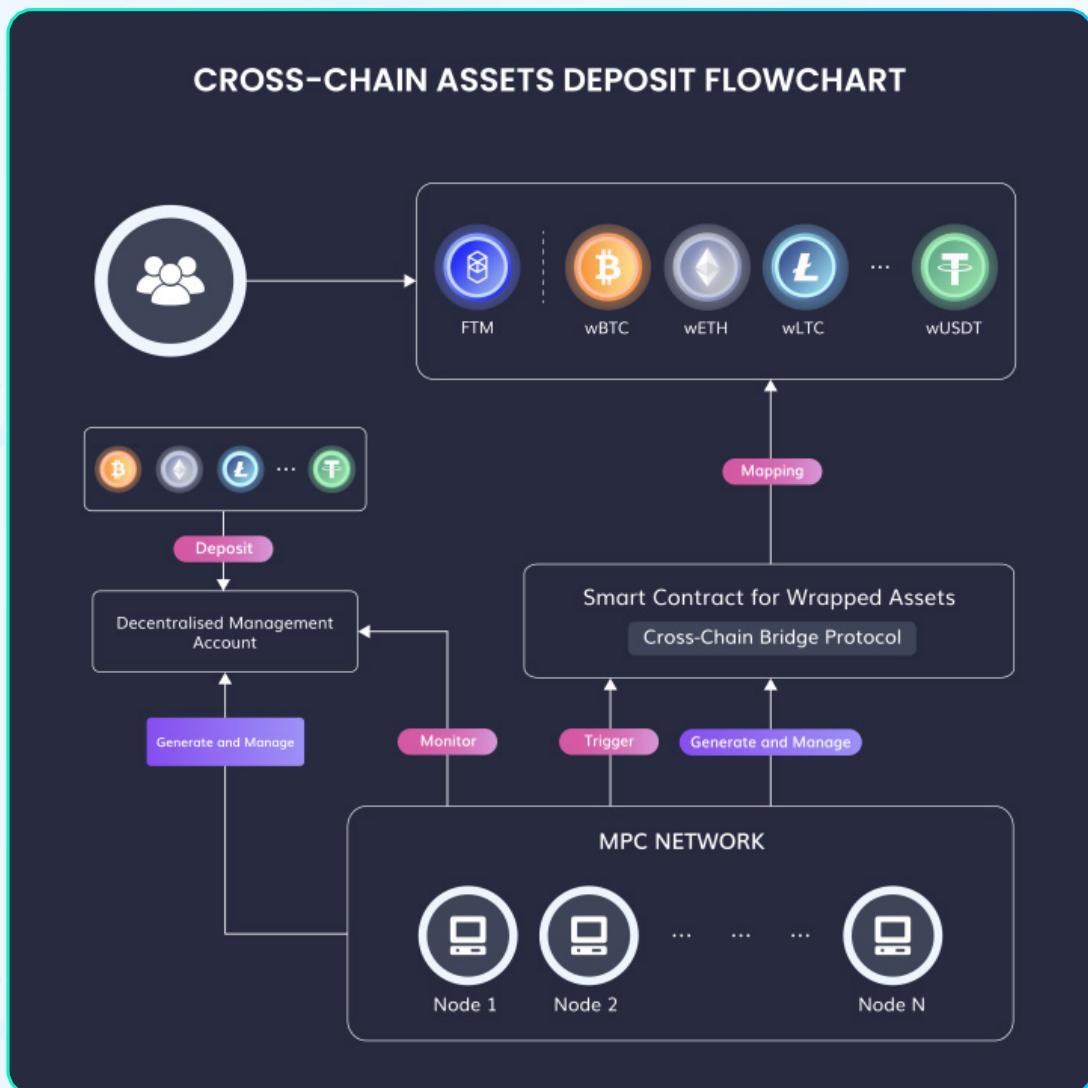
5 攻击手法是什么？

这里主要分三个部分来讲述，因为上半年的攻击事件并没有利用到线下程序漏洞，为了补充该部分，这里会提到去年的攻击事件作为补充。

■ 合约漏洞

(一) 2022/1/18 Multichain事件累计损失134万美元。

此次主要原因是由于anySwapOutUnderlyingWithPermit函数未检查用户传入的Token的合法性，且未考虑并非所有underlying代币都有实现permit函数，导致用户资产被未授权转出。



Multichain的Deposit流程图

(二) 2022/1/27 Qubit Bridge事件累计损失8000万美元。

此次主要原因是由于抵押ETH和ERC-20的存款事件相同，因为在deposit函数中，当代币地址是EOA（如address(0)）时，“safeTransferFrom”函数不会回退，所以攻击者可以伪造存款事件。

(三) 2022/2/3 Wormhole事件累计损失约3.26亿美元。

黑客利用了Wormhole合约中的签名验证漏洞，这个漏洞允许黑客伪造sysvar帐户来铸造wETH。

(四) 2022/2/6 Meter.io事件累计损失430万美元。

攻击者通过调用deposit函数使”tokenAddress == _wtokenAddress”导致绕过了来源链上的burn或者lock代币的过程，所以攻击者不用转入代币即可触发Deposit事件，从而可以mint出代币。

■ 私钥泄露

(一) 2022/3/30 Ronin事件累计损失6.25亿美元。

(二) 2022/4/11 Marvin Inu事件累计损失35万美元。

(三) 2022/6/24 Harmony事件累计损失1亿美元。

■ 线下程序缺陷

(一) 2021/7/10 Anyswap事件累计损失787万美元。

该项目由于线下程序签名使用了相同的ECDSA签名的r值，如果该同一账户签名的交易拥有相同的ECDSA签名的r值，则黑客可以反向推导出该账户的私钥，从而盗取该账户资金。

(二) 2021/6/29 THORChain第一次攻击事件损失近35万美元。

本次攻击的发生是由于THORChain线下程序代码上的逻辑漏洞，即当跨链充值的ERC20代币符号为ETH时，线下程序会把充值的代币被识别为真正的以太币ETH，进而可以成功的将假ETH兑换为其他的代币。

(三) 2021/7/16 THORChain第二次攻击事件损失近800万美元。

攻击者在攻击合约中调用了THORChain Router合约的deposit方法，传递的amount参数是0。然后攻击者地址发起了一笔调用攻击合约的交易，设置交易的value(msg.value)不为0，由于THORChain线下程序的缺陷，在获取用户充值金额时，使用交易里的msg.value值覆盖了正确的Deposit event中的amount值，导致了“空手套白狼”的结果。

(四) 2021/7/23 THORChain第三次攻击事件损失近800万美元。

本次攻击利用了线下程序的一个退款逻辑漏洞，攻击者首先利用攻击合约触发一个deposit事件，攻击者随意构造asset和amount，同时构造一个不符合要求的memo，使THORChain线下程序无法处理，然后按照程序设计就会进入到退款逻辑。

■ 对于项目方

- (一) 尽可能的了解跨链项目相关的风险，实现安全开发。
- (二) 线下进行风控，即使跨链桥存在问题，项目方也能及时发现异常跨链行为并进行应急响应。例如项目方可以统计跨链桥两侧的资金是否平衡，来判断跨链桥是否遭受攻击。
- (三) 需保证线下多个签名服务器实现验签，同时定期检查线下签名服务器的安全性或者更换签名地址，防止签名服务器被攻击。
- (四) 项目上线前对合约进行安全审计。
- (五) 版本更新时需要对相关接口及签名安全进行重新评估。
- (六) 需要对跨链签名者进行严格审查以保证签名不被恶意人员控制。
- (七) 制订漏洞赏金计划，并及时修复白帽提出的安全问题。赏金计划用于激励白帽黑客审查代码并在漏洞被不良行为者利用之前披露漏洞，防止用户的资金损失。

■ 对于用户

- (一) 选择经过多家知名安全公司审计的跨链项目
- (二) 查看审计报告，看报告中安全公司提出的问题项目方是否已经妥善解决

数据二

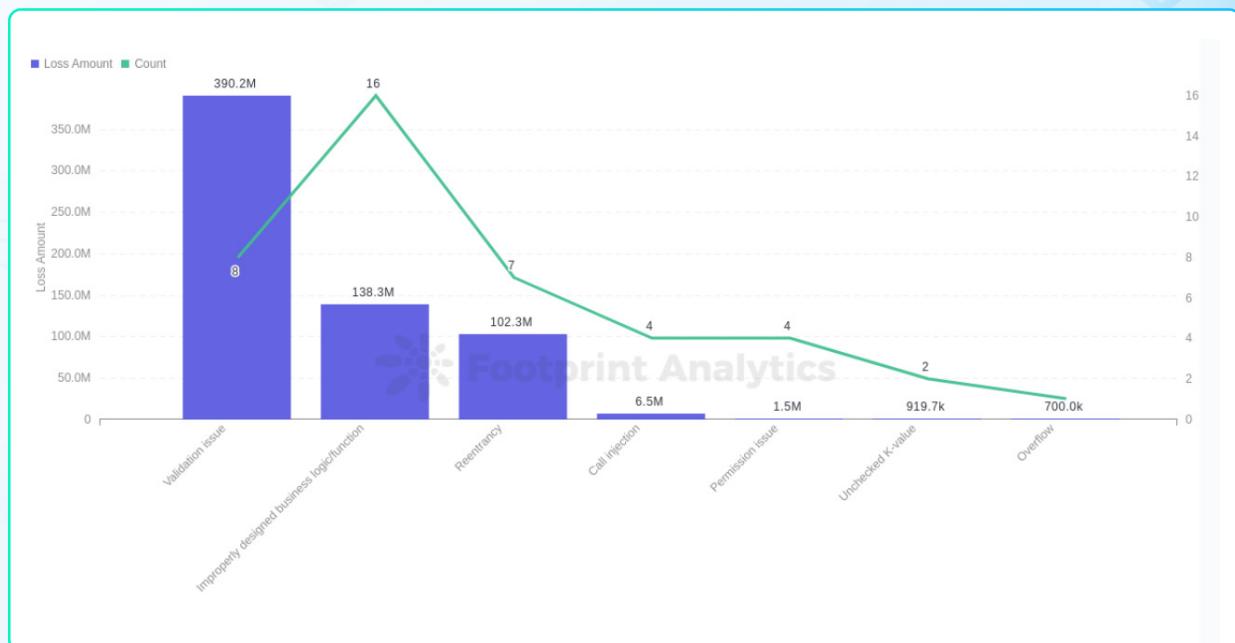
53%的攻击方式为合约漏洞利用

2022上半年共监测到因合约漏洞造成的主要攻击案例42次，约53%的攻击方式为合约漏洞利用。这些漏洞实际造成了多少损失？它们能在审计阶段被发现吗？审计中出现的漏洞和实际被黑客利用的漏洞有区别吗？

因漏洞造成的总损失

通过统计，2022上半年共监测到因合约漏洞造成的主要攻击案例42次，总损失达到了6亿4404万美元。

在所有被利用的漏洞中，逻辑或函数设计不当被黑客利用次数最多，其次为验证问题、重入漏洞。



各漏洞利用次数及造成的损失金额

单次损失金额最大的是哪种类型的漏洞？

单次损失金额最高的是签名验证漏洞。2022年2月3日，Solana跨链桥项目Wormhole遭到攻击，累计损失约3.26亿美元。黑客利用了Wormhole合约中的签名验证漏洞，这个漏洞允许黑客伪造sysvar帐户来铸造wETH。

单次金额损失第二的漏洞是重入漏洞。2022年4月30日，Fei Protocol官方的Rari Fuse Pool遭受闪电贷加重入攻击，总共造成了8034万美元的损失。

审计过程中最常出现的漏洞有哪些？

在审计过程中最常见出现的总体来说分为四大类：

◆ 1 ERC721/ERC1155重入攻击：

在通过成都链安形式化验证工具VaaS平台检测合约中不乏存在ERC721 / ERC1155标准相关的业务合约，在ERC721中，ERC1155中存在分别存在一个onERC721Received()/onERC1155Received () 函数用于转账通知，类似于以太坊转账的fallback()函数，在相关的业务合约中使用ERC721/ERC1155标准中的_safeMint (),_safeTransfer(),safeTransferFrom()进行铸币或者转账时都会触发转账通知函数。如果在转账的目标合约中的onERC721Received()/onERC1155Received () 中包含了恶意代码，就可能形成重入攻击。除此之外在相关业务函数未严格按照检查-生效-交互模式设计，上述两点共同导致了漏洞的产生。

◆ 2 逻辑漏洞：

(一) 特殊场景考虑缺失：

特殊场景往往是审计最需要关注的地方，例如转账函数设计未考虑自己给自己转账导致无中生有。

存放费用的合约没有提取功能，借贷合约不含清算功能等。

(三) 鉴权缺失：

铸币、设置合约特殊角色、设置合约参数的相关函数没有鉴权，导致三方地址也可以调用。

(四) 价格操控：

Oracle价格预言机未使用时间加权平均价格；

未使用价格预言机，直接使用合约中两种代币的余额比例作为价格等。

实际被利用的漏洞有哪些？

根据成都链安鹰眼区块链安全态势感知平台所感知的安全事件统计，审计过程中出现的漏洞几乎都实际场景中被黑客利用过，其中合约逻辑漏洞利用仍然为主要部分。

哪些漏洞能在审计阶段发现？

通过成都链安形式化验证工具VaaS平台检测和安全专家人工检测审计，以上漏洞均能在审计阶段被发现，并且可由安全专家在做出安全评估后提出相关安全修补建议供客户作为修复参考。

The screenshot shows the VaaS tool's user interface during a contract audit. On the left, the Solidity code for the 'FakeNft' contract is displayed, with specific lines of code highlighted in red. On the right, a list of 21 detected issues is shown, categorized by severity and type. The interface includes a 'View Report' button.

Issue ID	Description
1	Reentrancy vulnerabilities(1725row)
2	Missing return value(1756row)
3	Compile Problem(1row)
4	Check code using extcodesize(745row)
5	Unused return(1563row)
6	Unused return(1565row)
7	Unused return(1593row)
8	Unused return(1595row)
9	Unused return(1620row)
10	Unused return(1621row)
11	Unused return(1623row)
12	Unused return(1753row)
13	Compile Problem(1757row)
14	Compile Problem(1758row)
15	Compile Problem(1759row)
16	Compile Problem(1760row)
17	Unused return(1766row)
18	Multiple pragma directives are used(40row)
19	Assembly usage(745row)
20	Low-level calls(769row)
21	Public function that could be declared as external(1063row)

图：通过VaaS工具扫描出某合约存在重入漏洞

数据三

约26.6%的攻击方式为闪电贷

2022年上半年，使用闪电贷进行攻击的案例达到了21次，占比26.6%，涉及金额高达3亿3291万美元。什么是闪电贷？闪电贷通常和哪些漏洞结合起来被黑客利用？有没有什么防止闪电贷的机制？

◆ 1 什么是闪电贷？

闪电贷概念最早由Marble协议于2018年提出。Marble自诩「智能合约银行」，其产品是很简单、但很具智慧的DeFi创新——通过智能化合约完成的零风险贷款。

闪电贷就是在单笔交易中贷出借款人需要的金额，然而在交易结束时，借款人必须偿还不少于贷款金额的数目。如果借款人做不到，交易就会自动回滚，就像贷款根本没发生一样。其主要特征包括下面三点：

- 1) 这是一种无抵押贷款，这意味着借款人不需要用任何资产或存款来获得贷款（但会收取少许手续费）。此外，与传统的无抵押贷款不同，闪电贷没有信用检查流程。
- 2) 所有闪贷都是通过区块链上的智能合约完成的，并且规定如果借款人没有在单个区块链交易中归还资金，则贷款过程将被逆转，就好像它从未发生过一样。这个关键的特性就是为什么借款人能够在没有任何抵押品或信用检查的情况下获得快速贷款，因为它消除了贷方的任何风险。
- 3) 贷款过程是即时的，即借款人在借款后，必须调用其他智能合约来利用资金尝试执行几乎即时的交易，然后在单块交易结束前将资金返还。

◆ 2 闪电贷与区块链安全

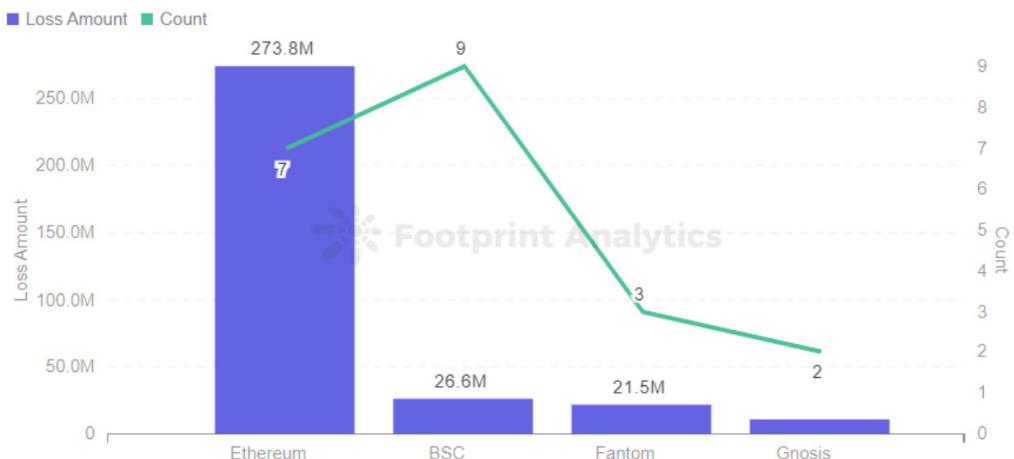
闪电贷本身不是一种攻击，但有心之人将其利用，以极低的成本撬动巨量资金，在多个协议间进行价格操纵或套利，就存在风险。

今年上半年使用闪电贷进行黑客攻击的案例总计21次，占比26.6%，涉及金额高达3亿3291万美元。其中上半年影响较大的攻击手法主要有闪电贷加治理攻击，闪电贷加价格操纵攻击，闪电贷加重入攻击等。



上半年各月闪电贷攻击次数及损失金额

H1 Flashloan Attacked by Chain



各链平台闪电贷攻击频次及损失金额

1) 2022年4月17日，**算法稳定币项目Beanstalk Farms遭到闪电贷治理攻击**，黑客获利7600万美元，协议损失达1亿8200万美元。

攻击过程大致如下：

准备阶段：

由于在BEAN合约中，所有治理行动都有1天的延迟，即提案后1天才能开始投票，所以攻击者实际上是在前一天提出两个治理提案，然后调用emergencyCommit进行紧急提交来执行提案。

其中，第一个提案（提议#18）提取合约中所有的钱。下一个提案（提议#19）将价值25万美元的\$BEAN发送到乌克兰的捐赠地址。

攻击阶段：

- a) 攻击者从Synapse协议桥（最初来自Tornado Cash）获取初始资金；
- b) 利用闪电贷获得价值超10亿资金：从Aave获得3.5亿 DAI，5亿 USDC，和1.5亿 USDT；从Uniswap v2获得3200万 BEAN；从SushiSwap获得1160万 LUSD。
- c) 这些代币被用来为Curve池子增加流动性，临时获得巨额的提案代币，保证了提案不需要其他人投票也能通过，从而将所有的资金从协议合约转移到攻击者地址。
- d) 下一步是移除流动性，偿还闪电贷，并将所有收到的资金转换为24800 WETH（价值7600万美元），这些资金随后被送到Tornado Cash。

2) 2022年4月28日，**多链衍生品平台DEUS Finance遭遇闪电贷加价格操纵攻击**，造成了约**1570万美元**的损失。

攻击过程大致如下：

- a) 攻击者在攻击之前先往 DeiLenderSolidex 抵押了 Solidex sAMM-USDC/DEI 的 LP；
- b) 随后攻击者利用攻击合约从多个池子闪电贷借出 143,200,000 USDC 用以发动攻击；
- c) 随后攻击者使用借来的 USDC 在 BaseV1Pair 进行了 swap 操作，兑换出了 9,547,716 个的 DEI。由于 DeiLenderSolidex 中的 getOnChainPrice 函数是直接获取 DEI-USDC 交易对的代币余额进行 LP 价格计算，因此在此次 Swap 操作中将拉高 getOnChainPrice 函数获取的 LP 价格；
- d) 由于 DeiLenderSolidex 合约是用预言机来确定用户抵押品的价值，而预言机合约使用被恶意操纵的交易对池的价格作为价格来源。因此通过提高的价格和之前提供的抵押，攻击者可从借贷池（DeiLenderSolidex）中总计借贷到 17,246,885 DEI，这一数额远大于之前攻击者提供抵押的金额。
- e) 攻击者用 9,547,716 个 DEI 交换到的 143,184,725 USDC 来偿还闪电贷款，最终获取差价离场。

3) 2022年4月30日，**Fei Protocol官方的Rari Fuse Pool遭受闪电贷加重入攻击**，黑客获利28380 ETH，价值约 8000万美元。

攻击过程大致如下：

- a) 攻击者用闪电贷借得 150,000,000 USDC 和 50,000 WETH
- b) 将 150,000,000 USDC 作为抵押品存入 fUSDC-127 合约，该合约是 compound 的漏洞分叉版本。
- c) 利用存入的抵押品，攻击者通过 "borrow()" 函数借走了 1,977 个 ETH。
- d) 然而，"borrow()" 函数并没有遵循检查-实施-交互模式。具体来说，在更新攻击者的实际借款记录之前，它将 ETH 转移到攻击者的合约中。因此，在攻击者的借款记录没有更新的情况下，攻击者在回调函数中对 "exitmarket()" 进行了可重入的调用，这使得攻击者可以提取他所有的抵押品（150M USDC）。
- e) 攻击者在其他多个代币上重复步骤 1~5。
- f) 最后，攻击者偿还了闪电贷，并将剩下的钱作为利润转到自己的地址，并将部分资金转到 Tornado Cash。EI 交换到的 143,184,725 USDC 来偿还闪电贷款，最终获取差价离场。

③ 如何防范闪电贷攻击

闪电贷攻击频出不穷，那么项目方应该如何防范或者减缓闪电贷攻击呢？我们这里提出几条可能的建议：

要求关键交易跨越两个区块

如果一个资本密集型交易需要跨越至少两个区块，用户需要至少在两个区块时间段取出贷款，那么闪电贷攻击将会失效。但是要达到这一效果，两个区块之间用户价值必须锁定，以防止其偿还贷款。

时间加权平均定价 (TWAP)

在价格操纵案例中，建议使用时间加权平均价格 (TWAP) 来跨多个区块计算流动性池中的价格。因为整个攻击交易序列需要在同一个区块内处理，但如果操纵整个区块链就无法操纵 TWAP，从而可以避免闪电贷导致的瞬时价格异常。

更高频率的价格更新机制

同样在价格操作案例中，可以适当增加流动性池向预言机查询并更新价格的频率，随着更新次数的增加，池中代币的价格会更新得更快，并使价格操纵无效。

更严格的治理逻辑

在涉及到项目治理时，应该多方面考虑治理逻辑的严谨性，避免出现Beanstalk Farms那样的逻辑漏洞，一旦有个微小的漏洞，就有可能通过闪电贷无限放大，最后造成巨大的损失。

业务逻辑设计和实现时确保安全可靠

项目方在进行业务逻辑的设计和开发人员进行开发实现时，应充分考虑业务逻辑的完整性和安全性，注意极端情况。必要时，应找专业的审计机构进行审计和研究，防范各种可能的风险。

目前成都链安团队成员近200人，技术人员占比高达85%，其中包含几十位形式化验证专家和区块链安全专家，涵盖上线前的代码安全审计、项目运行时的风险预警与监控、虚拟货币被盗资产追回等全方位区块链安全产品+服务，目前已为全球2000多份智能合约、100多个知名区块链平台提供了安全审计与防御部署服务。

④ 监控闪电贷攻击

上述的建议一定程度上可以缓解闪电贷攻击，但是有些方案过程复杂，且代价过大，在实际项目中难以实现。那么我们在无法完全解决闪电贷攻击的前提下，能及时准确的监控闪电贷攻击就显得尤为重要。

成都链安鹰眼态势感知监测平台，能提供7x24小时的实时风险预警，平台使用了AI等技术，通过自动检测合约安全状态，监控链上运行状态、实时交易行为，自动识别异常交易，全面评估项目安全运行状态。能够帮助项目方发现诸如闪电贷攻击、套利交易、私钥泄漏导致的资金被盗等风险交易。

数据四

上半年共发生5起损失过亿的安全事件

2022年上半年，共发生了5起损失过亿的安全事件，分别为：

Ronin Network: 6.25亿美元
Wormhole: 3.26亿美元

Beanstalk Farms: 1.82亿美元
Elrond: 1.13亿美元

Harmony: 1亿美元

这5起黑客攻击事件造成的总损失就达到了13.46亿美元，占2022年上半年总损失金额的70%。

在Q2的季报里，我们看到了一些项目在被攻击后TVL直接归零，后续也没有再重启。那么这些损失过亿的项目被攻击后都如何了呢？

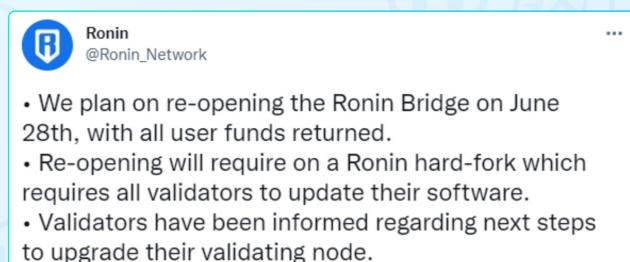
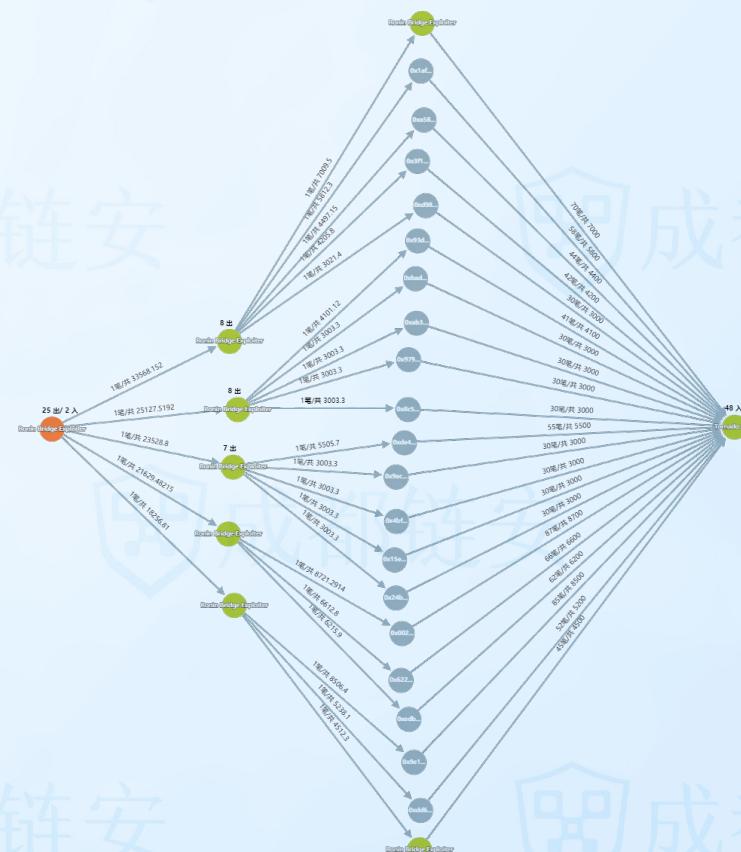
Ronin: 损失6.25亿美元，所有资产已全部转入Tornado Cash

3月29日，Axie Infinity的以太坊侧链Ronin Network遭到黑客攻击，损失约6.25亿美元。Ronin 侧链由 9 个验证器节点组成，要确认存款或取款，需要五个验证者签名。攻击者设法控制了 Sky Mavis 的四个 Ronin 验证器和一个由 Axie DAO 运行的第三方验证器。

攻击发生之后，Ronin 攻击者将部分盗取资金转入 Huobi、FTX、Binance、Crypto.com 等交易所，但各大交易所均发文表示将全力协助追回被盗资金。

随后，攻击者对被盗资产分散到了多个地址，并分批次通过 Tornado Cash 进行清洗。5月20日，Ronin 攻击者将最后一笔盗取资金转入 Tornado Cash，所有资产清洗完成。此时的ETH单价已从3,330美元下降到了约2,000美元，黑客实际获利比攻击时少了1.6亿美元。

使用链必追-虚拟货币案件智能研判平台对被盗资金进行分析，可以看到最终所有被盗资金都流向了 Tornado Cash。



6月28日，Ronin 在推特宣布重新开放。

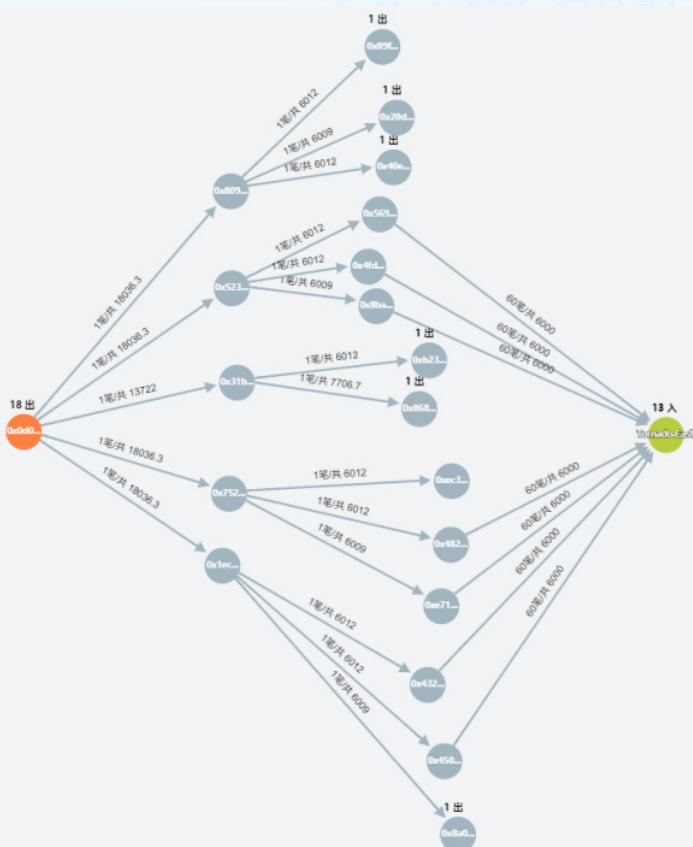
Harmony：4.2万枚ETH转入Tornado Cash

6月24日，Harmony 跨链桥 Horizon Bridge 遭到攻击，损失金额逾 1 亿美元。

6月26日，Harmony创始人表示，Horizon 被攻击并非因为智能合约漏洞，而是由私钥泄露导致。资金从跨链桥的以太坊一侧被盗。虽然 Harmony 对私钥进行了加密存储，但攻击者还是解密了其中部分私钥并签名了一些未经授权的交易。

Harmony 表示已经开始联合执法部门和所有交易平台对黑客进行全球追查。与此同时，Harmony 也将黑客盗币返还让利的金额从最初的100万美元提升至 1000 万美元。然而黑客还是通过Tornado Cash对赃款进行了洗钱。

截止到6月30日，[通过链必追-虚拟货币案件智能研判平台对被盗资金进行分析](#)，可以看到黑客已将约4.2万枚 ETH（价值约4620万美元）转移至Tornado Cash。



7月 27 日，Harmony 发布跨链桥 Horizon 被盗事件补偿提案，提案计划将对 Harmony 区块链进行硬分叉，增加 ONE 供应，并为期三年以 ONE Token 的形式对 Horizon 被盗事件受影响的用户进行补偿，Token 分配将按月进行。

Wormhole

Wormhole 在 2 月 3 日遭黑客攻击，经Wormhole官方确认，本次攻击事件中损失达 12 万枚 ETH。

随后，跨链协议 Wormhole 宣布已恢复其跨链桥资金，并已重新上线。加密投资基金 Jump Crypto 2月4日宣布，已投入 12 万枚以太坊以弥补跨链桥 Wormhole 的被盗损失，支持 Wormhole 继续发展。

目前，黑客地址0x629e7...6b71A仍持有93,750.97 ETH未转出。



Beanstalk Farms：所有资金全进Tornado Cash

4月17日，去中心化稳定币协议 Beanstalk Farms 遭到闪电贷攻击，协议损失1.82亿美元，攻击者获利约8000万美元。攻击者在攻击后很快便将所获8000万美元全部转入Tornado Cash混币。

4月19日，官方在推特表示，如果黑客能归还90%被盗资金，将为黑客提供10%的白帽赏金。

If you will return 90% of the withdrawn funds to the Beanstalk Farms multi-sig wallet
Ox21DE18B6A8f78eDe6D16C50A167f6B222DC08DF7
, Beanstalk will treat the remaining 10% as a Whitehat bounty properly payable to you.

4:45 AM · Apr 19, 2022 · Twitter for iPhone

6月2日，去中心化稳定币协议 Beanstalk Farms 推出筹款活动「The Barn Raise」，旨在恢复因治理漏洞而损失的 7700 万美元流动性。

Elrond：几乎所有被盗资金都已追回

6月7日，Elrond网络遭黑客攻击，超165万美元EGLD被盗，价值超1.13亿美元。

6月8日，Elrond 创始人兼首席执行官 Beniamin Mincu 发推称，Elrond 生态 DEX 项目 Maiar 此前出现的 bug 已经解决，几乎所有被盗取的资金都已被追回。已知错误造成的剩余缺失资金都将由 Elrond 基金会全额承担。

4/ Nearly all of the exploited funds have already been recovered in this address:
erd1pml9k2tsqsnvtmmalgt2su0sn3cguvr8e8jq0gy69zw2ldcej2qapml9a

Any remaining missing funds caused by the known bug, will be covered in full by the Elrond Foundation.

6:45 AM · Jun 8, 2022 · Twitter Web App

随后，Beniamin Mincu 发推表示，Maiar DEX 已完全恢复，DEX 和 API 均已重启上线。

Maiar DEX full recovery is complete.

The DEX is now live. APIs are live. Exchanges are live.

All funds are safe, all users are safe.

Carefully monitoring everything during the next hours.

Super though 48 hours. Amazing efforts and support from the team, community, partners.

6:20 PM · Jun 8, 2022 · Twitter Web App

数据五

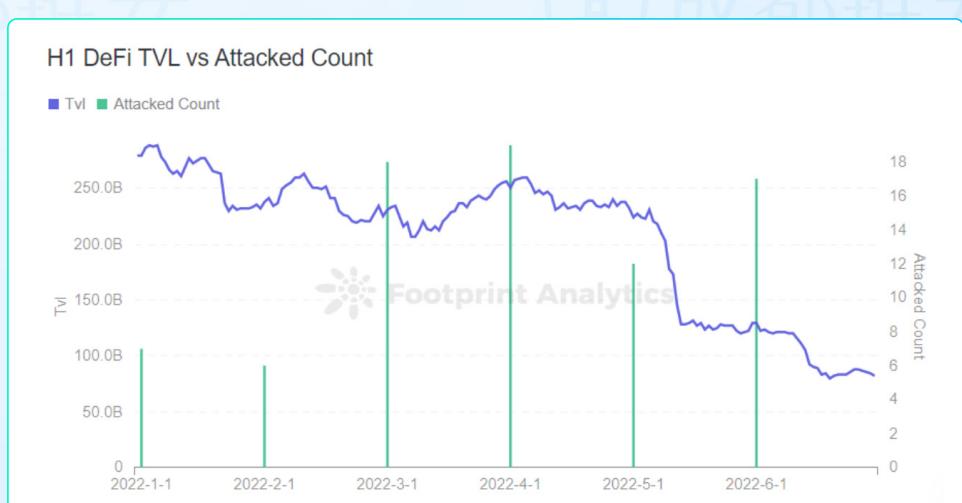
整个DeFi TVL从1月初的2798亿美元跌到了6月末的824亿美元，下跌70.5%

整个DeFi TVL从1月初的2798亿美元跌到了6月末的824亿美元，半年下跌70.5%。其中，TVL在5月和6月累计跌幅就达到了63.2%，光是5月5日至5月13日几天内就跌去了44.5%。

从攻击活动损失金额和攻击次数综合来看，3月、4月为黑客活跃程度最高的月份，同样3月、4月的TVL也处在半年的相对高点。5月TVL骤降，黑客攻击频次和盗取金额随之大幅降低。6月TVL持续降低，黑客活跃度较5月有所增加，但相对于3、4月仍是低位。

1月TVL虽然处于半年来最高位，但黑客活跃程度却相对较低。通过比对2021年1月的数据，我们发现2021年1月因黑客活动造成的损失约为25万美元，也处于全年相对的低位。因此，2022年1月黑客活跃度较低的原因或是因为1月是历来黑客活动的淡季。

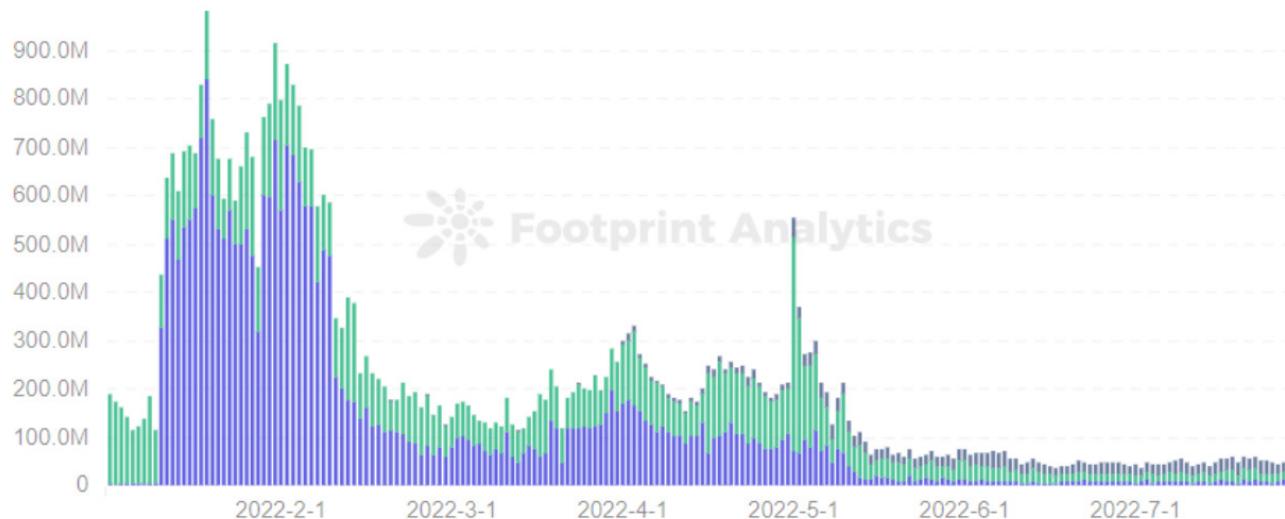
抛开淡季的因素，黑客攻击事件与市场行情走势是有一定关联性的。链上资金的增加会吸引更多黑客的目光。



除了DeFi以外，NFT、GameFi等各大赛道上半年也出现了明显的周期波动。其中GameFi的市值走势与加密货币市值走势（以BTC为例）大致趋同，均在五六月份出现了比较明显的市值缩水。而NFT的交易量在2月达到了今年上半年以来的最高峰，随后持续走低，直至上半年结束时都处于比较低迷的状态。

NFT Marketplace Trading Volume on Ethereum

■ looksrare ■ opensea ■ x2y2



以太坊NFT市场交易量走势

H1 GameFi Token vs BTC MC

■ Q2 GameFi Token MarketCap ■ Q2 BTC MarketCap



上半年GameFi及BTC市值走势

数据六

黑客通过Tornado Cash共洗钱11亿4070万美元

2022年上半年，约有11亿4070万美元的被盗资金被黑客转进了Tornado Cash，约占总损失金额的60%。约有6亿3536万美元的被盗资金暂时还存放在黑客地址。

据统计显示，2022年上半年共有95000枚以太坊（约合23亿4000万美元）存入了Tornado Cash。也就是说，存入Tornado Cash里的资金至少有48.7%都来源于黑客。这还是在假设剩余所有人使用Tornado Cash作为交易隐私工具的情况下。事实上还有相当一部分人使用Tornado Cash进行加密货币犯罪交易，此类数据不在本报告的统计范围之内。

黑客为何偏好用Tornado Cash进行洗钱？进入Tornado Cash的被盗资金一定无法追回吗？

黑客为何偏好用Tornado Cash洗钱？

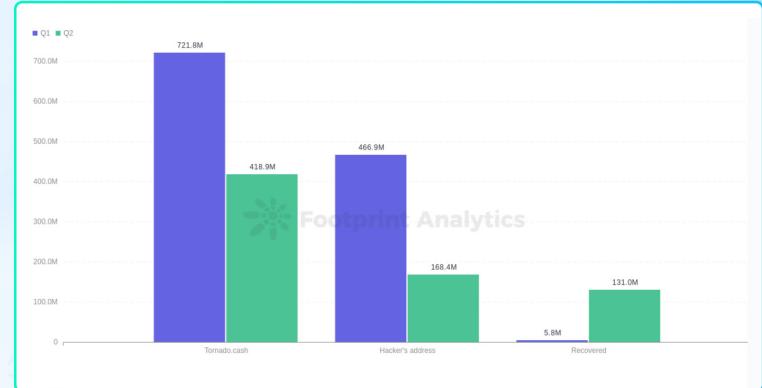
Tornado Cash 是基于 ZK-SNARK（也称零知识简洁非交互式知识论证）技术的以太坊和其他支持智能合约的区块链的去中心化、非托管隐私解决方案。它可以通过打破源地址（存款人）和目标地址（取款人）之间的链上连接来提高交易隐私。Tornado Cash的用户想要将一笔资产进行匿名转移或者混币，先需要将资产转移至Tornado Cash的智能合约上，Tornado Cash给用户一个随机生成的密钥作为凭据，此凭据可以证明你已经执行了存款，但未透露原始地址；取出时只需向Tornado Cash提交之前系统给予的随机密钥，同时用户提交一个新地址后，智能合约会将资产转到新地址中并完成资产的“混币”，这样就无法追溯到该笔交易了。这也是大多数黑客选择Tornado Cash的原因。

进入Tornado Cash的资金一定无法追回吗？

虽然混币技术增强了链上交易的匿名性和隐私性，但也被滥用于洗钱等犯罪，混币技术增加了犯罪资产的链上追踪难度。但是黑客采用Tornado Cash进行洗钱过程中，也会暴露出一些数据痕迹。通过对黑客所有转到Tornado 的地址和金额进行金额聚合，同时对单位时间内所有从Tornado Cash转出的目的地址和金额进行金额聚合，进而对混币充币金额与混币提币金额进行关联匹配，从而达到黑客入金地址与出金地址关联进行违法资金的追踪。

成都链安作为一家致力于区块链安全生态建设的公司，成都链安同时致力于全链条打击虚拟货币犯罪能力建设体系，提供全链条打击虚拟货币犯罪的服务+产品。

依托协助执法部门破获数百起区块链犯罪案件的经验积累（包括数起进入Tornado 的案件），以案件研判过程为场景切入打造的契合执法机构办案流程的虚拟货币案件智能研判平台——链必追。能为执法机构提供链上线索发现、链上行为刻画、资金追溯溯源、混币穿透、调查取证、判例库等一站式虚拟货币犯罪分析研判技战术能力，解决执法机构面对新型虚拟货币犯罪案件侦破难的痛点问题。如果您在案件侦办过程中，遇到资金追踪、洗钱活动技术协助需求，可直接联系我们（仅限执法人员）。



上半年被盗资金流向



数据七

约71%的攻击发生在DeFi领域

2022年上半年，整个区块链生态共发生79起较大的安全事件，其中涉及DeFi安全的共有56起，占比71%；损失金额达5.5亿美元。DeFi为什么是黑客攻击重点？DeFi有哪些最佳安全实现方式？

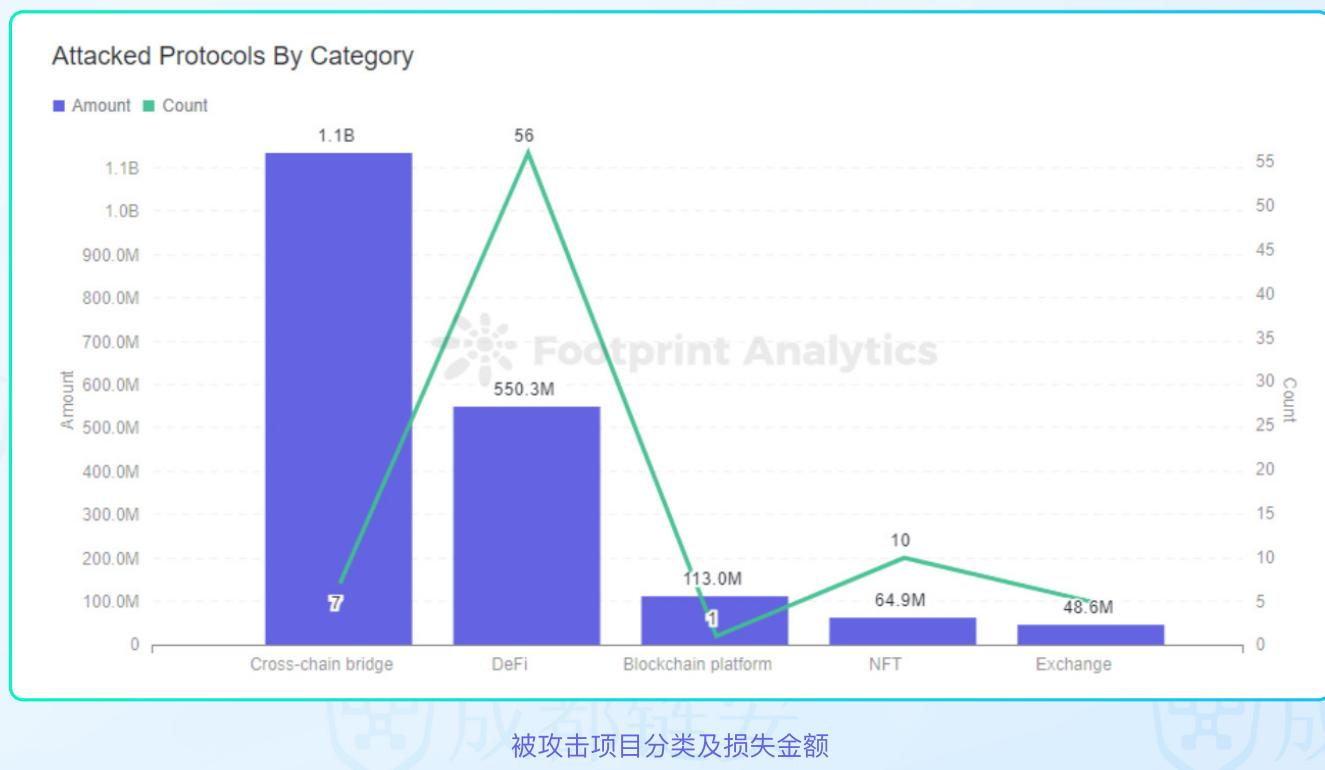
◆ 1 DeFi是什么？

DeFi即Decentralized Finance，去中心化金融。是一种用于构建开放式金融系统的去中心化协议，该协议建立了一套具有透明度、可访问性和包容性的点对点金融系统，将信任风险最小化，让参与者更轻松便捷地获得融资。

当前DeFi生态中的项目多种多样，各种金融功能的项目交互对接，某些大型项目甚至是金融领域中大多金融功能的集合，形成了一个庞大的去中心化金融网络。DeFi生态目前按照功能分类主要包括交易、借贷、资产管理、稳定币、金融设施、保险、衍生品、交易平台等。

◆ 2 DeFi为什么是黑客攻击重点

根据数据显示，2022年上半年，整个区块链生态共发生79起较大的安全事件，其中涉及DeFi安全的共有56起，占比71%；损失金额达5.5亿美元。在web3.0世界里，DeFi已经成为黑客攻击的重灾区。

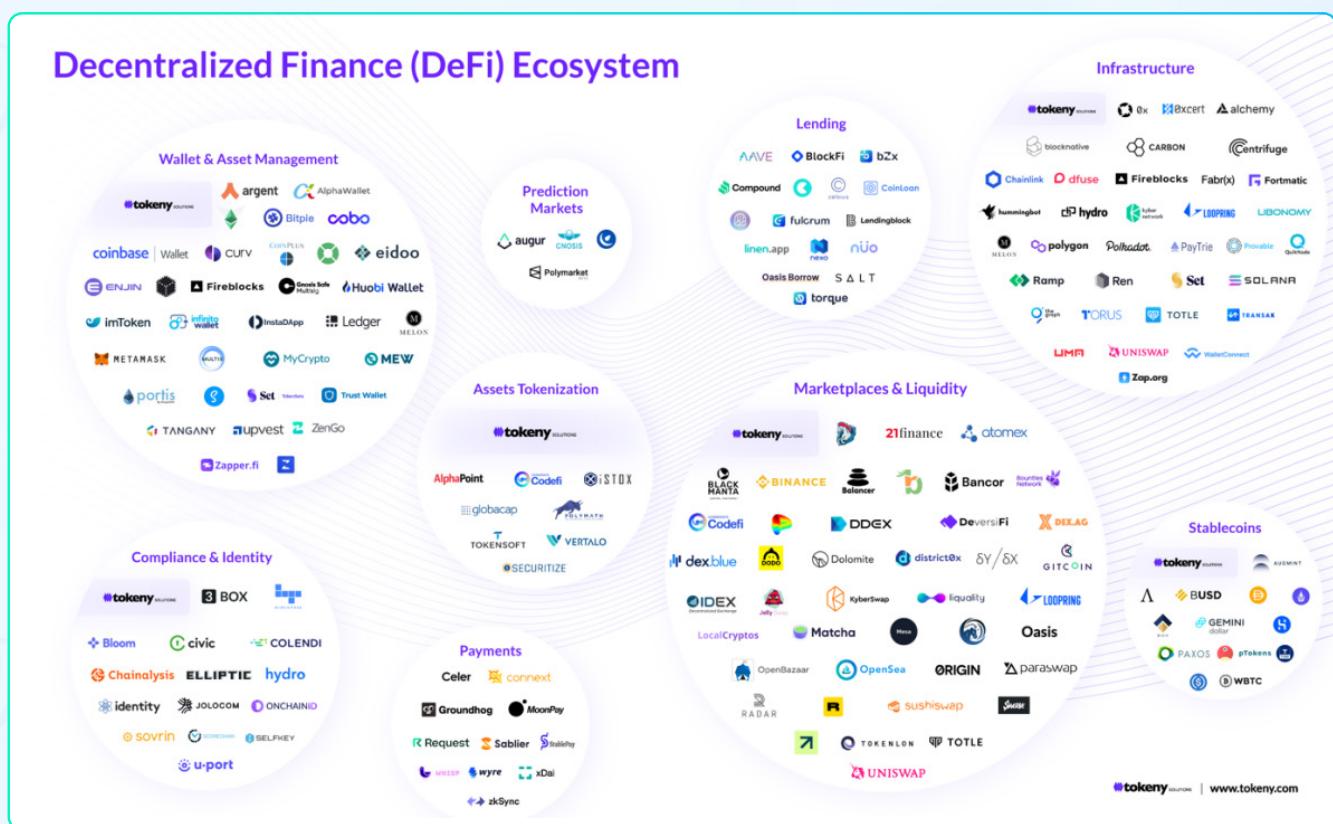


那么，DeFi为何成为了web3.0世界里黑客攻击的重灾区呢？

(一) DeFi活跃度高。作为区块链最火的领域，DeFi从诞生开始就备受关注。活跃度高，参与的项目和用户自然也越多，也就更容易被黑客列为攻击目标。

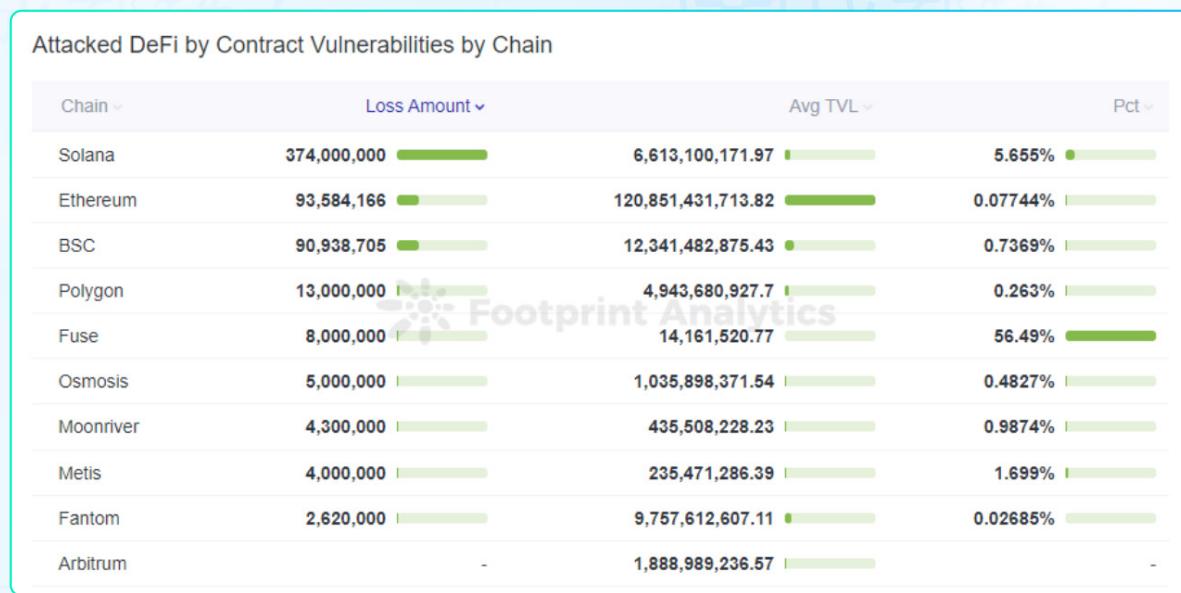
(二) 资金量大。统计数据显示，截止6月30日，DeFi总锁仓量高达824亿美元。虽然今年以来，加密行业市值缩水，DeFi的TVL也大量下滑，在加密行业整体市值下跌的大背景下，DeFi相对来说仍保持着巨额资金。如此巨大的资金量，则无疑是对黑客最好的吸引。

(三) DeFi业务逻辑复杂。如今，DeFi 生态越来越庞大，其业务的复杂度也越来越高。又因为DeFi产品之间也有较强的可组合性，这导致不同DeFi产品之间产生了流通性和资产共享。因此，DeFi业务逻辑上的复杂度，加上产品之间的组合和交互，就很可能会导致一些安全问题，从而被黑客抓住其中的机会。



DeFi生态系统

(四) 不少开发者缺乏安全意识，低估了漏洞的风险。数据显示，上半年DeFi项目中共发生33起因合约漏洞遭受的攻击。其中，最常见的是由代码逻辑错误引发的安全问题。



各链平台因合约漏洞攻击造成的损失占该链平台平均TVL百分比

◆ 3 DeFi最佳安全实现

全面的外部安全审计、符合安全规范的编码和测试网络环境下的模拟测试是确保DeFi项目安全的最佳实现。

上述提到的代码级别技术规范问题，如果在项目上线前，接受第三方安全审计，是可以将问题扼杀在摇篮之中。或许正是出于这样的考虑，许多DeFi项目逐渐开始认识到安全审计的重要性，并选择资质过硬的安全公司加以执行。

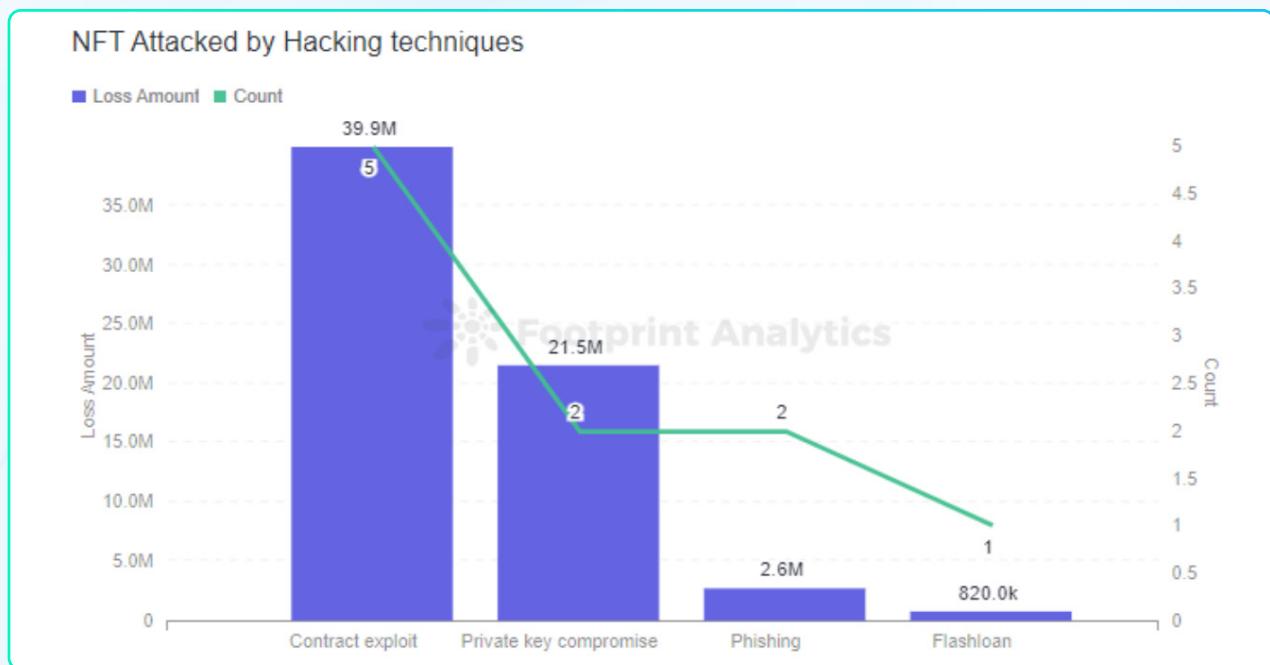
而从投资者的角度看，要选择投资DeFi项目，如果候选项目自身加持“已审计”标签，其受信程度自然会提高不少。毕竟，类似Uniswap这样的头部DeFi项目也无法幸免黑客利用合约漏洞盗取资产的宿命。投资者单靠热度进行投资判断，其中泡沫不知深浅，很容易导致投资失败。有投资者甚至表示，安全审计与否，是他对一个DeFi项目的可信度和风险评估最重要的参考指标。

审计完成后，下一阶段就是启动局部范围的真实网络测试。这是识别网络上所有错误的大好机会，可以邀请热心的社区成员和团队来参与测试智能合约。

数据八

NFT领域主要安全事件10起，损失约为6490万美元；NFT钓鱼事件频发

2022年上半年，共监测到NFT领域主要安全事件10起，统计到的损失约为6490万美元，主要攻击方式为合约漏洞利用、私钥泄露、钓鱼等。而上半年Discord钓鱼事件频发，几乎每天都有Discord服务器受到攻击，个人用户因点击钓鱼链接而遭受损失的情况频繁发生。



上半年NFT典型安全事件

TreasureDAO事件

2022年3月3日，TreasureDAO交易平台遭到黑客攻击，造成100多个NFT 被盗。

漏洞原因：逻辑漏洞

该漏洞存在于TreasureMarketplaceBuyer合约中，该合约的buyItem函数在传入_quantity参数后，并没有做代币类型判断，直接将_quantity与_pricePerItem相乘计算出了totalPrice，因此safeTransferFrom函数可以在ERC-20代币支付数额只有0的情况下，调用TreasureMarketplace合约的buyItem函数来进行代币购买。本次安全事件主要原因是ERC-1155代币和ERC-721代币混用导致的逻辑混乱，ERC-721代币并没有数量的概念，但是合约却使用了数量来计算代币购买价格，且最后在代币转账的实现中也未进行逻辑分离。

APE Coin空投事件

2022年3月17日，黑客通过闪电贷拿到了超过6万的APE Coin空投。

漏洞原因：逻辑漏洞

该漏洞存在于AirdropGrapesToken空投合约中，由于其使用 alpha.balanceOf()和beta.balanceOf()判定调用者对BAYC/MAYC NFT的所有权。而这种方式仅能获取到用户对该NFT所有权的瞬时状态，但该瞬时状态可以通过闪电贷借入进行操控。攻击者利用该漏洞，以闪电贷借出BAYC NFT并获取对应的空投。

Revest Finance事件

2022年3月27日，Revest Finance项目遭遇黑客攻击，损失余额12万美元。

漏洞原因：ERC-1155重入

该漏洞存在于Revest合约中，当用户采用depositAdditionalToFNFT()追加FNFT的抵押资产时，合约需要将先把之前的FNFT销毁，之后再铸造新的FNFT。但是在铸造时，由于min()函数中未判断需铸造的FNFT是否已经存在，并且状态变量fnftId自增在_mint()函数后。而_min()中存在ERC-1155中的隐藏外部调用_doSafeTransferAcceptanceCheck()，造成了重入漏洞。

NBA薅羊毛事件

2022年4月21日，NBA项目方遭遇黑客攻击。

漏洞原因：签名冒用和复用

该漏洞存在于The_Association_Sales合约中，项目当在采用签名校验的方式验证白名单时，主要存在两个安全问题：签名冒用和签名复用。其中签名复用问题是由于项目方并未在合约中存储已经使用过的签名，造成签名可以被攻击者重复多次使用；签名冒用的问题是由于vData memory参数info在传参时未进行msg.sender校验导致签名可冒用。

Akutar事件

2022年4月23日，NFT项目方Akutar的AkuAuction合约由于智能合约本身漏洞，导致11539ETH（价值约3400万美元）被锁死在合约中。

漏洞原因：逻辑漏洞

该合约存在两个逻辑漏洞，第一是退款函数processRefunds使用call函数进行退款操作，并且把退款结果作为require判定条件，如果攻击者在fallback中进行恶意revert会导致整个合约的退款操作无法继续进行。第二个漏洞是造成此次事件的根本原因，即退款函数中存在的两个判断条件，由于没有考虑到一个用户可以投标多个NFT的情况，使得项目方后续的退款操作永远无法执行。

XCarnival事件

2022年6月24日，NFT 借贷协议 XCarnival 遭到攻击，黑客获利 3087 枚以太坊（约 380 万美元）。

漏洞原因：逻辑漏洞

该漏洞存在于XNFT合约中，该合约中的pledgeAndBorrow 函数在质押NFT时并未检查攻击者传入的xToken 地址是否为项目方白名单中的地址；并且在借贷时，并未对抵押记录的状态进行检测，导致攻击者反复使用无效的抵押记录进行借贷。

NFT合约安全

上半年发生了多起NFT合约相关的安全事件，主要原因还是没有进行全面的安全审计。那么NFT合约在审计过程中都会出现哪些常见问题呢？

成都链安审计团队在审计NFT系列合约时，发现NFT合约主要的问题包括以下几类：

1) 签名冒用和复用：

签名数据缺少重复执行验证(例如：缺少用户nonce)，导致可以重复使用签名数据铸造NFT；

签名检查不合理(例如：未检查签名者为零地址的情况)，导致任意用户均可通过检查进行铸币；

2) 逻辑漏洞：

合约管理员可以通过私募等特殊方式铸币而不受总量的限制，导致NFT的实际量超过预期；

拍卖NFT时，获胜者可在领取交易顺序依赖攻击，修改竞拍价格，导致竞拍获胜者可以低价获取NFT；

3) ERC721&ERC1155重入攻击

当合约使用转账通知功能时(onERC721Received函数)，NFT合约会主动向转账的目标合约发送一次调用，那么这就可能导致重入攻击；

4) 授权范围过大

用户在进行质押或者拍卖时，仅需要对单个代币授权，但合约要求_operatorApprovals授权，一旦用户授权成功，那么就存在NFT被盗的风险。

5) 价格操控

NFT的价格依赖于某合约的代币持有量，导致攻击者利用闪电贷拉高代币价格，使得质押的NFT被异常清算。

从上半年发生的NFT合约安全事件来看，审计过程中经常出现的漏洞在实际中也会被黑客利用。因此寻求专业的安全公司对NFT合约进行审计也是非常有必要的。

钱包安全

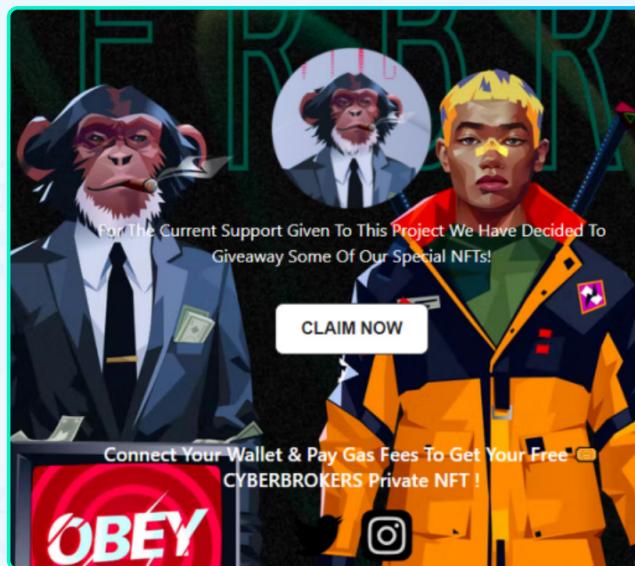
区块链中钱包安全的重要性不言而喻，对于个人用户而言，今年由于钓鱼事件频发造成大量用户钱包资产被盗；对于项目方而言，今年也发生多起私钥泄露相关事件，造成大量项目资产被盗。下面将针对危害个人用户的钓鱼攻击和危害项目方的私钥泄露事件分别进行介绍。

钓鱼

目前的钓鱼手法通常会以各种方式诱骗用户对钱包授权，从而危害钱包安全，以下是几种常见的钓鱼手法：

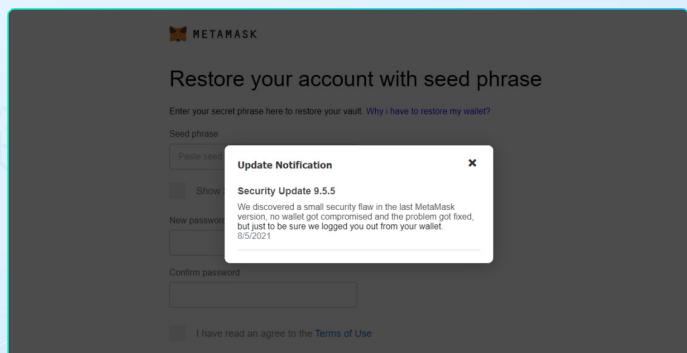
假空投

该类钓鱼网站主要是利用假空投等手段，诱骗用户访问钓鱼网站。在用户连接钱包后，就会出现“CLAIM NOW”等引诱用户进行点击的按钮，用户点击之后就会对钓鱼网站的黑地址进行授权。目前成都链安的钓鱼插件已经发现数个类似的钓鱼网站，如：



诱骗用户填写助记词

该类钓鱼网站主要是在网页连接钱包处，或者其他位置诱骗用户点击，之后弹出一个伪造的网页，提示用户诸如“MetaMask插件版本需要升级”等信息。如果用户相信并填写了自己的钱包助记词，那么用户的私钥就会上传到攻击者服务器导致用户钱包被盗。



APP假钱包

该类假APP钱包通常通过以下三种方式诱骗用户下载，第一种方式是通过购买搜索引擎的广告位，诱骗用户访问虚假的钱包官网进行下载，如：2022年5月10日，Sentinel 创始人 Serpent发文称有钓鱼网站利用Google广告漏洞将其URL伪装得与官网URL极为相似，从而使得用户受到攻击；第二种方式是向受害者发送邮件、海报等，引诱用户下载假钱包；第三种方式是通过社工的方式，首先获取受害者信任，然后再诱骗其下载假APP钱包。上述方式涉及到的假钱包几乎包括目前主流的所有钱包，如：imToken、MetaMask等。

Discord钓鱼

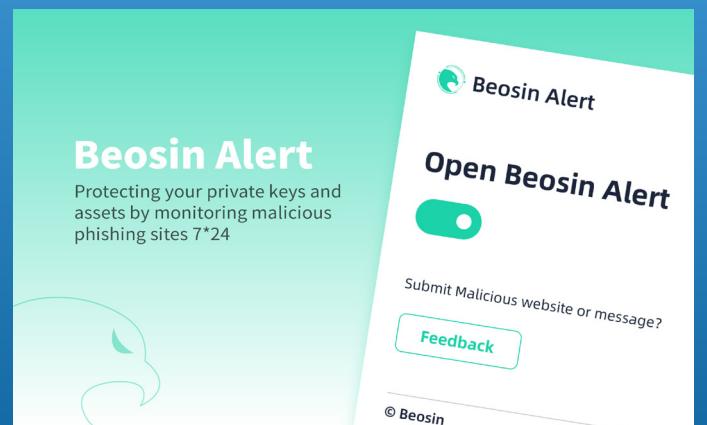
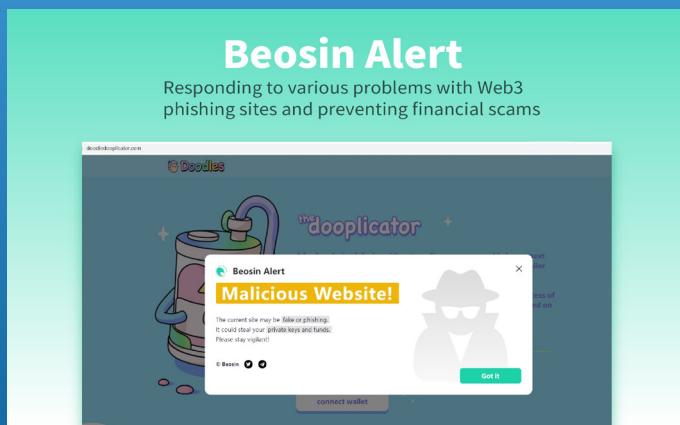
该类钓鱼方式主要是NFT项目的Discord 被攻击，攻击者获取到Discord的管理员权限，然后在Discord中发布钓鱼链接，诱骗用户点击从而危害其钱包安全。或者直接获取到服务器的管理员权限，要求用户通过共享屏幕等方式进行身份验证，从而盗取用户私钥等信息。

如何有效防范钓鱼？

反钓鱼插件

由于NFT项目的火爆，各种钓鱼网站层出不穷，仅靠用户自己进行识别已经很难防范，因此建议用户在浏览器上安装反钓鱼插件。这类插件可以识别出用户当前访问的web3站点是否为钓鱼、诈骗等类型的恶意网站。

安装下面这款反钓鱼插件，可辅助识别部分钓鱼网站。**(复制链接谷歌浏览器直接安装↓)**



<https://chrome.google.com/webstore/detail/beosin-alert/lgbhcpagiobjacpmcgckfgodjeogceji?hl=zh-CN>

防范签名被盗

目前多数网站为了保护用户安全已经不支持盲签的签名方式，但是如果用户访问某些网站时仍然遇到盲签的情况，请尽量拒绝签署。

1. 用户签署交易时需要确认签署的内容；

2. 用户在进行交易签名前，应进行多方信息交叉验证，确保发起交易的网站是真官网；

识别NFT官网

一般在访问NFT官网时，首页通常有官方社交媒体账号，如：twitter、discord等。且目前很多NFT官方网站都不会直接提供“mint”功能，或将更多数量的NFT放到了诸如X2Y2/Opensea之类的交易所上进行售卖。用户可以访问这些社交账号，首先识别其账号是否是官方账号，通常直接在twitter上搜索项目名称可以发现官方账号，如果存在同名的情况那么注意筛选出认证账号或是关注人数较多的账号，当然能也需要警惕钓鱼大号，最好是进行信息的交叉验证，确保自己访问的是官网。

资产隔离

在进行这类危险交易时，可以采用资产隔离的方式进行，比如：用户可以将钱包根据用途分为两类，第一类用于存储资产，包括一些大额资产等，该类资产可以使用冷钱包存储提高安全性；第二类用于资产交易，尤其是在进行诸如领取空投这样的危险交易时，可以使用一些临时钱包，如：Burner Wallet。

私钥安全

今年上半年已经发生多起因项目方私钥泄露事件且涉及金额巨大，例如6月Harmony跨链桥因私钥泄露损失约1亿美元。项目方应以用户资产安全为核心，做好钱包安全、智能合约等相关模块的风险评估和安全审计，保证系统安全。下面列举了几种保证私钥安全的相关建议：

多签地址

项目方应该使用多签地址，其需要多个私钥持有者的授权才能进行钱包交易。同时持有者的数量应当在一个合理的范围内，过少也可能会造成安全问题。

风险评估

项目方应该对系统进行一个全面的安全评估，避免因为服务器等存在的安全问题造成私钥泄露。

Validator安全

建议项目方在设计验证者节点时，尽量选择较多节点。同时尽量使用硬件钱包保护私钥。

从整个加密货币市场上半年行情走势来看，DeFi、NFT、GameFi等各大赛道发展总趋势都是持续走低。整个DeFi总锁仓量从1月初的2798亿美元跌到了6月末的824亿美元，半年下跌70.5%。分析发现，黑客攻击事件频率与市场行情走势呈现出一定的关联性。五六月份在TVL大幅缩水的情况下，黑客攻击事件相对于前几个月有所减少，更多的链上资金会吸引更多黑客的目光。

上半年发生7起跨链桥攻击事件，共损失11亿3599万美元。跨链桥的攻击手法主要为合约漏洞利用、私钥泄露和线下程序缺陷。对项目方而言，安全审计、线下风控、定期检查签名服务器、对签名者严格审查、版本更新时重新进行安全评估、制定漏洞赏金计划等都是保障跨链桥项目安全运行的有效手段。

在上半年的攻击事件中，约53%的攻击方式为合约漏洞利用。通过对审计过程中常见漏洞和实际被利用漏洞进行比对，可以发现，大部分漏洞在审计阶段都能检测出来，如逻辑漏洞、重入漏洞等。成都链安VaaS能在项目合约开发阶段，对代码进行自动的形式化验证，包括代码规范检测、标准规范检测、函数调用检测和业务逻辑安全检测（试用链接：<https://vaas.lianantech.com>）。通过工具加上审计专家人工检测，成都链安审计服务能在项目上线前提供全面的安全保障，极大减少项目被攻击的风险。

另外还有26.6%的闪电贷攻击事件造成了3亿3291万美元的损失，除了采用一些措施如时间加权平均定价（TWAP）、更高频率的价格更新机制、更严格的治理逻辑等之外，还可使用一些工具及时监控闪电贷。

上半年，共发生了5起损失过亿的安全事件，而好消息是，这5个被攻击的项目均在一段时间后发布了补救措施并重新上线。在过往的事件里，反倒是一些资金量中小规模的项目方，在遭到了重大攻击后将会很难重启。

2022年上半年，约有11亿4070万美元的被盗资金被黑客转进了Tornado Cash，约占总损失金额的60%。虽然混币技术增强了链上交易的匿名性和隐私性，但也被黑客滥用于洗钱等犯罪。成都链安在过往的案例中，已有数次成功分析黑客数据痕迹并追踪Tornado Cash的经验。截止报告发布时，美国财政部已经宣布将Tornado Cash列入制裁名单。可以预测，未来极有可能会出现更多新型的洗钱方式，隐蔽性和技术追踪难度更高，执法难度将会进一步加大。

作为头部区块链安全企业，成都链安自成立以来，不断打造区块链安全颠覆性和核心技术，基于网络信息安全、形式化验证、人工智能和大数据分析等多重先进技术打造了“链必安一站式区块链安全服务平台”，涵盖了行业顶尖的安全产品 and 安全服务。

截至目前，成都链安已与工信部、中国通信院、网信办、公安等执法监管部门和国内外头部区块链企业建立了深度合作；为全球2000多份智能合约、100多个区块链平台和落地应用系统提供了安全审计与防御部署服务；具备全链条打击虚拟货币犯罪的技术服务能力，为公安等执法部门提供案件前、中、后期全链条技术支持服务500+，成功协助破获案件总涉案金额数百亿。（包括数起进入Tornado 的案件）

未来我们将持续探索，助推Web3生态的安全建设，继续为全球区块链安全生态保驾护航。

*特别鸣谢Footprint Analytics对本报告的图表及数据支持。本报告中所有图表均可通过以下链接进行在线查看：<https://www.footprint.network/@Beosin/Footprint-Beosin-H1-2022-Report>

成都链安介绍

让区块链生态更安全

SECURING YOUR BLOCKCHAIN ECOSYSTEM

成都链安科技有限公司（简称成都链安）是一家致力于区块链安全生态建设的全球领先的区块链安全公司，也是最早将形式化验证技术应用到区块链安全的公司。2018年3月由电子科技大学教授、博士后联合创立，团队成员均来自从事信息安全行业多年的国内外知名院校教授、博士后、博士以及企业精英。现有团队成员近200人，技术人员占比85%。

成都链安已获前海母基金、联想创投、复星高科、成创投、任子行等知名机构的多轮投资，已与工信部、信通院、网信办、公安等执法监管机构建立了深度合作。获得软件发明专利和著作权30多项。自主研发的“链必安”一站式区块链安全服务平台可为执法监管机构、金融机构、区块链企业等提供安全审计、安全防护、安全监管、安全预警、安全咨询等全生命周期安全保障解决方案。同时具备全链条打击虚拟货币犯罪的技术服务能力，为公安等执法部门提供案件前、中、后期全链条技术支持服务。

核心技术

网络安全

智能合约形式化验证

人工智能

大数据分析

隐私计算

虚拟货币反洗钱和监管

内核安全

区块链安全相关技术

产品服务

安全产品

智能合约形式化验证平台

虚拟货币案件智能研判平台

区块链安全态势感知平台

区块链安全舆情平台

区块链安全检测平台

联盟链智能合约安全开发IDE

安全服务

智能合约安全审计服务

链平台安全检测服务

虚拟资产追踪溯源及调查取证服务

安全舆情服务

安全咨询服务

安全应急响应服务

声明

本报告版权为成都链安所有，其他第三方不得出于任何目的传输、披露、引用、依赖或篡改出具的报告。其中的任何描述、表达或措辞均不得被解释为对该项目的肯定或确认，此外成都链安出具的相关报告内容绝不提供任何项目的投资建议，也不应作为任何类型的投资建议加以利用。本报告代表了一个广泛的评估过程，旨在帮助用户提高安全风险预估，同时降低区块链技术带来的高风险。

028-83262585

market@lianantech.com

www.lianantech.com



成都链安官方公众号



业务咨询