成都链安 | Footprint Analytics

2022

成都链安Q2全球WEB3安全生态报告

www.lianantech.com

让区块链生态更安全

SECURING YOUR BLOCKCHAIN ECOSYSTEM

目录

CONTENTS

https://www.footprint.network/@Beosin/Footprint-Beosin-Q2-Report

1. 2022第二季度Web3安全态势综述

主要攻击事件超48起，总损失约7亿1834万美元

2022年第二季度，**成都链安链必应-区块链安全态势感知平台**共监测到Web 3领域主要攻击事件超48起，总损失约7亿1834万美元，较第一季度的12亿美元下降约40%，约是2021年第二季度损失（2亿9656万美元）的2.42倍。

2022年1-6月，Web 3领域因攻击事件损失的总金额已达约19亿1287万美元。

Q Over Q Growths

Date	Total Loss
2022-Q1	1,194,525,820
2022-Q2	718,343,550
Quarter-over-quarter	-0.3986

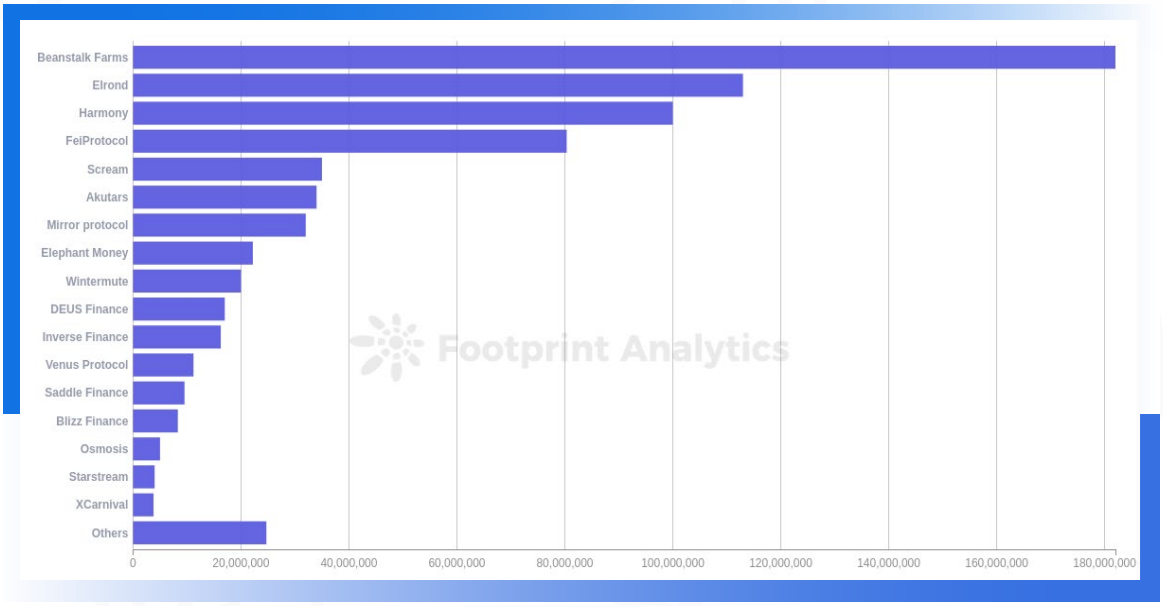
Q on Q Growths

Date	Total Loss
2021-Q2	296,560,000
2022-Q2	718,343,550
Quarter-on-Quarter	1.42

- 从时间上来看，4月是黑客攻击最活跃的月份，5月攻击事件数量和损失金额都出现了大幅下降，6月黑客活跃度有回升趋势。
- 从TVL（总锁仓价值）来看，所有的链和被攻击的项目的TVL值在5月都出现了大幅下降。大部分项目在遭受攻击的时间点之后都会出现TVL骤降的情况。
- 从攻击手法来看，最常见的攻击手法依旧为合约漏洞利用和闪电贷。约有45.8%的攻击为合约漏洞利用。因闪电贷造成的损失达2亿3300万美元，居各种攻击方式损失金额第一位。
- 从审计情况来看，被攻击的项目中，仅有52%的项目经过了审计。
- 从被攻击项目类型来看，DeFi依旧是被攻击次数最多的项目类型，约79.2%的攻击发生在DeFi领域。
- 从链平台来看，本季度Ethereum上损失的金额最多，达到了3亿8135万美元。被攻击频率最高的链为BNB Chain，达到了26次。
- 从资金流向来看，约4亿1889万美元的被盗资金被黑客转入了Tornado.cash，占该季度总被盗金额的58.3%。
- 其他方面，本季度共监测到链上主要Rug pull事件超43起，项目方共计卷走约3426万6402美元。据不完全统计，Discord服务器被黑案例超151个。Rug pull和钓鱼安全事件在5、6月份频发。

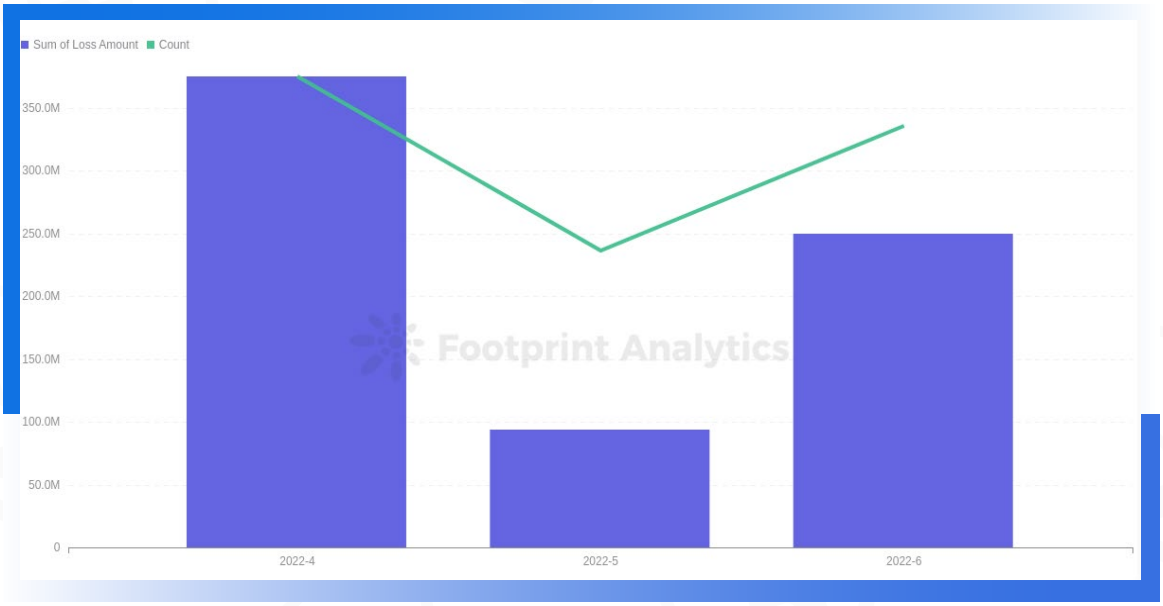
2. 攻击事件总览

4月是本季度黑客攻击最活跃的月份



2022第二季度，共监测到Web 3领域主要攻击事件超48起，总损失约7亿1834万美元。其中损失达一亿美元及以上的攻击事件3起，千万美元以上的攻击事件共12起，百万美元以上的攻击事件共28起。损失最高的前三为Beanstalk Farms、Elrond和Harmony，分别为1亿8200万美元、1亿1300万美元和1亿美元。

从时间上来看，2022年4月是本季度黑客攻击最活跃的月份，共发生19起主要安全事件，损失约为3亿7489美元。5月攻击事件数量和损失金额都大幅减少，或与5月整个加密货币市值大幅缩水有关。6月虽然行情并未见回暖趋势，但黑客攻击频率和项目损失金额却较5月大幅增加。

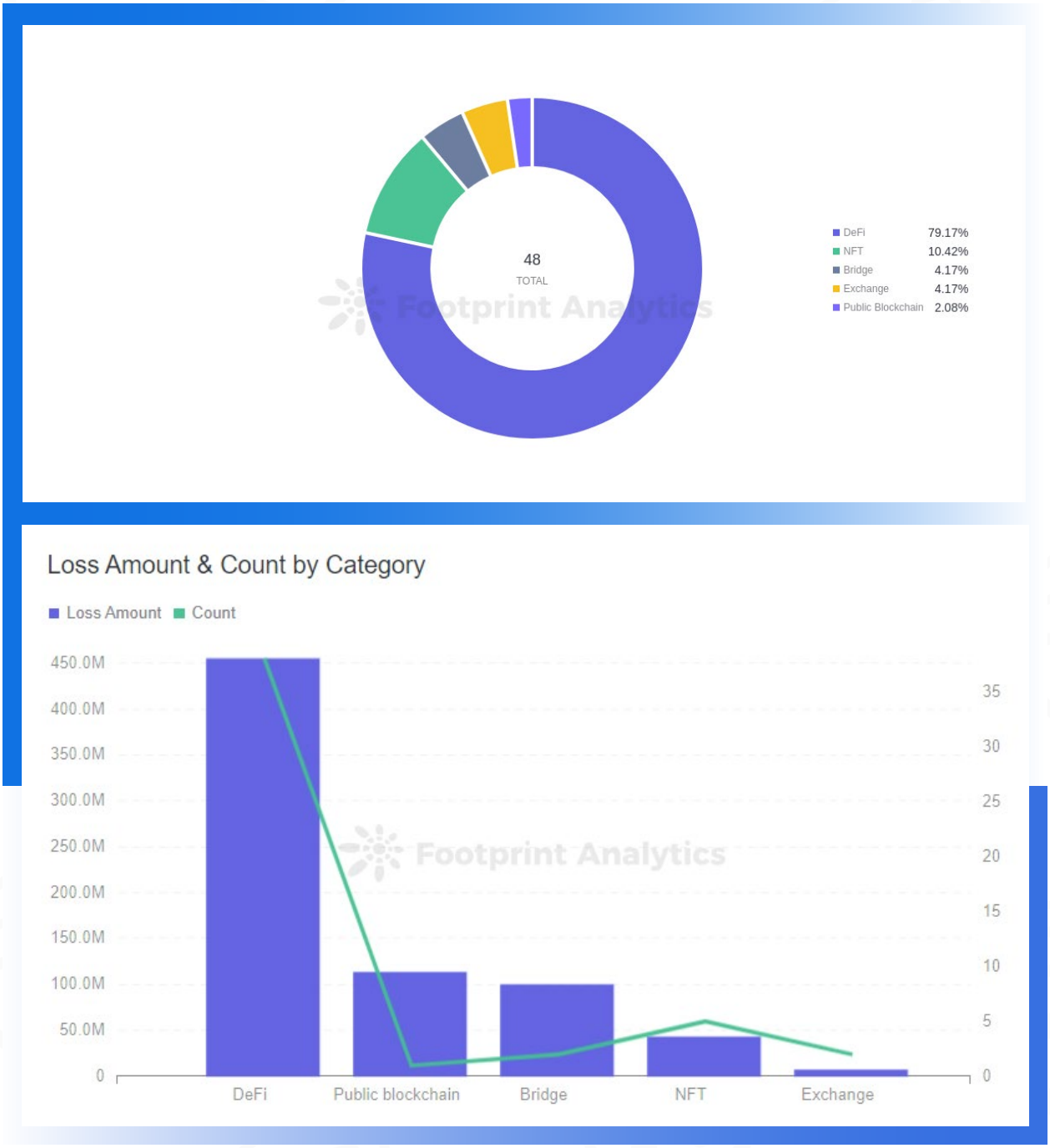


3. 被攻击项目类型

79.2%的攻击发生在DeFi领域

和第一季度相同，DeFi依旧是被攻击次数最多的项目类型，约79.2%的攻击发生在DeFi领域。其损失总金额约为4亿5474万美元，占到了Q2总损失金额的63.3%。

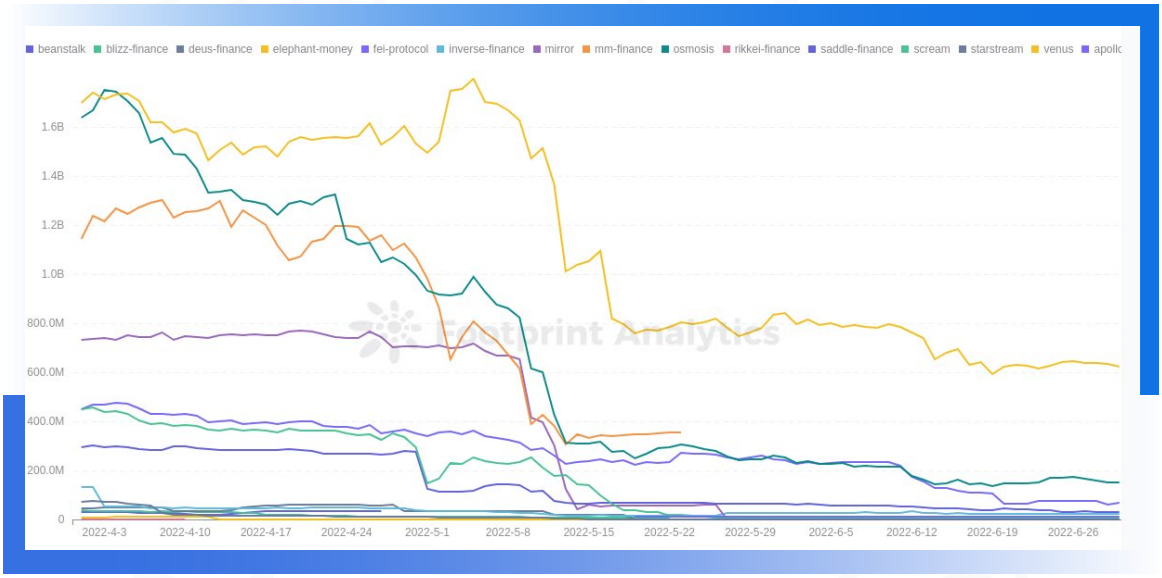
本季度依旧发生了两起跨链桥攻击事件，累计损失金额约为1亿美元。在2022年第一季度，4次跨链桥攻击的总损失为9亿5000万美元。至此，2022年上半年因跨链桥攻击造成的损失金额已达10亿5000万美元。



4. 被攻击项目TVL分析

部分项目在被攻击后TVL直接归零

从部分被攻击项目的TVL来看，5月几乎所有项目TVL都出现了集体缩水。大部分项目在遭受攻击的时间点之后都会出现TVL骤降的情况。一些项目在被攻击后TVL直接归零，例如Beanstalk、Blizz Finance。



从被攻击项目与被攻击时间的TVL比例来看，大部分情况下损失金额在项目TVL的30%以下。其中也有个别项目如Blizz Finance、Beanstalk，损失达到了TVL的100%甚至500%。

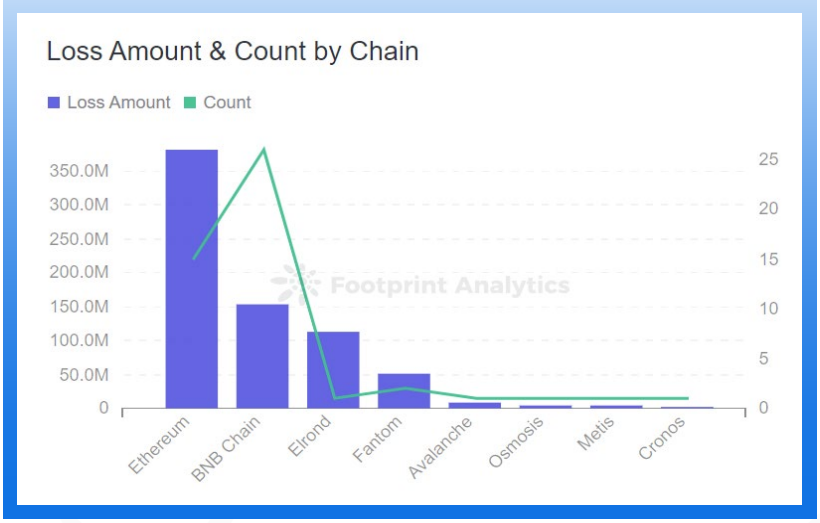
Date	Protocol Slug	TVL	Loss Amount	Pct
2022-4-2	inverse-finance	67,344,176	15,000,000	22.27%
2022-4-8	starstream	28,662,864	4,000,000	13.96%
2022-4-17	beanstalk	35,934,428	182,000,000	506.48%
2022-4-28	deus-finance	60,549,740.02	17,000,000	28.08%
2022-4-30	fei-protocol	352,825,568	80,340,000	22.77%
2022-4-30	saddle-finance	278,756,557.24	9,540,000	3.422%
2022-5-4	mm-finance	745,404,608	2,000,000	0.2683%
2022-5-13	blizz-finance	8,284,470.5	8,300,000	100.19%
2022-5-13	venus	1,012,455,104	11,200,000	1.106%
2022-5-16	scream	98,347,120	35,000,000	35.59%
2022-6-8	apollox	13,024,072	1,600,000	12.28%
2022-6-8	osmosis	220,895,040	5,000,000	2.264%
2022-6-16	inverse-finance	13,258,454	1,260,000	9.503%

5. 各链平台损失金额情况

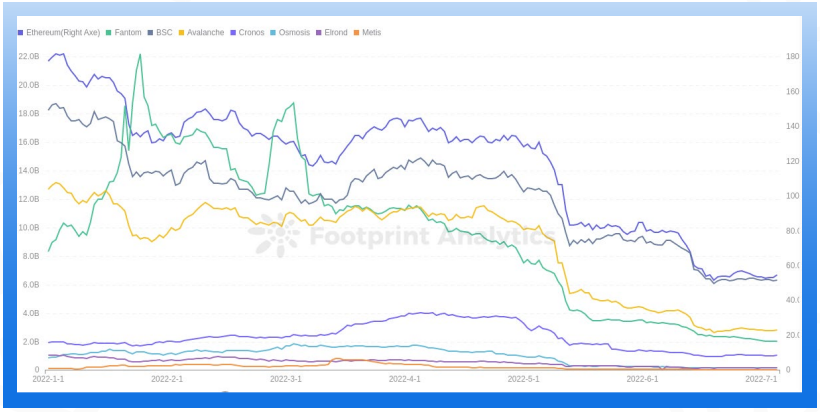
Ethereum上损失金额最多，BNB Chain攻击事件最多

本季度Ethereum上损失的金额最多，达到了3亿8135万美元。被攻击频率最高的链为BNB Chain，达到了26次。

和上一季度相比，连续两个季度都发生过攻击事件的链包括Ethereum、BNB、Fantom和Cronos。在第一季度因2次攻击事件造成了3亿7400万美元的损失的Solana链，在本季度并未监测到重大安全事件。



第二季度，所有的链TVL值在5月都出现了大幅下降。TVL排名前2的Ethereum和BNB Chain仍然是黑客攻击的主要目标。本季度攻击事件总共损失了7亿1834万美元，比6月时Osmosis、Elrond、Metis加起来的TVL总值都还要多。



Chain	Sum of Loss Amount	Avg TVL	Pct
Metis	4,000,000	123,950,280.75	3.227%
Fantom	52,000,000	5,824,023,179.65	0.8929%
BSC	49,539,085	10,551,478,231.19	0.4695%
Ethereum	340,900,000	98,980,928,368.9	0.3444%
Avalanche	8,300,000	6,945,411,851.15	0.1195%

Chain	Attacked Count	Q2 Total Protocal Count	Pct
BSC	23	324	7.099%
Metis	1	21	4.762%
Ethereum	11	428	2.57%
Fantom	2	211	0.9479%
Avalanche	1	181	0.5525%

从DeFi项目来看，以太坊上被攻击的DeFi项目金额最多，但占二季度TVL均值的比例并不高，Metis链损失的金额占TVL比例反而最高。占比最小的为Avalanche。

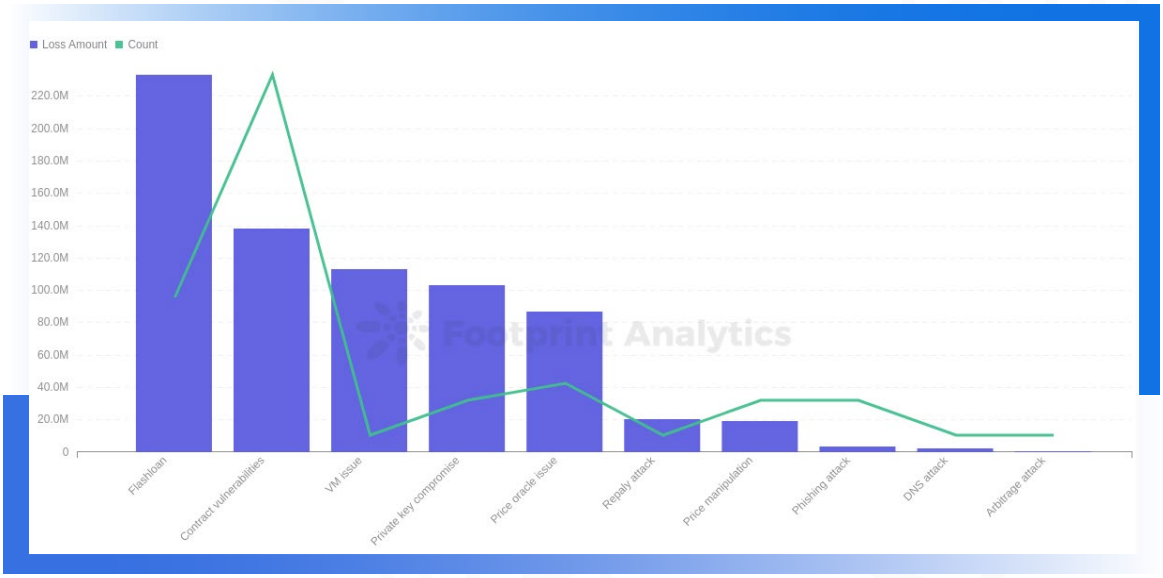
从DeFi协议被攻击的次数上看，二季度BNB Chain上被攻击的DeFi协议占其总协议数量的比例最高，达到了7%。Metis上DeFi生态还不够丰富，虽然仅1笔攻击，但不论在笔数和金额上都占比较高。

6. 攻击手法分析

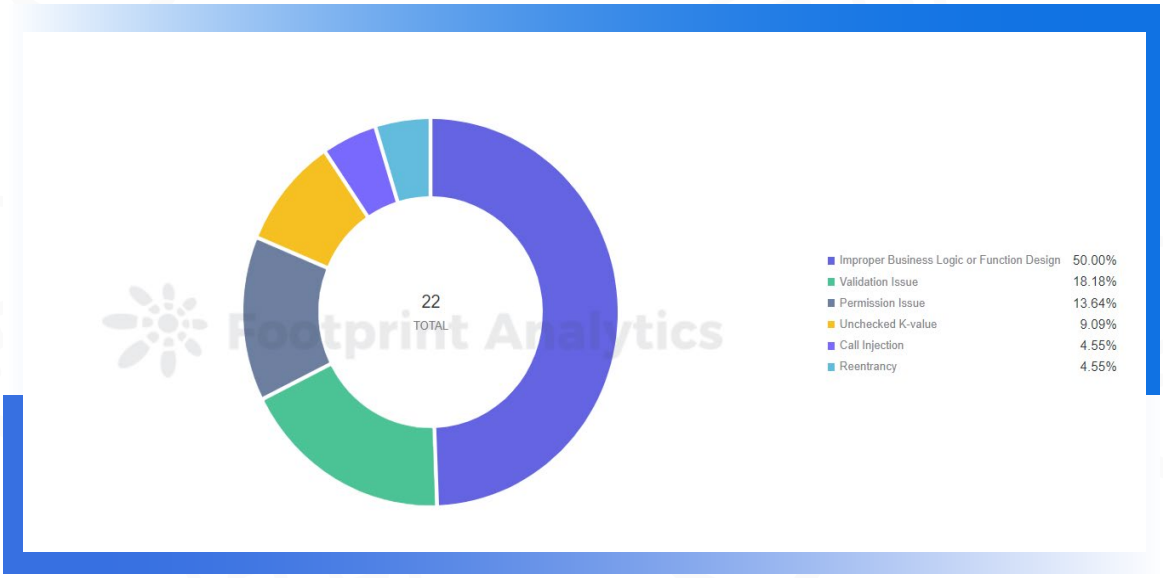
最常见的攻击手法依旧为合约漏洞利用和闪电贷

合约漏洞利用为本季度最常见的攻击手法，22次攻击为合约漏洞利用，频次占到了45.8%，因合约漏洞造成的总损失约为1亿3800万美元。第二常见的攻击方式为闪电贷，本季度共发生9次闪电贷攻击，造成的损失达2亿3300万美元，居各种攻击方式损失金额第一位。

和第一季度相同的是，Web3领域最常见的攻击手法依旧为合约漏洞利用和闪电贷（第一季度的数据分别为50%和24%）。此外，因私钥泄露导致的损失仍然达到了1亿315万美元，私钥安全问题依旧值得重视。

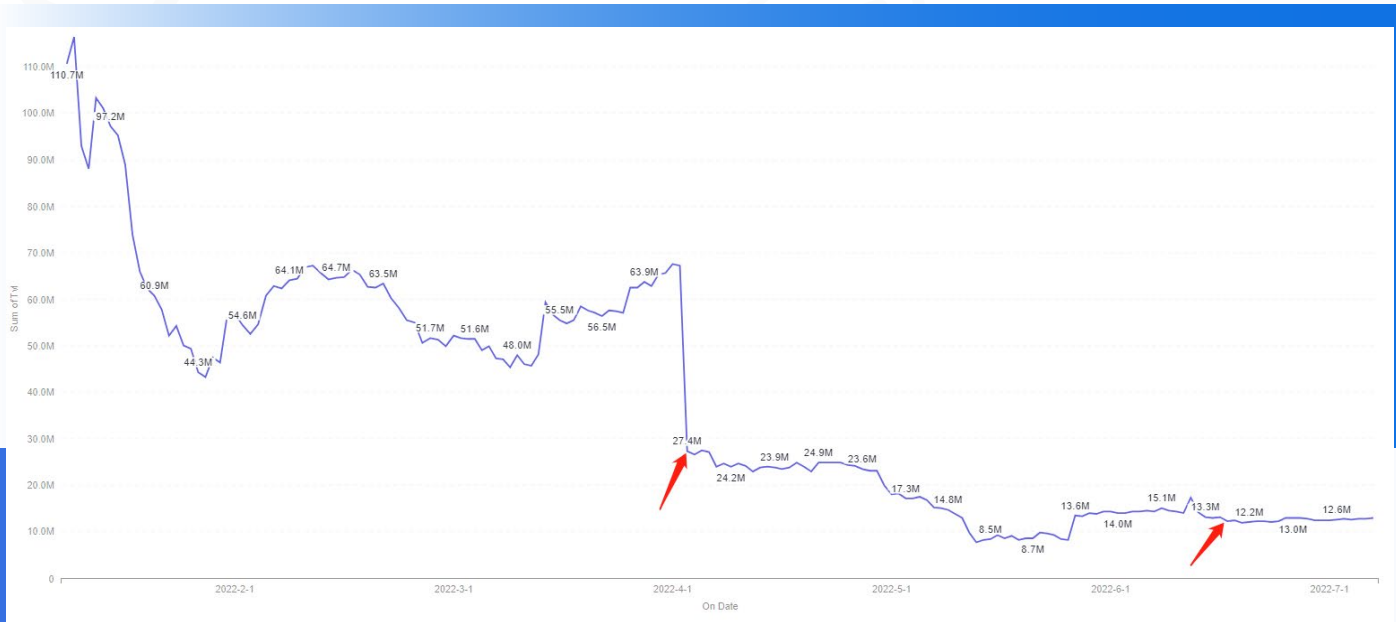


本季度被利用的漏洞主要包括：**业务逻辑/函数设计不当、验证问题、权限问题、k值校验问题、重入漏洞和call注入漏洞。**其中利用次数最多的漏洞为业务逻辑/函数设计不当，远高于其他漏洞。重入漏洞在本季度被黑客利用了1次，造成的损失却达到了8034万美元。



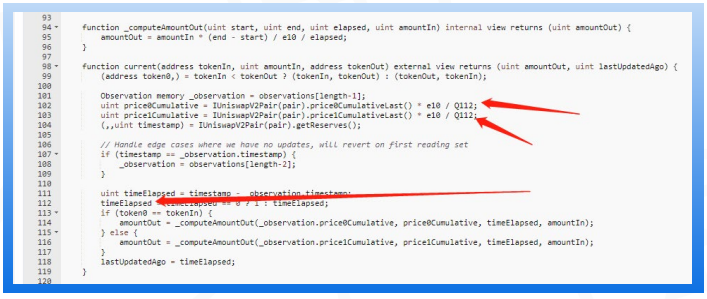
7.典型案例攻击手法分析

7.1 被攻击两次的Inverse Finance

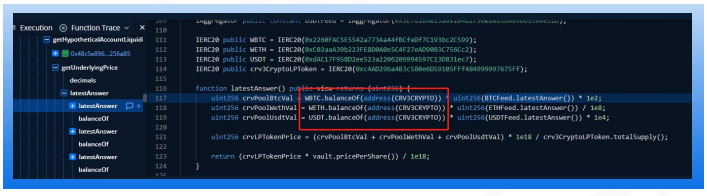


事件详情：

2022年4月2日，Inverse Finance项目遭受价格操纵攻击，累计损失估计大约1500万美元。攻击的主要原因在于TWAP预言机使用的时间窗口太短。在计算Xinv代币价格时，依靠WETH/INV这个pair去计算。由于pair这个池子已经被操纵了，再加上timeElapsed间隔时间短，那么攻击者需要满足不在当前区块调用，就可以操纵xINV代币的价值。



2022年6月16日，Inverse Finance再次遭受黑客攻击，黑客获利120万美元。主要原因在于项目合约在计算抵押品价格时，使用了balanceOf函数，攻击者得以通过大额兑换将抵押品anYvCrv3Crypto的价格拉高。



安全建议：

获取代币价格时应避免依赖于代币实时余额，而应使用TWAP类型的价格预言机，并设置足够的时间窗口。

7.2 Akutars: 由于智能合约漏洞，3400万美元被锁定无法提取

事件详情：

2022年4月24日，NFT项目Akutars因智能合约漏洞导致3400万美元被锁定无法提取。值得注意的是，该项目的合约没有经过安全公司的审计。经分析，发现Akutars的合约包含有两个漏洞。

漏洞一：

第一个合约漏洞在processRefunds中，设计者根据refundProgress计数器进行循环退款。而这里使用了call函数进行退款操作，且把退款的结果作为require的判定条件。因此如果此时有攻击者在队列中进行退款操作，调用call退款给攻击者时，攻击者在fallback中进行进行恶意的revert，则会导致队列后面的所有人都无法进行退款。这个漏洞所幸没被攻击者进行实际利用。

漏洞二：

该漏洞是导致价值约3400万美元资产被锁死在合约中的直接原因。

在claimProjectFunds函数中，该函数主要用于项目方提款。函数中require（refundProgress >= totalBids），此处refundProgress表示已经处理了多少个用户的退款，totalBids表示所有用户总投标了多少个NFT。由于一个用户可以投标多个NFT，导致单从数值上比较，refundProgress可能小于totalBids。

```
618     function claimProjectFunds() external onlyOwner {
619         require(block.timestamp > expiresAt, "Auction still in progress");
620         require(refundProgress >= totalBids, "Refunds not yet processed");
621         require(akuNFTs.airdropProgress() >= totalBids, "Airdrop not complete");
622
623         (bool sent, ) = project.call{value: address(this).balance}("");
624         require(sent, "Failed to withdraw");
625     }
```

而退款函数processRefunds中：require(_refundProgress < _bidIndex); bidIndex表示所有参与竞标的用户，refundProgress永远不会高于bidIndex。而bidIndex的值为3669，totalBids的值为5495。

因此，refundProgress>=5495且refundProgress<3669这个判断条件永远不会成立，项目方团队将永远无法执行后续的提款操作。此处应将refundProgress与bidIndex做对比，开发者犯了一个很低级的错误。这最终导致了项目方3400万美元的资产被锁定无法提取。

安全建议：

项目上线前的专业安全审计非常有必要。

7.3 Beanstalk Farms：黑客获利近8000万美元，恶意提案如何防范？

2022年4月17日，算法稳定币项目Beanstalk Farms遭到闪电贷攻击，黑客获利近8000万美元，协议损失达1亿8200万美元。这是本季度损失金额最高的项目。

回顾本次攻击，攻击者在前一天发起提取Beanstalk: Beanstalk Protocol资金的提案，然后调用emergencyCommit进行紧急提交来执行提案。这是要因为项目方规定提案后1天才能开始投票。

攻击过程中，攻击者利用“投票合约中的票数由账户的提案代币持有量计算得到”的漏洞，通过闪电贷借出价值10亿美元的巨额资金，换取代币后投入到矿池中，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。最终提案通过并执行，攻击者成功提取项目方资金，随后兑换并偿还闪电贷，获利离场。

```
balanceOfRoots in GovernanceFacet:34
29          emit Vote(account, bipId, balanceOfRoots(account));
30      }
31
32      function recordVote(address account, uint32 bipId) internal {
33          s.g.voted[bipId][account] = true;
34          s.g.bips[bipId].roots = s.g.bips[bipId].roots.add(balanceOfRoots(account));
35      }
36
```

```
180     function emergencyCommit(uint32 bip) external {
181         require(isNominated(bip), "Governance: Not nominated.");
182         require(
183             block.timestamp >= timestamp(bip).add(C.getGovernanceEmergencyPeriod()),
184             "Governance: Too early.");
185         require(isActive(bip), "Governance: Ended.");
186         require(
187             bipVotePercent(bip).greaterThanOrEqualTo(C.getGovernanceEmergencyThreshold()),
188             "Governance: Must have super majority."
189         );
190         _execute(msg.sender, bip, false, true);
191     }
```

安全建议：

1.投票所用资金应在合约中锁定一定时间，避免使用账户的当前资金余额来统计投票数量；

2.项目方和社区应关注所有提案，如果提案是恶意提案，建议在提案投票期间应及时做出处理措施，将提案废弃，禁止其接受投票以及执行；

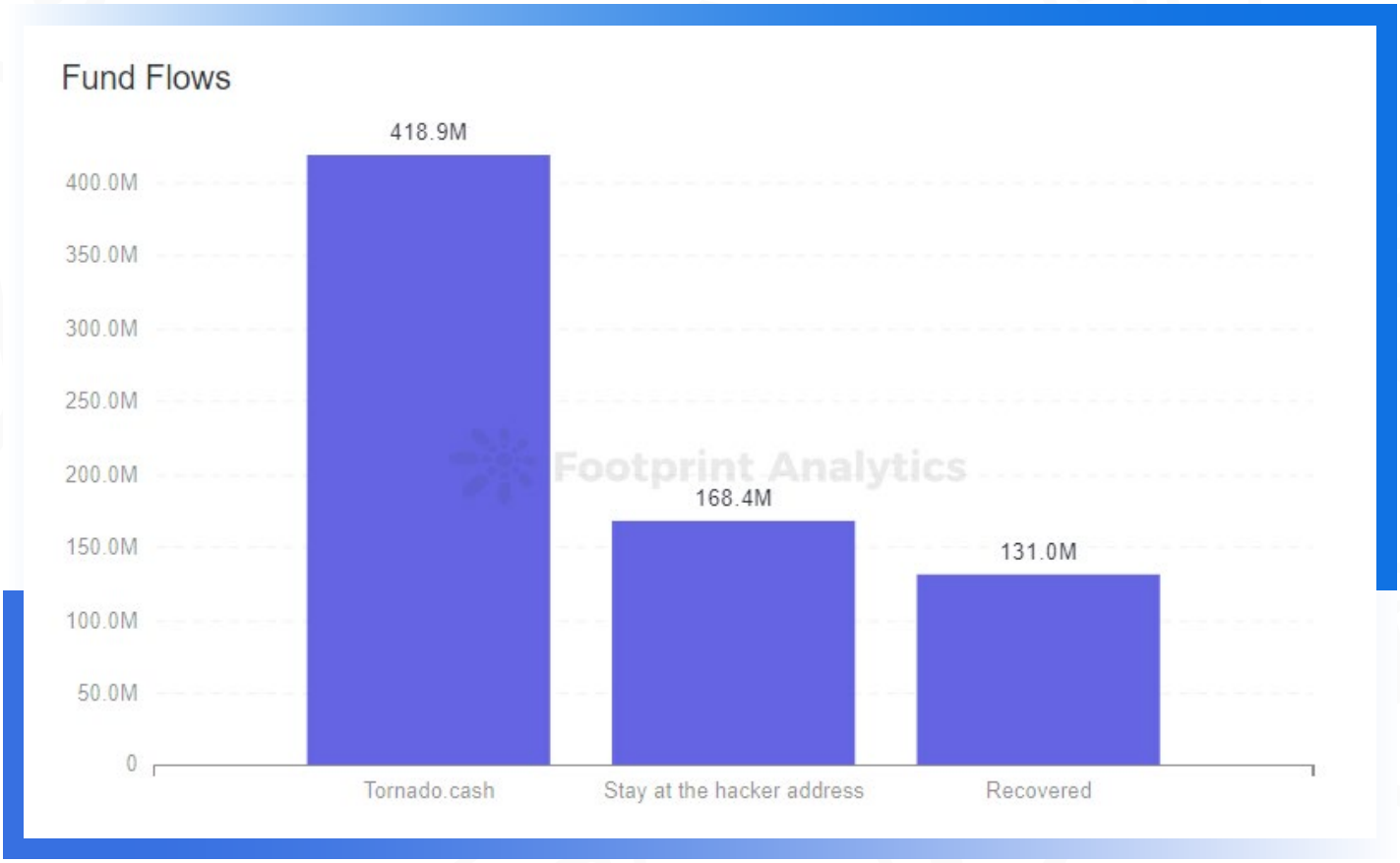
3. 可考虑禁止合约地址参与投票。

8. 资金流向分析

约4亿1889万美元的被盗资金流入Tornado.cash

从资金流向来看，在2022年第二季度，约4亿1889万美元的被盗资金被黑客转入了Tornado.cash，占该季度总被盗金额的58.3%。另外有1亿3100万美元的资产被追回，1亿6845万美元的资产留在黑客地址暂未进行混币或流入交易所。

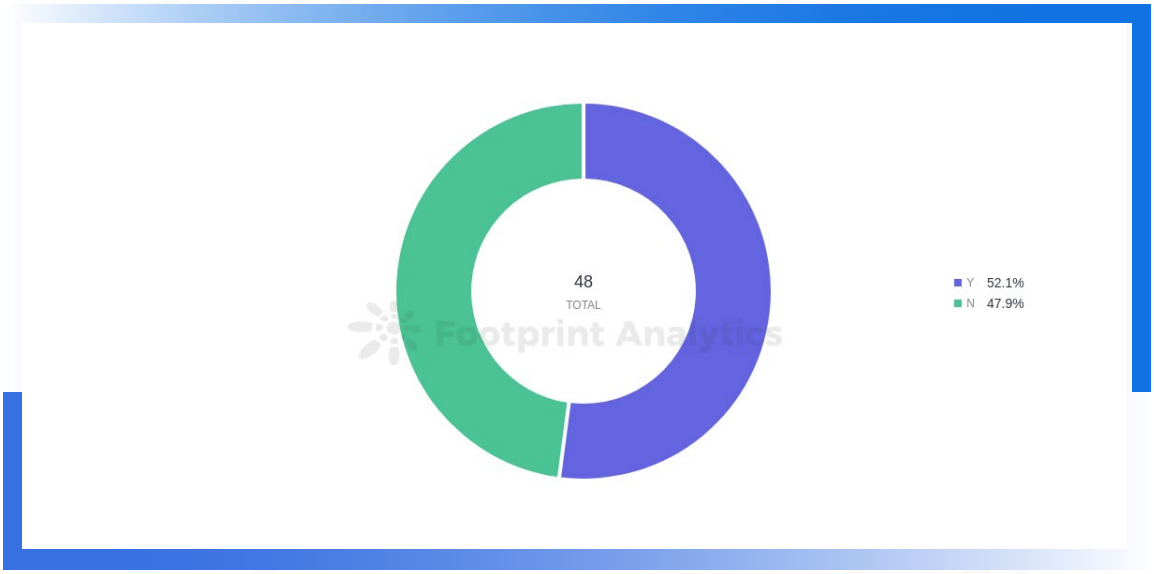
数据表明，龙卷风依旧为黑客进行洗钱的惯用途径。本季度资金追回的情况优于上一季度，在一些情况下，项目方会和黑客通过链上信息进行协商，部分黑客会选择返还一定数量的赃款以“免于法律制裁”。



9. 项目审计情况分析

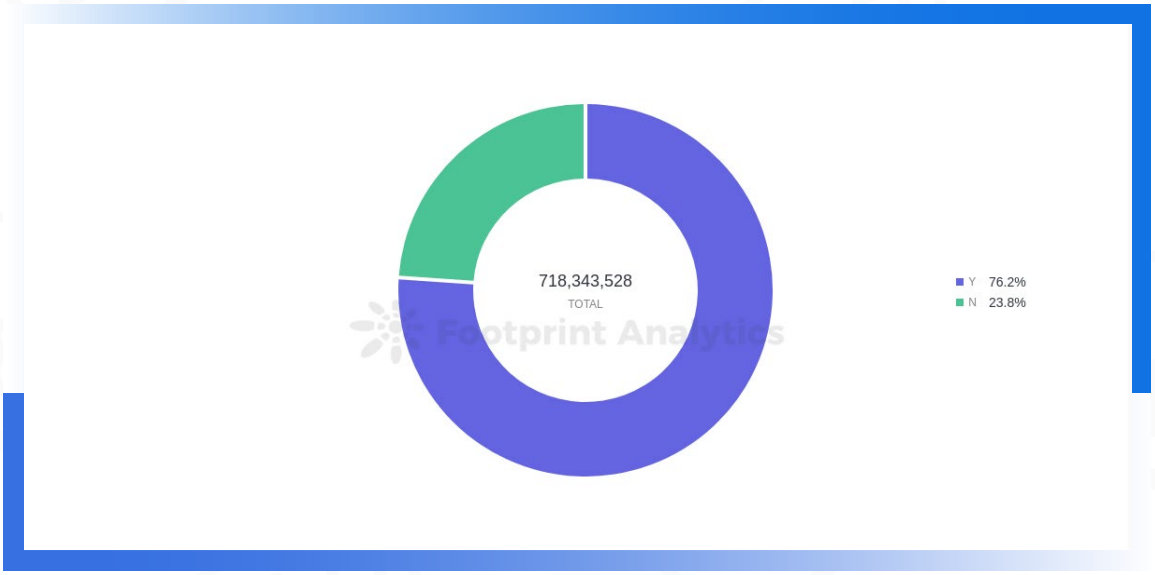
仅有52%的项目经过了审计

被攻击的项目中，仅有52%的项目经过了审计，而上个季度，该项比例为70%。本季度经过审计的项目因攻击造成的损失达5亿4763万美元，占损失金额的76.2%，远高于上一季度。



虽然经过审计的项目损失金额仍达到了5亿4763万美元，但这并不意味着审计不再重要了。

随着越来越多的安全公司踏足审计业务，审计市场参差不齐，鱼龙混杂。由于一些不专业的公司，导致智能合约中一些本应该审计出的漏洞没有审计出来，因此一些项目方和投资者开始质疑审计的必要性和专业性，认为“审计了也是白审”。例如，本季度合约漏洞中最常出现的“业务逻辑/函数设计不当”，这类漏洞是完全可以在审计阶段发现的。**因此建议项目方一定在项目上线前要寻找专业的安全公司进行审计。**

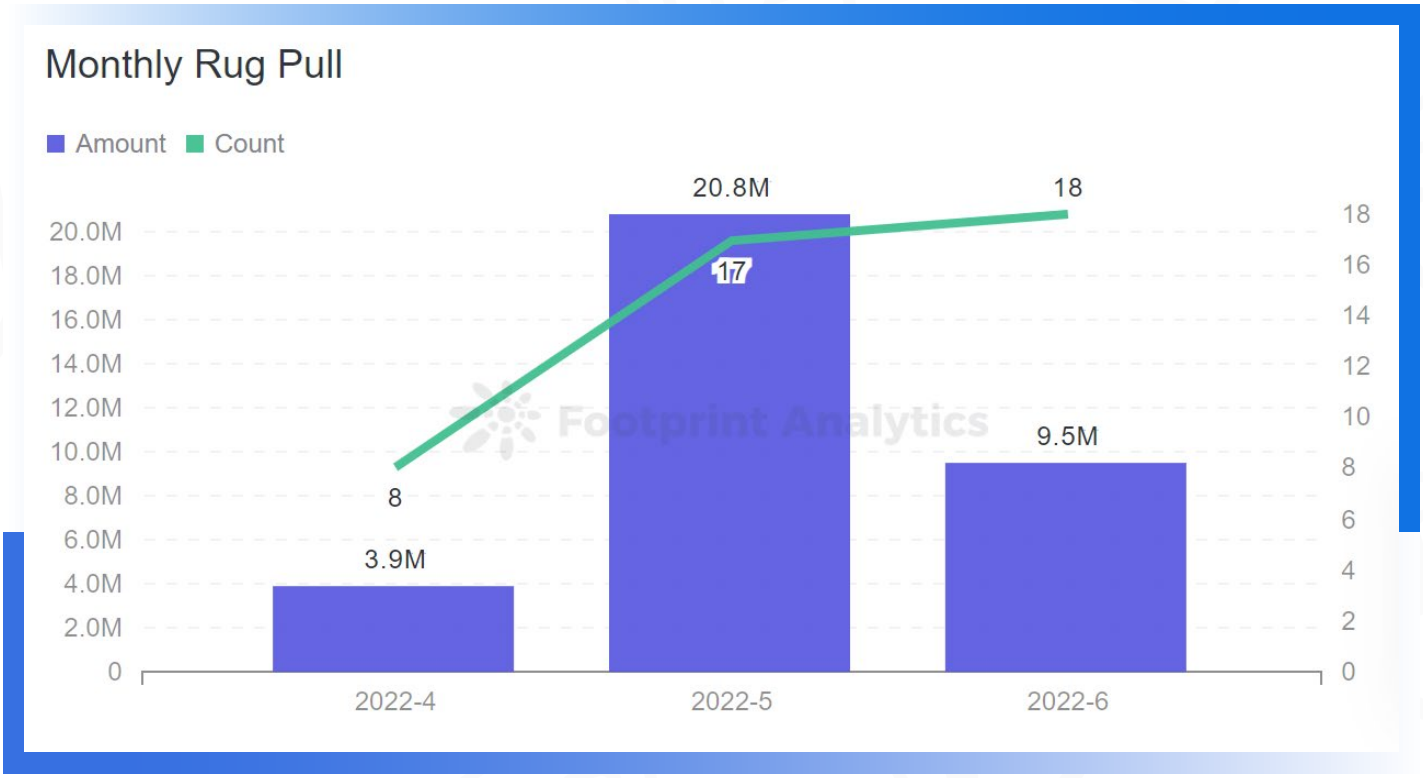


10. Rug pull分析

项目方共计卷走约3426万6402美元

Rug pull通常指的是开发人员撤出 DEX 流动性池或突然放弃一个项目，毫无征兆地就卷走投资者的资金，通俗来讲就是“跑路”。2022年第二季度，共监测到链上主要Rug pull事件43起，项目方共计卷走约3426万6402美元。

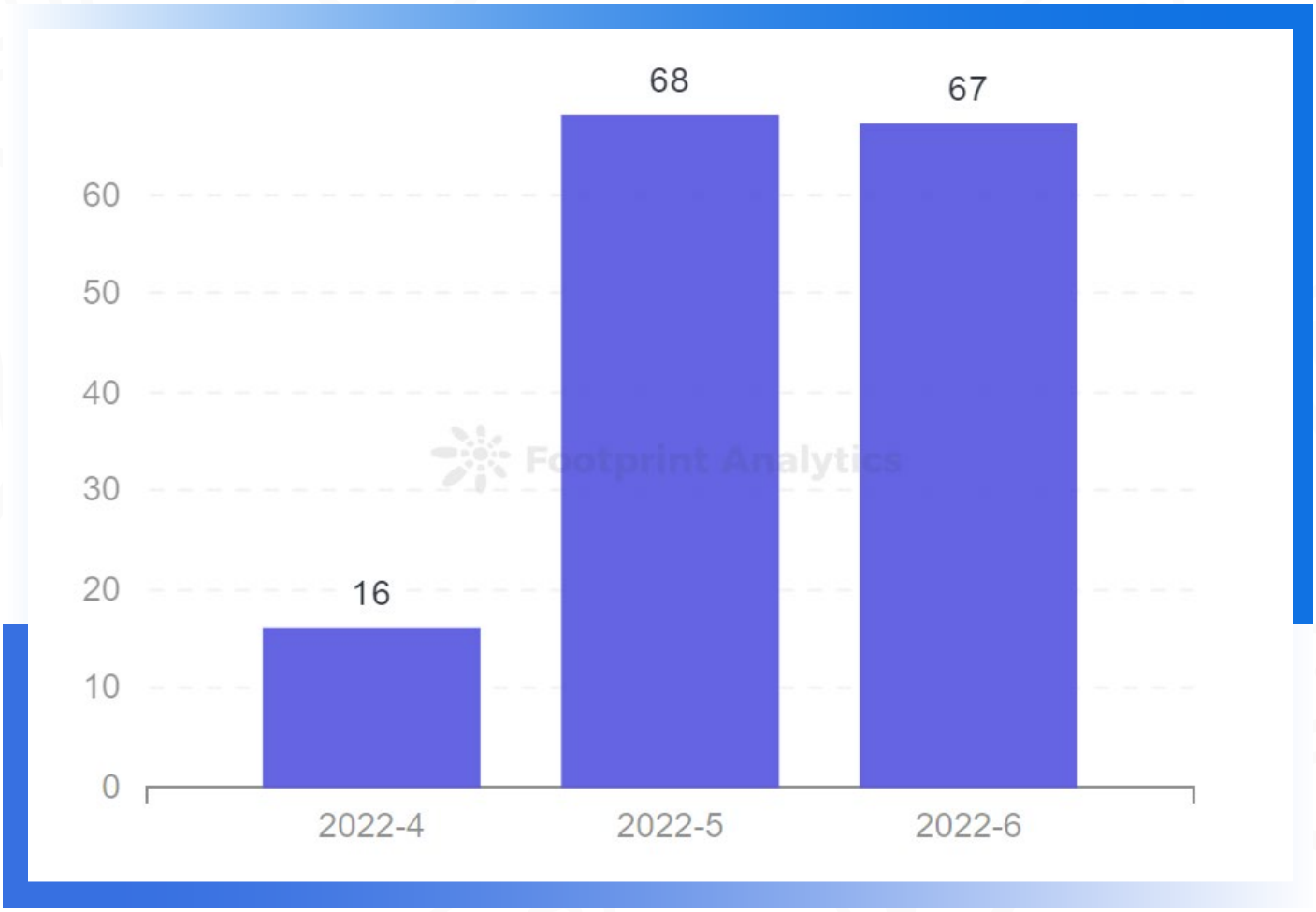
攻击事件数据表明，5月黑客活跃度大幅降低，然而与之不同的是，5月却是Rug pull最高频的月份。在5月各公链和项目TVL大幅缩水的情况下，一些项目方选择了Rug pull，导致一大批投资者受损。其原因或许是无法继续运营，或许是认为“与其等着TVL归零，不如自己先跑路”，或许是本就预谋好跑路，只是TVL急剧的下降加速了这一过程。



11. Discord钓鱼分析

本季度Discord钓鱼案例频发

据不完全统计，2022年第二季度，Web3领域共有包括Opensea、BAYC、Moonbirds、RTFKT、Akutars、Doodles、Otherside在内的超151个Discord服务器被黑，其中5月、6月尤为严重。其中个别服务器在本季度内被攻击了两次甚至三次。



和Rug pull数据类似的是，在市场行情低迷的情况下，钓鱼类安全事件或许反而会增多。本季度出现的Discord钓鱼方式形式繁多，**例如机器人账号被黑、伪装管理员或机器人私信发送钓鱼链接、通过社交媒体散播高仿Discord邀请链接等等。越是熊市，用户和项目方反而越是应该提高反诈意识，保护好自己的资产安全。**

12. 总结页

2022年第二季度，DeFi安全仍然是值得关注的焦点，约79.2%的攻击发生在DeFi领域。连续两个季度，DeFi一直都是黑客攻击的重点对象。而NFT、跨链桥、交易所安全事件虽然频次没有DeFi那么高，但个别事件涉及金额也很巨大。因此，Web 3各类型项目方都应加强安全意识，做好安全防护工作。

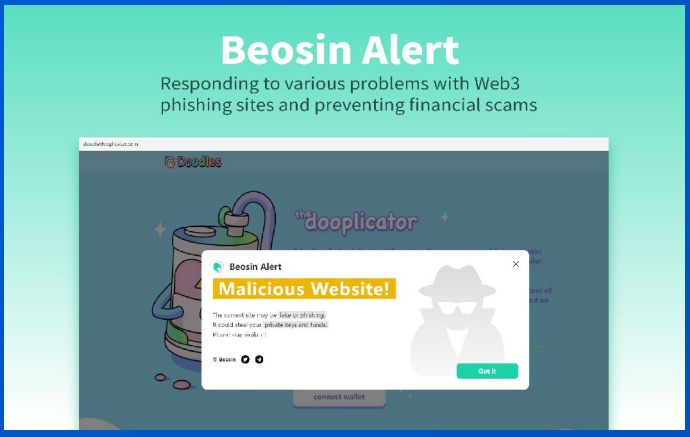
本季度约有45.8%的攻击为合约漏洞利用，其中绝大部分漏洞都可以在审计阶段发现和进行修复。而在本季度被攻击的项目中，仅有52%的项目经过了审计。建议项目在上线之前寻找专业的审计公司进行审计。

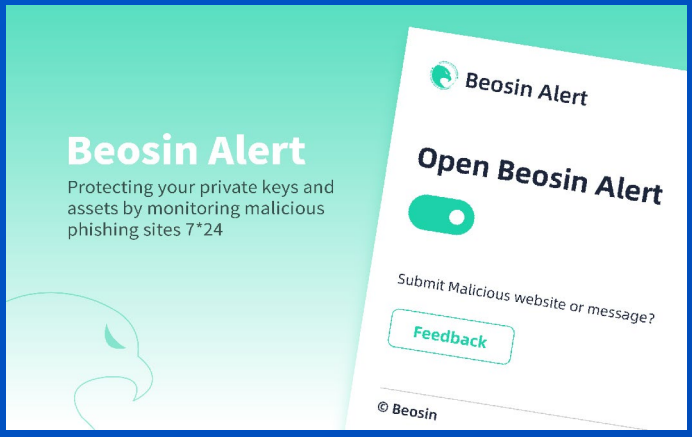
本季度，约4亿1889万美元的被盗资金被黑客转入了Tornado.cash进行洗币。另外约有1亿3100万美元的资产被追回，但追回方式大多是通过链上和黑客进行协商，让黑客返还部分被盗资金。其实被盗资金进入龙卷风后不是毫无办法。成都链安在协助被盗资金追踪方面已积累了不少成功案例，包括一些资金进入龙卷风的情况。建议项目方在不幸遇到被黑时，除了和黑客协商返还，也可寻求一些专业的安全公司进行资金追踪。

本季度各公链和项目的TVL值都出现了较大波动，也有因为各类安全事件导致项目资金异常或出现风险交易的情况。建议项目方和投资者都因及时关注项目运行情况。成都链安【链必应-区块链安全态势感知平台】可以让项目方和用户及时发现风险交易，从而快速采取措施。

在本季度行情低迷的情况下，Rug pull和钓鱼等各类安全事件反而更加频发，一些Web 2的攻击方式在Web 3领域依旧活跃。各项目方和用户都应该提升安全意识，保管好自己的私钥，不要轻易点击来路不明的链接，对各类信息进行多渠道验证。

安装下面这款钓鱼插件，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

*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-Q2-Report

成都链安

让区块链生态更安全

SECURING YOUR BLOCKCHAIN ECOSYSTEM

成都链安是一家致力于区块链安全生态建设的全球领先区块链安全公司，也是最早将形式化验证技术应用到区块链安全的公司，总部位于四川成都。公司由电子科技大学教授联合创立，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。

目前已与公安、工信部、中国通信院、网信办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。

公司已获前海母基金、联想创投、复星高科、成创投、任子行等知名机构的多轮投资。是工信部“网络安全技术应用试点示范项目”单位、CNVD国家区块链安全漏洞平台技术支持单位、中国信通院区块链安全检测的主要技术合作单位、中央网信办“国家区块链创新应用试点”参与单位、国家互联网应急中心“区块链安全技术检测中心”的主要技术合作单位、四川省区块链安全工程技术研究中心依托单位、四川省区块链基础设施—蜀信链安全检测和准入测试支撑单位。是多个区块链相关行业协会成员，并参与了多项国家级区块链安全技术标准和白皮书的撰写，承担了多项国家级、省部级项目，依托技术优势现已申请软件发明专利和软件著作权30多项。

成都链安将以“让区块链生态更安全”为使命，以“成为全球第一的区块链安全公司”为愿景，不断打造区块链安全监管技术和安全保障体系，为区块链生态的安全发展保驾护航。

安全产品	安全服务
链必追-虚拟货币案件智能研判平台	智能合约安全审计服务
链必验-智能合约形式化验证平台	链平台安全检测服务
链必检-区块链检测平台	虚拟资产追踪溯源和调查取证服务
链必应-区块链安全态势感知平台	安全舆情服务
链必知-区块链安全舆情平台	安全咨询服务
链必研-智能合约安全开发IDE	安全应急响应服务

声明

028-83262585
market@lianantech.com
www.lianantech.com

成都链安官方公众号

安全审计业务咨询

安全事件合集订阅