■ H1 2023 글로벌 Web3 보안 보고서,

AML 분석 및 암호화폐 규제 풍경

서문

글로벌 디지털화 과정의 지속적인 가속화로 인해, 블록체인은 신흥 탈중앙화 거래 방식으로서 점차 디지털 경제의 핵심 인프라 중 하나로 자리 잡고 있습니다. 그러나 블록체인 응용 시나리오의 계속적인 확대로 사용자가 직면하는 보안 위험도 점차 증가하고 있습니다. 따라서 Web3 의 보안 상황과 암호화폐 산업의 규제 정책을 이해하는 것은 블록체인의 안전과 안정성을 보장하기 위한 필수적인 방법 중 하나가 되었습니다. 이 연구 보고서는 2023 년 상반기 글로벌 블록체인 보안 상황, Web3 의 핫스팟 및 암호화폐 산업의 주요 규제 정책에 초점을 맞추어 깊이 있는 분석과 요약을 수행하며, 블록체인 보안의 건강한 성장을 돕기 위해 독자들에게 가치 있는 참고 자료와 영감을 제공하는 것을 목표로 합니다.

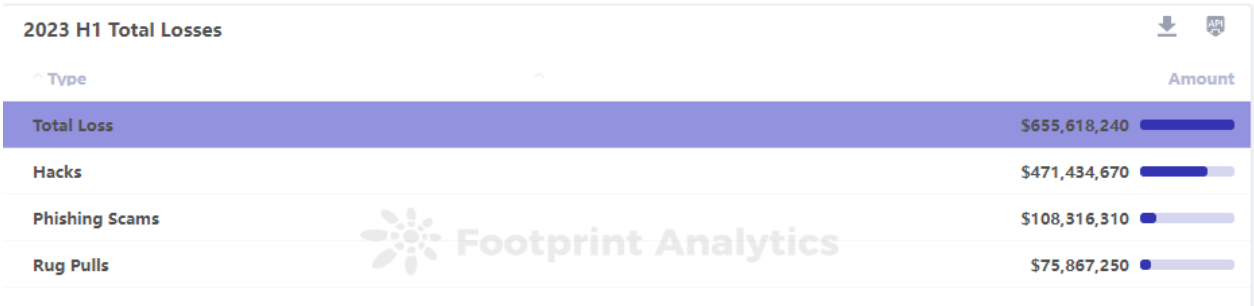
I. H1 2023 글로벌 Web3 보안 통계 및 AML 분석

본 장은 Beosin 연구팀의 Mario 와 Donny 가 작성하였습니다.

데이터 소스 (2023 년 6 월 25 일 기준): Footprint Analytics: Crypto Analysis 대시보드

1 H1 2023 Web3 보안 개요

Beosin EagleEye 플랫폼 통계에 따르면, 2023 년 상반기 Web3 에서의 해킹, 피싱 사기 및 러그 풀로 인한 총 손실은 6 억 5,561 만 달러에 이릅니다. 그 중 108 건의 공격으로 약 4 억 7,143 만 달러의 총 손실이 발생하였으며, 피싱 사기로 인한 총 손실은 약 1 억 8 백만 달러이며, 110 건의 러그 풀로 인한 총 손실은 약 7,587 만 달러입니다.



웹 3 에서의 해킹으로 인한 총 손실은 작년에 비해 크게 감소했습니다. 2022 년 상반기에는 공격으로 인한 총 손실이 약 19 억 1 천만 달러, 하반기에는 약 16 억 9 천만 달러였으나, 2023 년 상반기에는 이 값이 4 억 7 천 1 백만 달러로 줄었습니다.

프로젝트 유형별로 보면, DeFi 가 가장 빈번한 대상이자 손실이 가장 많이 발생한 유형입니다. 85 건의 DeFi 보안 사건으로 인한 총 손실은 2 억 9 천 2 백만 달러에 이르며, 전체 손실의 62%를 차지합니다.

블록체인 플랫폼 유형별로 보면, 손실 금액의 75.6%가 Ethereum 에서 발생하여 약 3 억 5 천 6 백만 달러로, 모든 블록체인 플랫폼 중에서 첫 번째로 높은 손실을 기록하였습니다.

공격 유형별로 분류하면, 가장 빈번하고 재정적 피해가 큰 공격 유형은 계약 취약점을 이용한 공격입니다. 계약 취약점으로 인한 60 건의 사건은 총 2 억 6 천 4 백만 달러의 손실을 발생시켰으며, 전체 손실의 56%를 차지합니다.

자금 흐름 관점에서, 약 2 억 1 천 5 백만 달러의 도난 자산이 회수되어 모든 도난 자산의 45.5%를 차지했습니다. 또한, 약 1 억 1 천 3 백만 달러가 Tornado Cash 와 기타 믹서로 이체되었습니다.

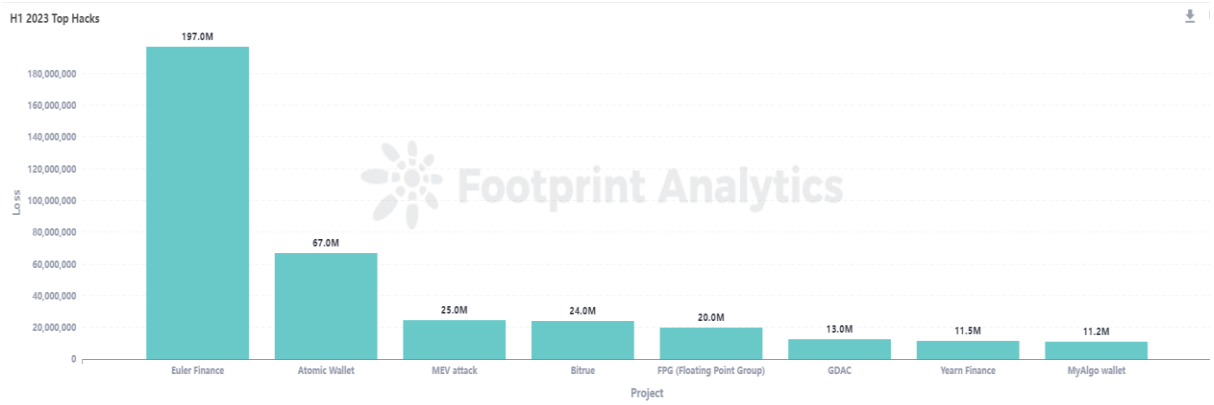
감사 상태 관점에서, 공격을 받은 프로젝트 중 약 49%는 감사를 받지 않은 상태였습니다.

2022 년과 비교하여 해커들의 감소 추세에 반대로, 2023 년 상반기에는 피싱 사기와 러그 풀 이벤트가 더욱 빈번히 발생했습니다. 불완전한 통계에 따르면, 이 두 가지 유형의 이벤트에서 관련된 총 금액은 최소 1 억 8 천 4 백만 달러에 이르렀습니다. 일부 지갑 유출자들이 악성 툴킷을 판매하고, 구매자들이 이익을 얻은 후에는 이익을 함께 공유할 수 있는 등 피싱 사기에 대한 진입 장벽이 낮아진 것은 2023 년 상반기에 피싱 사기가 크게 증가하는 주요 요인이 되었으며, 이는 Web3 사용자의 보안에 대한 중대한 위협이 되고 있습니다.

2. 해킹 개요

471 억 4300 만 달러의 손실을 초래한 108 건의 공격

2023 년 상반기 동안 Beosin EagleEye 는 Web3 공간에서 총 108 건의 주요 공격을 모니터링했으며, 총 손실은 약 4 억 7,143 만 달러에 이릅니다. 1 억 달러 이상의 손실이 발생한 보안 사건은 1 건이었으며, 1,000 만 달러에서 1 억 달러 사이의 손실이 있는 사건은 7 건, 100 만 달러에서 1,000 만 달러 사이의 손실이 있는 사건은 23 건이었습니다.



"손실이 1,000 만 달러를 초과한 공격 (내림차순):

● Euler Finance – 1 억 9,700 만 달러

2023 년 3 월 13 일, DeFi 프로토콜 Euler Finance 가 1 억 9,700 만 달러를 훔치는 공격을 받았습니다. 4 월 4 일, Euler Labs 는 트위터에서 공격자가 협상에 성공한 후 도난당한 자금을 모두 반환했다고 발표했습니다.

● Atomic Wallet – 6700 만 달러

2023 년 6 월 3 일, 여러 Atomic Wallet 사용자들이 소셜 미디어에 자신들의 지갑 자금이 도난당했다고 보고했으며, 추정 손실액은 적어도 6700 만 달러입니다. 훔친 자금은 해커들에 의해 Sinbad 믹서를 통해 세탁되었으며, 공격 원인은 아직 조사 중입니다.

● MEV 공격 – 2500 만 달러

2023 년 4 월 3 일, 악의적인 샌드위치 공격으로 여러 MEV 로봇들이 피해를 입어 약 2500 만 달러의 총 손실을 보았습니다.

● Bitrue – 2400 만 달러

2023 년 4 월 14 일, 암호화폐 거래소 Bitrue 의 핫 월렛이 해킹되어 2400 만 달러의 손실이 발생했습니다.

● FPG - 2,000 만 달러

2023 년 6 월 11 일, 암호화폐 중개업체 Floating Point Group (FPG)가 공격을 받아 약 2,000 만 달러의 손실을 입었습니다.

● GDAC - 1,300 만 달러

4 월 9 일, 한국의 암호화폐 거래소 GDAC 이 해킹 공격을 받아 약 1,300 만 달러의 손실을 입었습니다.

● Yearn Finance - 1,150 만 달러

4 월 13 일, Yearn Finance 의 YUSDT 계약이 해킹되어 공격자는 1,000 만 달러 이상의 이익을 얻었습니다.

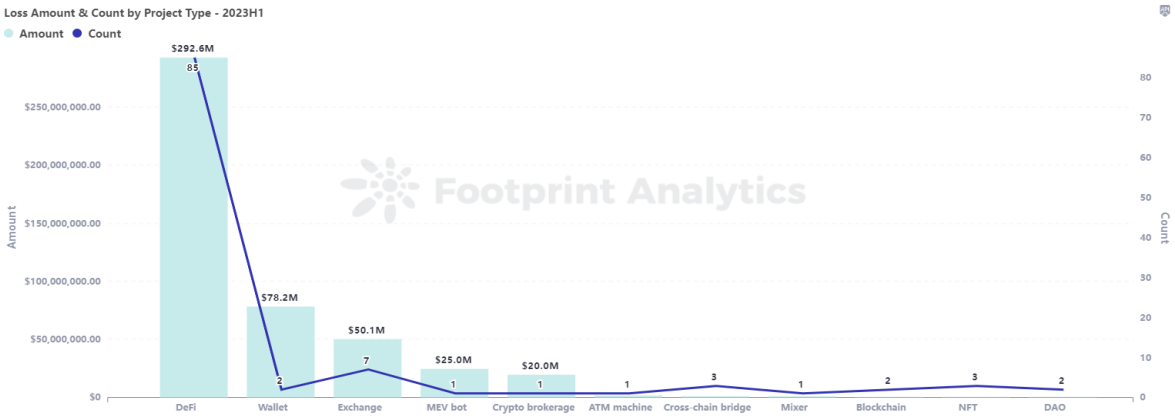
● MyAlgo Wallet - 1,120 만 달러

2 월에 MyAlgo Wallet 이 중간자 공격을 당해 1,120 만 달러의 손실을 입었습니다."

3. 공격된 프로젝트들의 유형

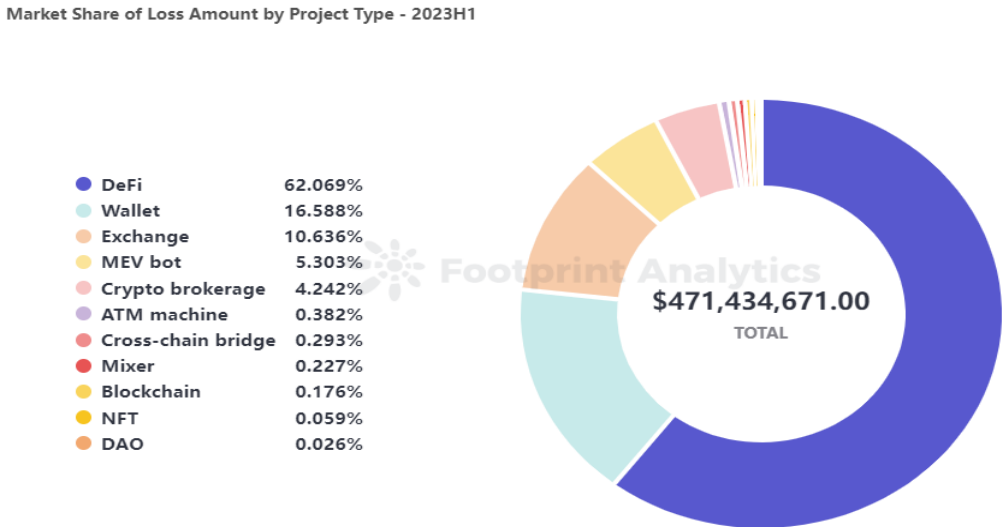
85 건의 DeFi 보안 사건으로 2 억 9,200 만 달러 손실했습니다.

2023 년 상반기 동안 DeFi 부문에서 총 85 건의 보안 사건이 발생하여 전체 공격 횟수의 78.7%를 차지했습니다. DeFi 에서의 총 손실은 2 억 9,200 만 달러에 이르며, 전체 손실의 62%를 차지하고 있습니다. DeFi 프로젝트는 다른 프로젝트 유형에 비해 가장 높은 공격 빈도와 손실 금액을 겪었습니다.



85 건의 DeFi 보안 사고 중 51 건은 계약 취약점에서 발생했으며, 이로 인해 2 억 4,900 만 달러의 손실이 발생하여 전체 DeFi 손실의 85%를 차지했습니다.

지갑 공격으로 인해 약 7,820 만 달러의 손실이 발생하여 모든 프로젝트 유형 중 두 번째로 높은 수준이었습니다. 단독으로 원자 지갑 공격으로 인해 최소 6,700 만 달러의 손실이 발생했으며, MyAlgo 지갑 공격으로 인해 1,120 만 달러의 손실이 발생했습니다.

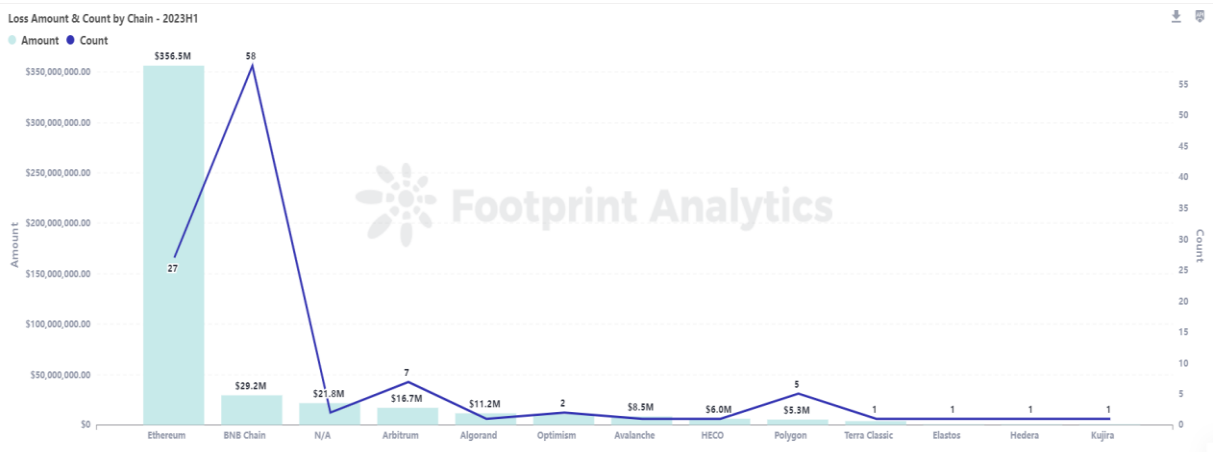


"손실 관점에서 세 번째로 많이 발생한 프로젝트 유형은 거래소로, 약 5,014 만 달러의 손실이 있었습니다. 거래소 공격은 2022 년 전체 기간 동안 손실 순위에서 자주 발생하는 공격의 추세를 유지하였습니다.

2022 년에는 교차 체인 브릿지 프로젝트가 가장 큰 손실을 기록했으며(18.9 억 달러), 하지만 2023 년 상반기에는 손실이 크게 감소하여 138 만 달러로 줄었습니다.

4. 체인별 손실

손실 금액의 75.6%는 Ethereum 에서 발생했습니다."

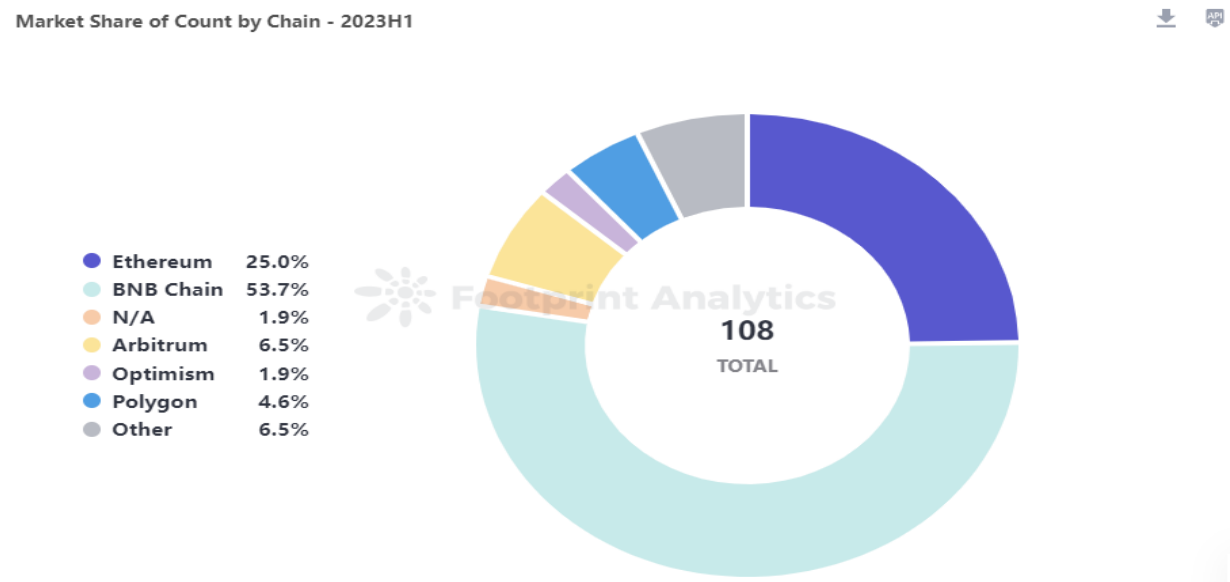


2023 년 상반기에는 Ethereum 에 대한 총 27 건의 주요 공격이 발생하여 약 3 억 5,600 만 달러의 손실이 발생했습니다. 손실액의 75.6%는 Ethereum 에서 발생하여 모든 블록체인 중에서 가장 많은 양을 차지하고 있습니다.

BNB 체인은 가장 많은 공격 사례를 경험했으며, 58 건의 공격으로 모든 보안 사건의 53.7%를 차지하고 있습니다. BNB 체인에 대한 58 건의 공격 중 40 개의 대상 프로젝트는 어떠한 형태의 감사도 거치지 않았습니다.

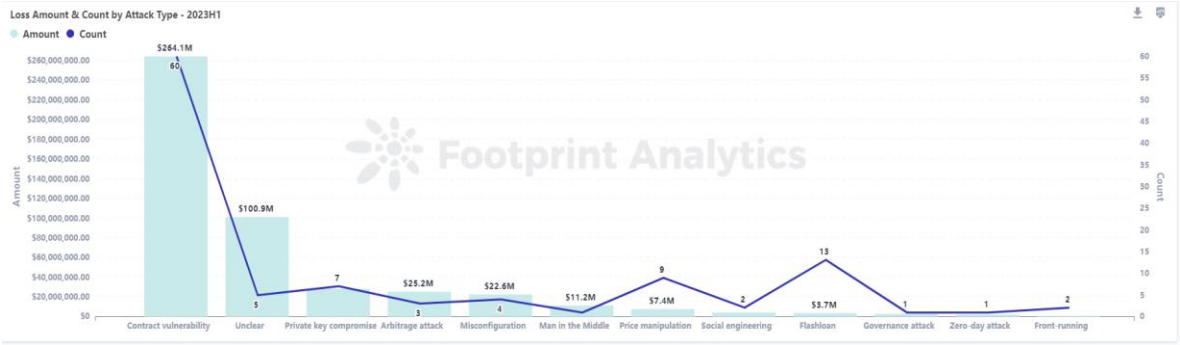
약 7 건의 공격으로 인해 Arbitrum 은 약 167 만 1 천 달러의 손실을 입었습니다. 손실액과 사건 수는 2022 년과 비교하여 증가하였으며, 전체 연도 동안 Arbitrum 은 2 건의 주요 보안 사건만을 경험한 바 있습니다.

2022 년에는 솔라나가 모든 공개 블록체인 중 손실액 기준으로 3 위를 차지했습니다. 그러나 2023 년 상반기에는 솔라나에서 주요한 공격 사례는 감지되지 않았습니다.



5. 공격 유형에 따른 손실

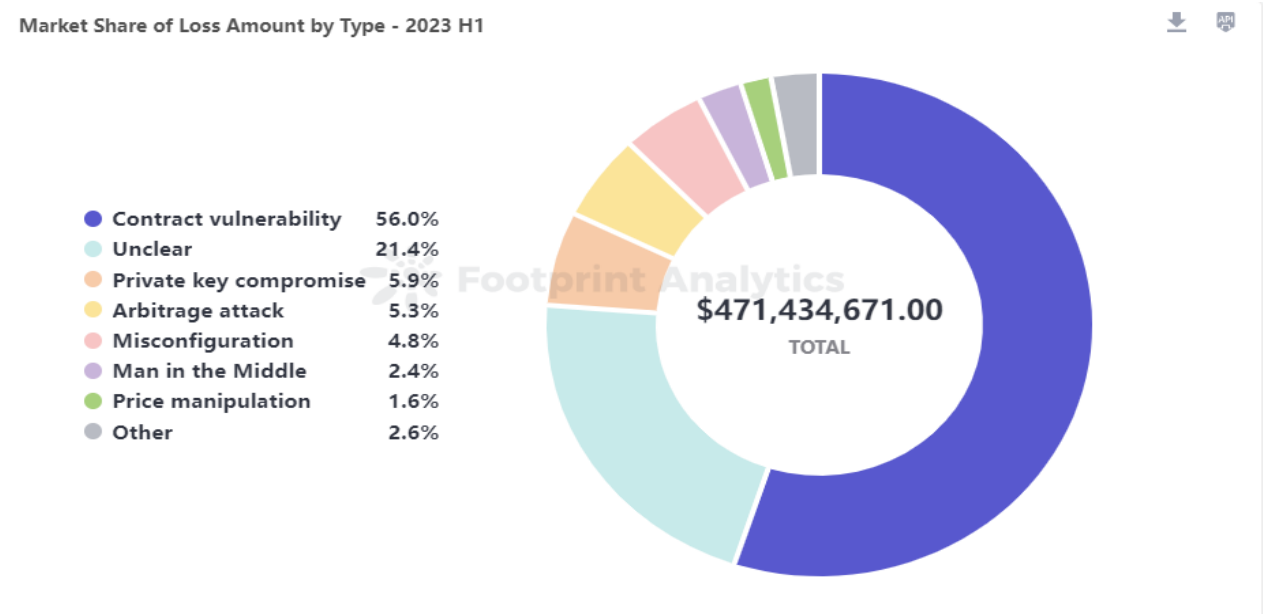
계약 취약점 공격은 가장 빈도가 높았으며 손실액이 가장 많았습니다.

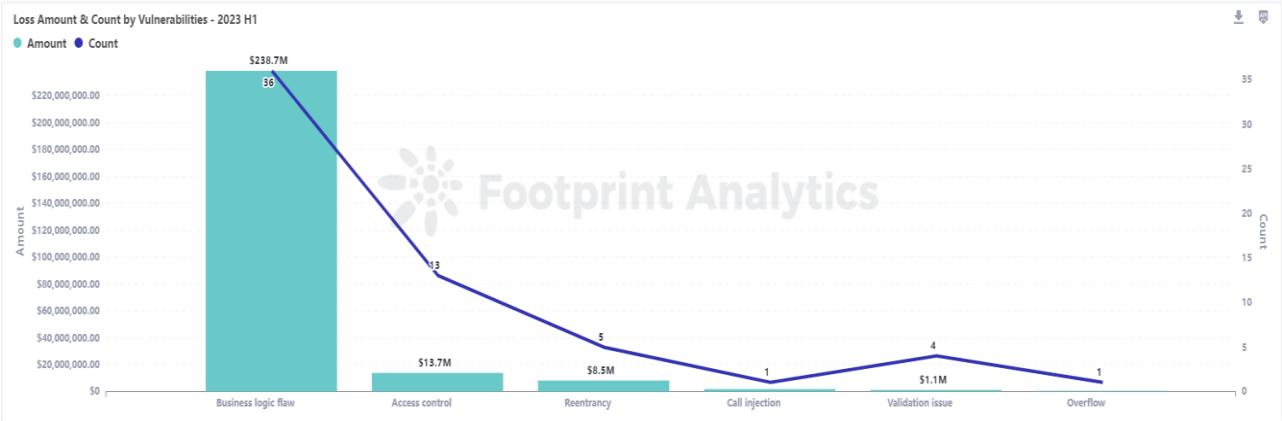


2023 년 상반기에 가장 빈번한 공격 유형과 가장 큰 손실액은 계약 취약점 공격이었습니다. 총 60 건의 계약 취약점 공격으로 인해 총 2 억 6,400 만 달러의 손실이 발생했으며, 이는 총 손실의 56%에 해당합니다.

공격 유형 관련하여 "미확인"으로 분류된 보안 사건은 약 1 억 달러에 해당합니다. 이에는 Atomic Wallet 에서 6,700 만 달러를 탈취한 사건과 암호화폐 중개업체 FPG 에 대한 2,000 만 달러의 공격 등이 포함됩니다. 이러한 사건은 상당한 금액의 자금을 포함하며 다수의 사용자에게 영향을 미칩니다. 이러한 사건의 원인을 조사하면서 프로젝트는 적극적으로 제 3 자 보안 회사와 협력하고 조사 결과를 신속히 공개하며 필요한 개선 조치를 취하고 사용자 자산의 보안에 대한 책임을 갖는 것이 권장됩니다.

또한, 개인 키 침해 사례가 7 건 있었으며 약 2,767 만 달러의 손실이 발생했습니다. 2022 년에도 개인 키 침해가 모든 공격 유형 중 세 번째로 많이 발생한 사례입니다. 개인 키 침해는 여전히 프로젝트 보안에 위협을 가하고 있습니다. 핵심 팀 구성원의 전문 윤리와 보안 인식 관리를 강화하는 것은 일부 사례들을 통해 명백히 확인되었듯이 특히 중요합니다.





"취약점 유형에 따라 손실의 주요 원인은 비즈니스 로직 결함, 접근 제어 및 재진입이었습니다. 총 36 건의 비즈니스 로직 취약점으로 인해 약 2 억 3,900 만 달러의 손실이 발생하여 계약 취약점으로 인한 모든 손실의 90%를 차지했습니다. 이러한 유형의 취약점은 종종 개발자들에게 무시되며, 악용되면 상당한 손실을 초래할 수 있습니다. 실제로 9 건의 사건에서 손실이 각각 100 만 달러를 초과했습니다. 프로젝트 팀은 경험 있는 전문 감사 기관을 찾아 감사를 수행하는 것이 권장됩니다.

6. 2023 년 상반기 보안 사건

6.1 Euler Finance

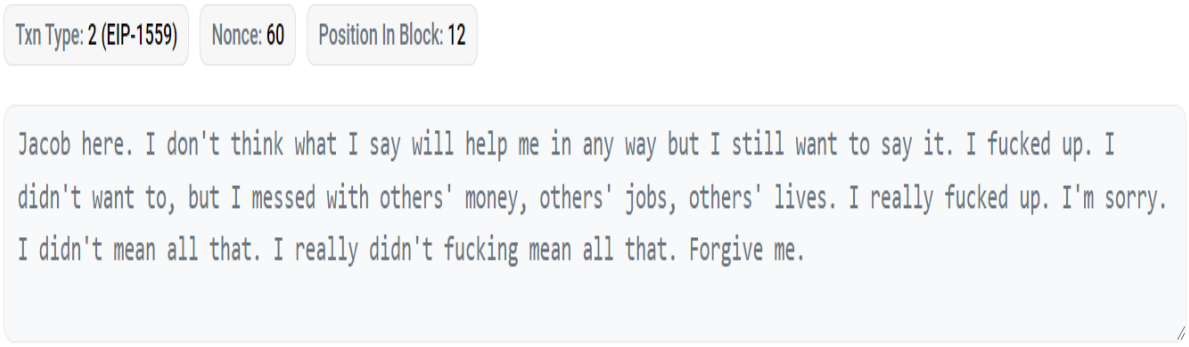
개요

2023 년 3 월 13 일, Ethereum 기반 대출 프로젝트인 Euler Finance 가 플래시 대출 공격의 피해자가 되어 1 억 9,700 만 달러의 손실이 발생했습니다.

2023 년 3 월 16 일, Euler 는 해커의 체포 및 도난된 자금의 반환을 돕는 정보에 대해 100 만 달러의 보상을 제시했습니다.

2023 년 3 월 17 일, Euler Labs 의 CEO 인 Michael Bentley 는 "Euler 는 항상 보안에 신경을 쓴 프로젝트였다"라고 트위터에 게시했습니다. 2021 년 5 월부터 2022 년 9 월까지 Euler Finance 는 Halborn, Solidified, ZK Labs, Certora, Sherlock, Omnisica 를 포함한 여섯 개의 블록체인 보안 기관에 의해 10 번의 감사를 받았습니다.

2023 년 3 월 18 일부터 4 월 4 일까지 공격자는 분할하여 도난된 자금을 반환하기 시작했습니다. 이 기간 동안 공격자는 온체인 메시지를 통해 사과하며 "다른 사람의 돈, 다른 사람의 일, 다른 사람의 삶을 망치는 것"을 인정하고 용서를 청했습니다.



오일러 해커로부터의 온체인 메시지

4 월 4 일, 오일러 랩스(Euler Labs)는 트위터를 통해, 협상에 성공한 후 공격자가 모든 훔친 자금을 반환했다고 발표했습니다.

취약점 분석

이번 공격에서, Etoken 계약의 donateToReserves 함수는 사용자가 보유한 토큰의 실제 금액과 기부 후 사용자의 원장 상태를 제대로 확인하지 못했습니다. 공격자는 이 취약점을 이용하여 1 억 개의 eDAI 를 기부하면서 사실은 3 천만 DAI 만 예치한 상태였습니다.

기부로 인해 사용자의 원장 상태가 청산 기준을 충족하게 되어 대출 계약이 청산되었습니다. 청산 과정에서 eDAI 와 dDAI 가 청산 계약으로 이전되었습니다. 그러나 대출에 대한 많은 부채로 인해 청산 계약은 최대 할인율을 적용하였습니다. 청산이 완료된 후, 청산 계약은 3 억 1,093 만 개의 eDAI 와 2 억 5,931 만 개의 dDAI 를 보유하게 되었습니다.

이 시점에서 사용자의 원장 상태는 복구되어, 사용자는 자금을 인출할 수 있게 되었습니다. 인출 가능한 금액은 eDAI 와 dDAI 의 차이입니다. 그러나 풀에 실제로 사용 가능한 DAI 는 3,890 만 개밖에 없기 때문에, 사용자는 이 부분의 자금만 인출할 수 있었습니다."

```
354    function donateToReserves(uint subAccountId, uint amount) external nonReentrant {
355        (address underlying, AssetStorage storage assetStorage, address proxyAddr, address msgSender) = CALLER();
356        address account = getSubAccount(msgSender, subAccountId);
357
358        updateAverageLiquidity(account);
359        emit RequestDonate(account, amount);
360
361        AssetCache memory assetCache = loadAssetCache(underlying, assetStorage);
362
363        uint origBalance = assetStorage.users[account].balance;
364        uint newBalance;
365
366        if (amount == type(uint).max) {
367            amount = origBalance;
368            newBalance = 0;
369        } else {
370            require(origBalance >= amount, "e/insufficient-balance");
371            unchecked { newBalance = origBalance - amount; }
372        }
373
374        assetStorage.users[account].balance = encodeAmount(newBalance);
375        assetStorage.reserveBalance = assetCache.reserveBalance = encodeSmallAmount(assetCache.reserveBalance + amount);
376
377        emit Withdraw(assetCache.underlying, account, amount);
378        emitViaProxy_Transfer(proxyAddr, account, address(0), amount);
379
380        logAssetStatus(assetCache);
381    }
382 }
```

6.2 BonqDAO

개요

2 월 1 일, DeFi 프로토콜인 BonqDAO 가 가격 조작 공격의 피해자가 되었습니다. 공격자는 1 억 BEUR 을 발행한 후 Uniswap 에서 다른 토큰으로 스왑했습니다. ALBT 의 가격은 거의 0 에 가까워지며, 이로 인해 ALBT 보관소의 청산이 발생했습니다. 공격 당시 토큰 가격을 기준으로 손실은 8,800 만 달러에 이를 정도였습니다. 그러나 유동성이 고갈되었기 때문에 실제 손실은 약 185 만 달러였습니다.

취약성 분석

이 공격에서 공격자는 가격 조작을 통해 두 가지 유형의 공격을 진행했습니다. 하나는 가격을 조작하여 대량의 토큰을 대출하는 것이었고, 다른 하나는 가격을 조작하여 다른 사람의 자산을 청산하고 이로 이익을 얻는 것이었습니다.

BonqDAO 플랫폼의 오라클은 'getCurrentValue' 함수 대신 'getDataBefore' 함수를 사용했습니다. 해커는 10 TRB 토큰을 스테이킹함으로써 가격 보고자가 되었으며, submitValue 함수를 호출하여 오라클에서 WALBT 토큰의 가격을 조작했습니다. 가격을 설정한 후, 공격자는 Bonq 계약에서 createTrove 함수를 호출하여 트로브 계약을 생성하고 0.1 WALBT 를 예금으로 보관했습니다. 일반적으로 대출 한도는 0.1 WALBT 의 가격보다 작아야 하며, 이는 스테이킹 비율이 안전한 범위 내에 있음을 보장합니다. 그러나 이 대출 과정에서 담보 가치는 TellorFlex 계약을 사용하여 계산되었습니다. 이전 단계에서 공격자는 이미 WALBT 에 대해 예외적으로 높은 가격을 설정했으므로, 이 거래에서 공격자는 1 억 BEUR 토큰을 대출한 것입니다.

두 번째 거래에서 공격자는 WALBT 가격을 예외적으로 낮게 설정하여 최소 비용으로 다른 사용자가 스테이킹한 WALBT 토큰을 청산할 수 있었습니다."

6.3 Platypus Finance

개요

2 월 17 일, Avalanche 상의 Platypus Finance 가 체크 메커니즘 결함으로 인해 약 8.5 백만 달러의 손실을 입었습니다. 그러나 공격자는 계약에서 인출 기능을 실행하지 않아 공격 수익은 공격 계약 내에 갇혀 철수할 수 없었습니다.

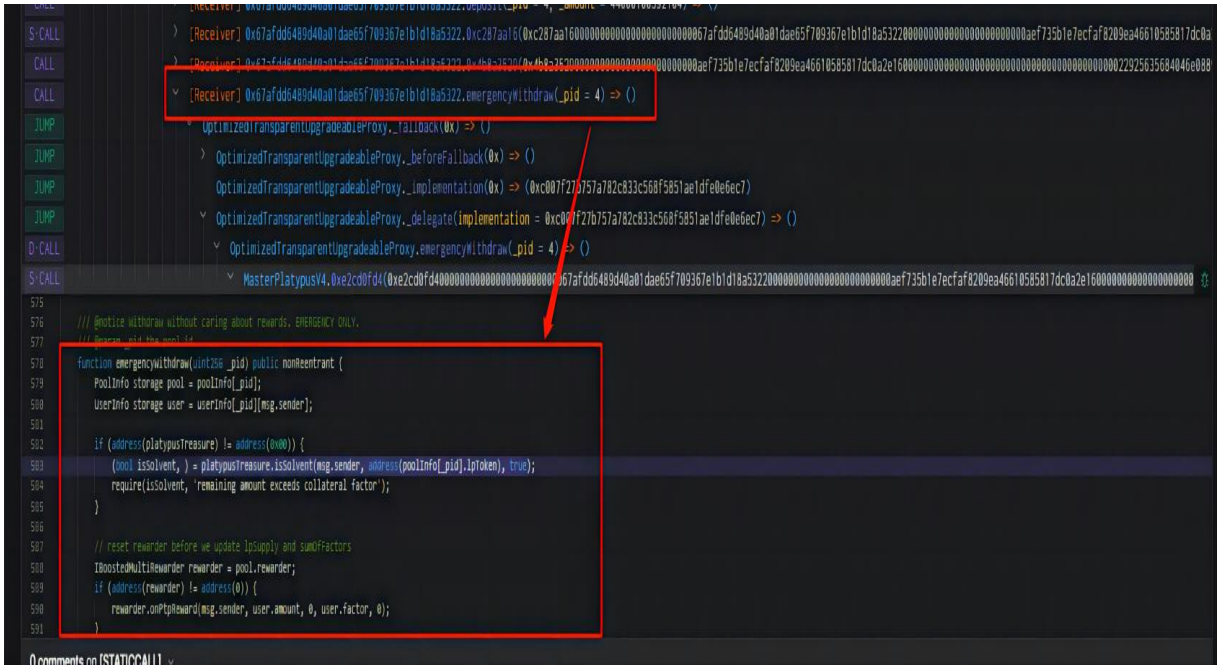
2 월 23 일, Platypus 는 바이낸스와 연락하여 해커의 신원을 확인했다고 발표했습니다. 또한 Platypus 는 사용자들에게 자금의 최소 63%를 상환할 것이라고 밝혔습니다.

2 월 26 일, 프랑스 국립 경찰은 Platypus 를 공격한 것으로 의심되는 두 명의 용의자를 체포하고 소환했습니다.

취약성 분석

공격의 원인은 MasterPlatypusV4 계약의 emergencyWithdraw 함수의 체크 메커니즘 결함이었습니다. 이 함수는 사용자의 차입 금액이 차입 한도(borrowLimitUSP)를 초과하는지만 확인했고, 사용자가 빚을 상환했는지는 검증하지 않았습니다.

공격자는 먼저 AAVE 계약을 사용하여 4400 만 USDC 를 플래시 대출하고 이를 Pool 계약에 입금한 후 4400 만 LP-USDC 를 발행했습니다. 그 다음, 공격자는 borrow 함수를 호출하여 4179 만 USP 를 차용하고 즉시 EmergencyWithdraw 함수를 호출했습니다.



EmergencyWithdraw 함수 내에는 잔액이 최대 대출 가능 금액을 초과하는지 확인하는 isSolvent 함수가 있습니다. 이 함수가 true 를 반환하면 빚을 상환했는지 여부를 고려하지 않고 이체 작업을 수행합니다. 따라서 공격자는 이 함수를 성공적으로 호출하여 이전에 입금한 4400 만 LP-USDC 를 빚을 상환하지 않고 인출할 수 있었습니다.

6.4 Yearn Finance

개요

2023 년 4 월 13 일, Yearn Finance 의 yusdt 계약이 플래시 대출 공격에 취약해져 해커는 1,000 만 달러 이상의 이익을 얻었습니다. yUSDT 계약이 1,000 일 전에 배포될 때 잘못된 구성을 받았던 것으로 보입니다. Fulcrum iUSDT 대신 Fulcrum iUSDC 를 잘못 사용하여 잘못 배포되었습니다.

5 월 26 일, Yearn 공격자는 4,134 ETH 를 Tornado Cash 로 이전했습니다.

취약성 분석

공격은 주로 yUSDT 토큰 계약의 잘못된 구성을 악용했습니다. 풀을 선택하는 재균형 과정에서 추가 금액으로 USDT 토큰만 사용되었으며, USDC 토큰은 풀 추가에 유효하지 않았습니다. 결과적으로, 공격자가 USDC 를 사용하여 계약 내의 모든 USDT 를 "소모"하면 풀 잔액이 0 이 되어 공격자가 상당한 수의 토큰을 생성할 수 있게 되었습니다.

```
679   function rebalance() public {
680     Lender newProvider = recommend();
681
682     if (newProvider != provider) {
683       _withdrawAll();
684     }
685
686     if (balance() > 0) {
687       if (newProvider == Lender.DYDX) {
688         supplyDydx(balance());
689       } else if (newProvider == Lender.FULCRUM) {
690         supplyFulcrum(balance());
691       } else if (newProvider == Lender.COMPOUND) {
692         supplyCompound(balance());
693       } else if (newProvider == Lender.AAVE) {
694         supplyAave(balance());
695       }
696     }
697
698     provider = newProvider;
699   }
```

```
556   function balance() public view returns (uint256) {
557     return IERC20(token).balanceOf(address(this));
558   }
```

6.5 MEV bot

개요

2023 년 4 월 3 일, 여러 MEV bot 들이 악성 선취 알고리즘 공격에 취약해져 약 2,500 만 달러의 손실을 입었습니다.

Sandwich 공격은 DeFi 에서 인기 있는 프론트런닝 기술입니다. "Sandwich" 거래를 실행하기 위해

공격자(포식 트레이더라고 함)는 대상 트랜잭션을 식별하고 해당 트랜잭션의 앞과 뒤에 자신의 트랜잭션을 배치하여 피해자를 공격합니다. 이 전략은 매수 및 매도 주문을 악용하여 자산 가격을 조작합니다.

Sandwich 거래의 목표는 피해자가 경험하는 예기치 않은 슬리피지(slippage)를 이용하는 것입니다. 또한, MEVBot 의 전략을 반대로 사용하는 악성 미끼 bot 들이 있습니다. 이들은 악성 미끼 토큰이나 특정 금액을 전송 함수에서 활용하는 등의 전술을 사용합니다. 이 특정한 공격에서는 MEVBot 과 관련된 취약점이 악용되었습니다.

취약성 분석

악성 노드는 MEV-boost-relay 와 관련된 취약점을 이용하여 악성 선취 알고리즘 공격을 통해 가격을 조작하고 최종적으로 이익을 얻었습니다. 보통 악의적인 제안자가 번들을 수정하는 것은 이중 서명 벌칙 때문에 어려울 것입니다. 그러나 이 공격은 parent_root 와 state_root 를 0x00 으로 설정하여 PublishBlock 이 오류를 반환하도록 만들었습니다. 이전 버전에서 오류 처리가 부족한 상태에서 이러한 공격으로 노출된 번들에 접근할 수 있게 되었고, 이로 인해 이벤트가 발생하게 되었습니다.

```
983  978
     979  +        // Publish the signed beacon block via beacon-node
     980  +        signedBeaconBlock := SignedBlindedBeaconBlockToBeaconBlock(payload, getPayloadResp)
     981  +        code, err := api.beaconClient.PublishBlock(signedBeaconBlock) // errors are logged inside
     982  +        if err != nil {
     983  +                log.WithError(err).WithField("code", code).Error("failed to publish block")
     984  +                api.RespondError(w, http.StatusBadRequest, "failed to publish block")
     985  +                return
     986  +        }
     987  +
     988  +        // give the beacon network some time to propagate the block
     989  +        time.Sleep(time.Duration(getPayloadResponseDelayMs) * time.Millisecond)
     990  +
984  991           api.RespondOK(w, getPayloadResp)
985  992           log = log.WithFields(logrus.Fields{
986  993                   "numTx":       getPayloadResp.NumTx(),
     @@ -1014,16 +1021,6 @@ func (api *RelayAPI) handleGetPayload(w http.ResponseWriter, req *http.Request)
1014 1021                           log.WithError(err).Error("failed to increment builder-stats after getPayload")
1015 1022                   }
1016 1023           }()
1017      -
1018      -        // Publish the signed beacon block via beacon-node
1019      -        go func() {
1020      -                if api.ffDisableBlockPublishing {
1021      -                        log.Info("publishing the block is disabled")
1022      -                        return
1023      -                }
1024      -                signedBeaconBlock := SignedBlindedBeaconBlockToBeaconBlock(payload, getPayloadResp)
1025      -                _, _ = api.beaconClient.PublishBlock(signedBeaconBlock) // errors are logged inside
1026      -        }()
1027 1024   }
1028 1025
```

공격자는 먼저 유동성이 낮은 풀을 대상으로하여 MEV bot 이 트랜잭션을 선취하는지를 테스트했습니다. 공격자가 테스트를 성공적으로 실행한 후, 이전에 Uniswap V3 에서 스왑한 대량의 토큰을 사용하여 유동성이 낮은 V2 풀 내에서 스왑을 수행했습니다. 그들은 MEV bot 을 유인하여 그들의 모든 WETH 를 가치가 낮은 토큰의 선취 매수에 사용하도록 했습니다. 그러나 선취된 트랜잭션은 실제로 MEV 를 향한

공격 트랜잭션으로, MEV 가 방금 선취에 사용한 WETH 와 교환하기 위해 상당한 양의 토큰을 WETH 로 스왑했습니다. 결과적으로 MEV bot 이 WETH 를 다시 스왑하려고 시도했을 때, 이미 공격 트랜잭션에 의해 WETH 가 스왑되어 실패하게 되었습니다.

7. 전형적인 타입의 AML 보안 사고

Atomic Wallet 6,700 만 달러 도난 사건

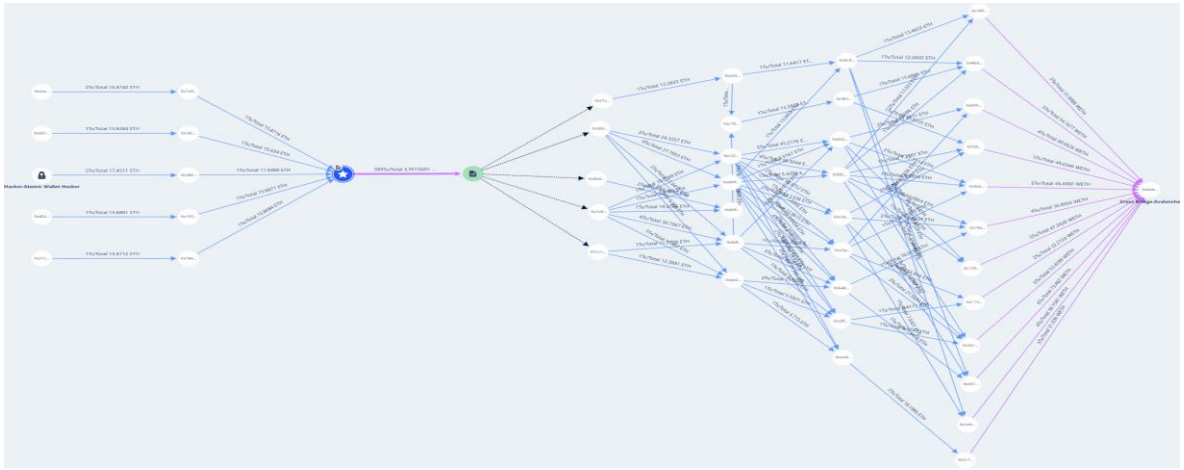
6 월 3 일, 여러 Atomic Wallet 사용자들이 소셜 미디어에서 자신의 지갑 자금이 도난당했다고 보고했습니다. 이 공격으로 약 6,700 만 달러 이상의 손실이 발생했습니다. 도난된 자금은 BTC, ETH 및 TRX 를 포함한 총 21 개의 체인에 주로 집중되었습니다.

Ethereum

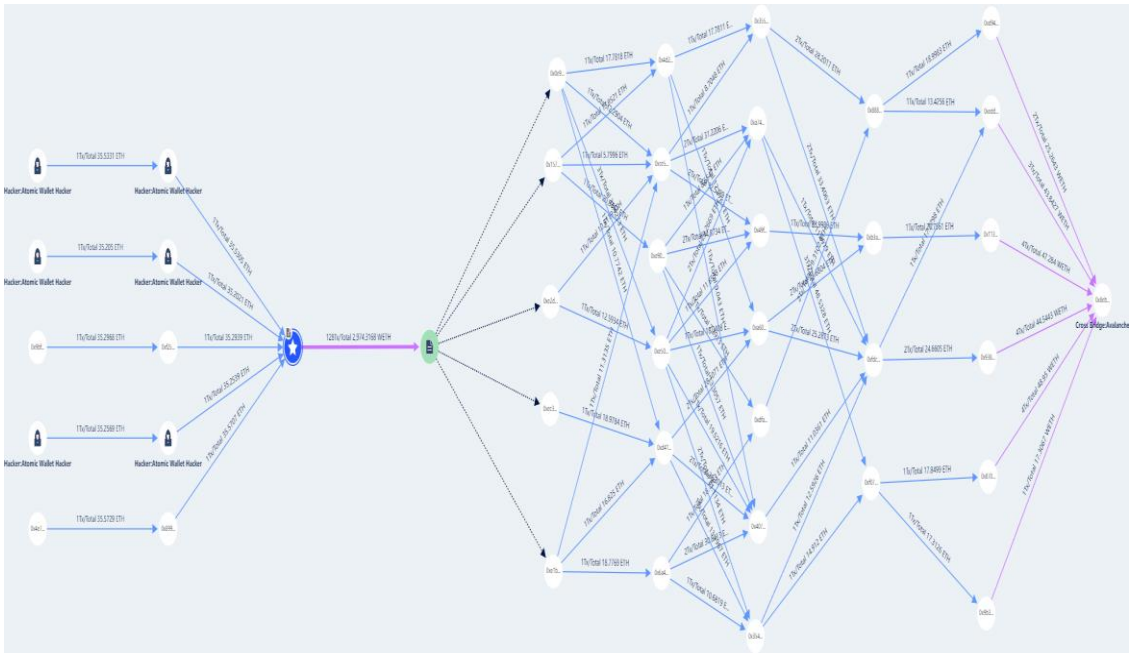
Ethereum 에서는 두 가지 주요한 자금 세탁 방법이 있습니다:

1. 계약 다양화와 Avalanche 크로스 체인을 통한 자금 세탁
해커들은 가치 있는 코인을 퍼블릭 블록체인의 기본 통화로 전환합니다. 그런 다음, 집계를 위해 두 개의 계약을 활용합니다.
계약 주소는 ETH 를 두 번의 전송을 통해 WETH 로 전환하여 ETH 를 통합합니다. 그런 다음, 계약 다양화를 위해 WETH 를 다른 계약으로 전송합니다. 이 계약 다양화는 Avalanche 의 지갑 주소로 최대 다섯 단계까지 전송을 통해 크로스 체인 작업을 용이하게 합니다. 이 크로스 체인 작업은 계약을 포함하지 않고 Avalanche 내부 회계 거래에 관련됩니다.

통합 계약 1:



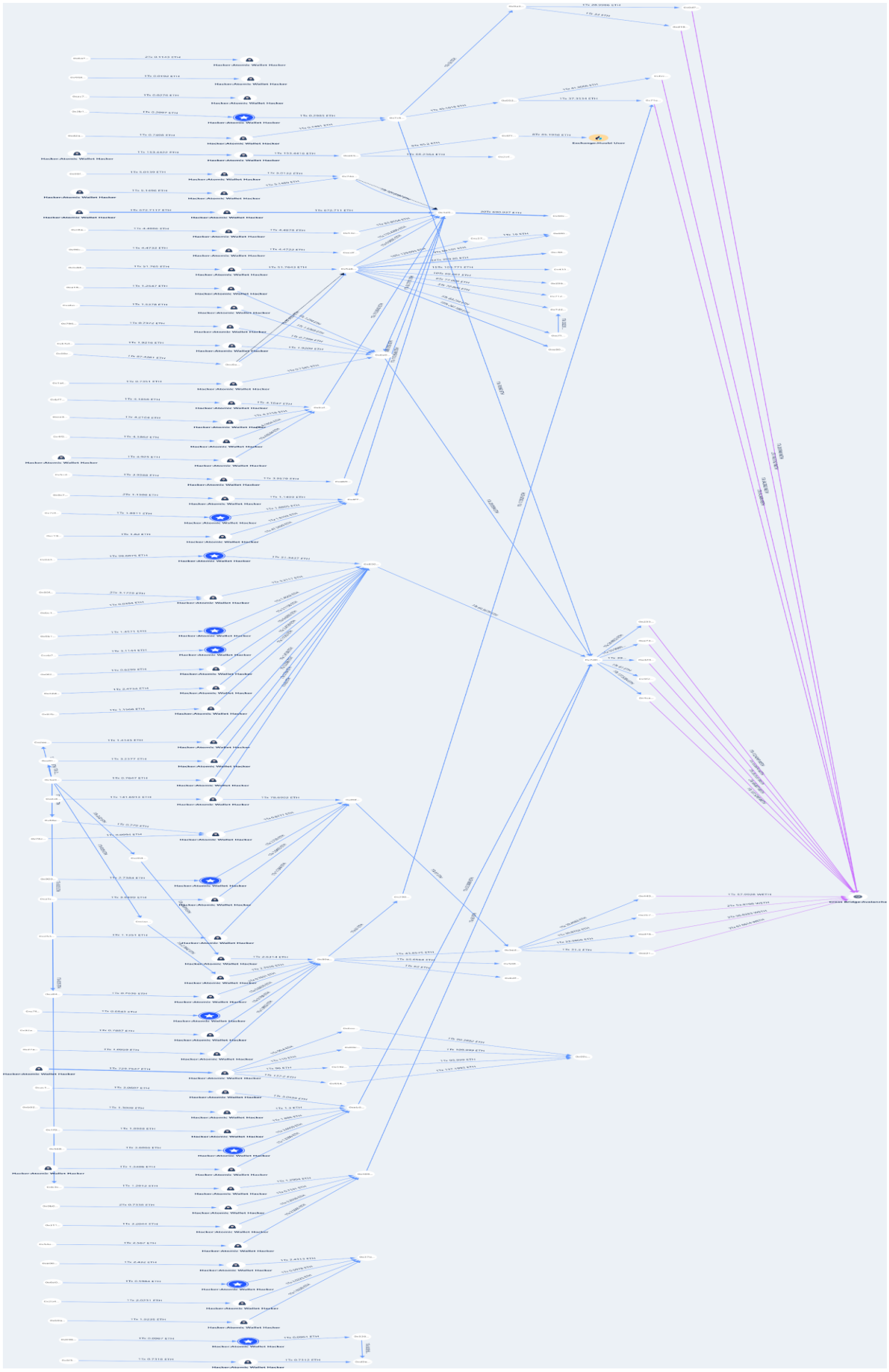
통합 계약 2 :



2. 계약 없이 직접 다양화하고 다양한 크로스 체인 브리지 프로토콜 및 거래소를 통해 자금 세탁

이 자금 세탁 부분은 계약을 사용하지 않고 직접 자금을 다양화하고 다양한 크로스 체인 브리지 프로토콜과 거래소를 활용하는 것을 포함합니다.

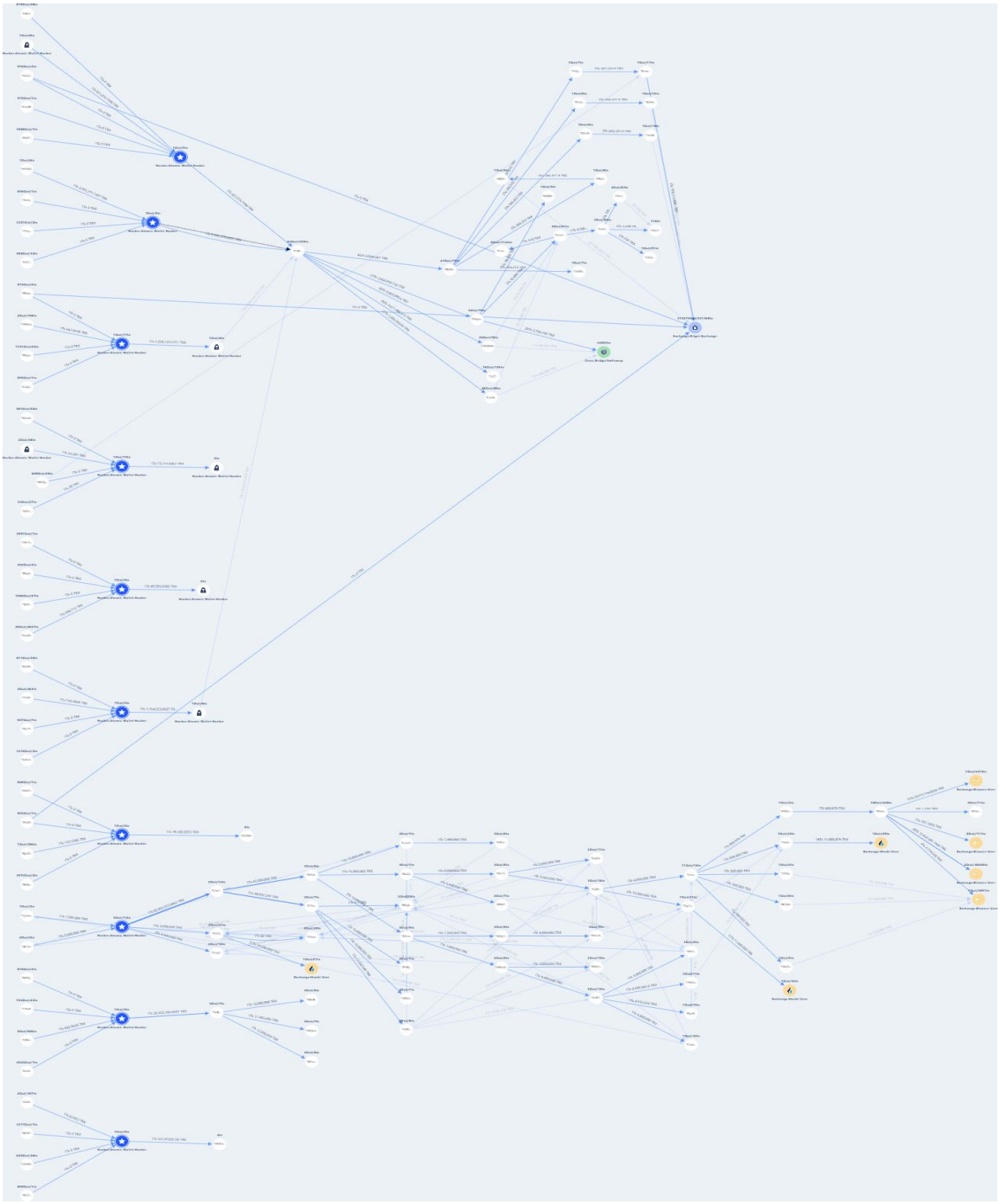
이 부분에서의 총 금액은 현재 9,896 ETH 로 기록되며, 다중 집계 주소를 통해 통합될 것입니다. 금융 연계도는 다음과 같습니다:


Hacker:Atomic Wallet Hacker
Exchange:Huobi User
Cross Bridge:Avalanche

TRON

Ethereum 체인과 유사하게 TRON 에서도 도난당한 지갑 가상 통화는 추가적인 이체 전에 두 단계의 주소를 거쳐 TRX 로 완전히 전환됩니다. 그러나 대조적으로, 집계 주소는 계약 기반이 아닌 일반적인 주소입니다. 다양한 거래소 예금 주소로 자금을 다각화한 후 이체됩니다. 일부 도난당한 자금은 전송되지 않은 채로 체인 상에 남아 있으며, 다양한 통합 주소가 있습니다.

해커들이 사용하는 다양한 돈세탁 경로가 관찰될 수 있으며, 이는 주로 다양한 거래소 계정을 통한 돈세탁을 포함합니다. 자금이 직접 크로스체인 브리지 계약으로 흐르는 경우도 있습니다.

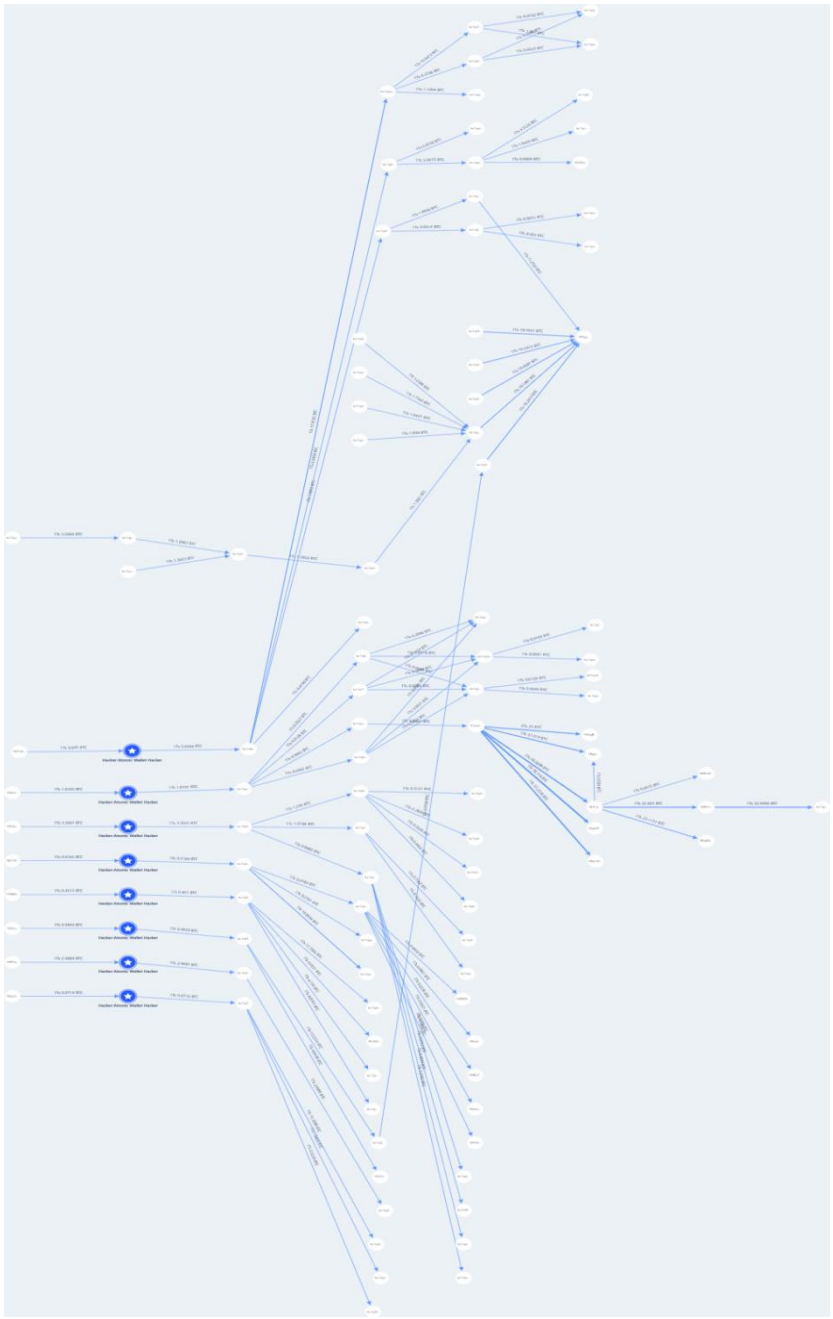


Beosin KYT – TRON

BTC Chain

BTC 와 관련된 알려진 집계 주소들은 총 420.882 BTC 를 포함하고 있습니다. BTC 체인에서는 이러한 주소들이 여러 집계 주소로 분산되어 있습니다. 통합 이후에는 이러한 주소들 간에 자금이 교차 이동되지 않으며, 이는 다양한 통합 주소들이 존재함을 나타냅니다.
기타 체인들과 마찬가지로, 도난된 지갑 자금은 직접 해커가 제어하는 주소로 이체됩니다. 그런 다음 해커는 자금을 제어하고 이를 중개인 주소 한 단계를 거쳐 집계 주소로 이체하여 다양화합니다. 다양화 과정은 적어도 네 단계를 거치며, 그 이후에는 자금이 입금되거나 더 큰 거래량을 갖는 의심스러운 자금 세탁 주소로 혼합될 수 있습니다.

아래 다이어그램에서 경로 패턴이 나와 있습니다:



Beosin KYT - BTC

최근 몇 년 동안 사이버 범죄, 자금 세탁 및 다크 웹 거래 등을 포함한 가상 자산 관련 범죄가 점점 더 늘어나고 있습니다. 블록체인의 탈중앙화, 개방성 및 익명성과 같은 특성으로 인해 규제 기관에게 상당한

어려움이 발생하고 있습니다.

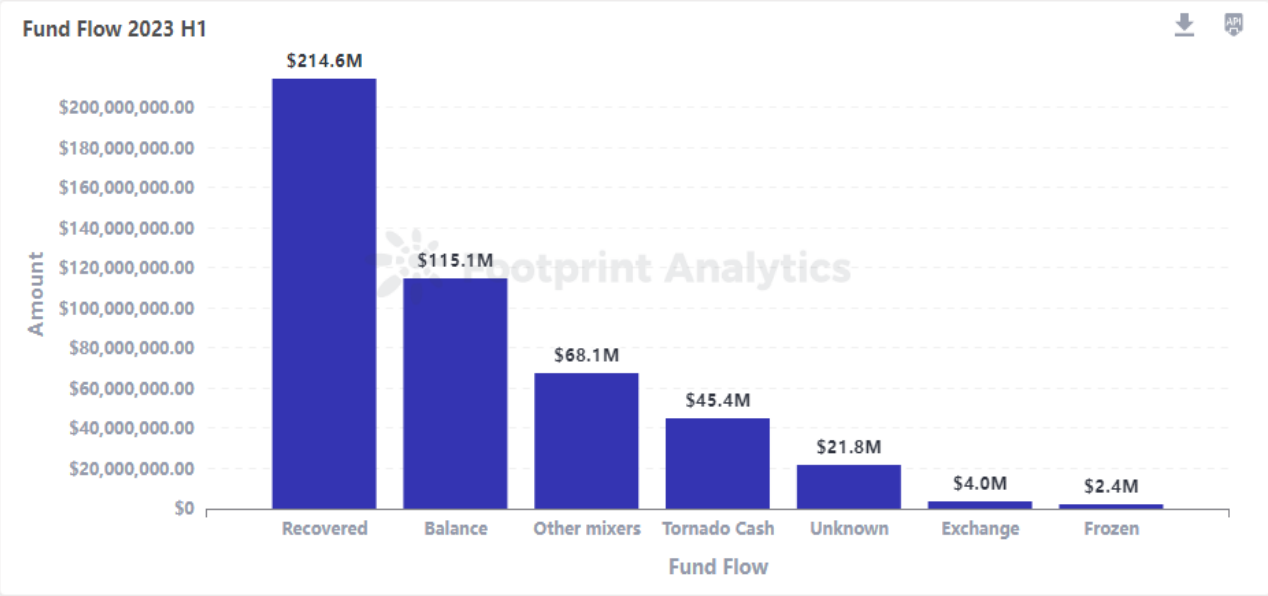
이러한 문제에 대응하기 위해 Beosin 을 비롯한 다양한 보안 기관들은 KYT(Know Your Transactions)라는 솔루션을 제안했습니다. KYT 의 목적은 거래 플랫폼과 규제 기관이 블록체인 상의 모든 거래를 이해할 수 있도록 하는 것입니다. 전통적인 금융 거래에서는 금융 서비스 제공 업체들이 KYC(Know Your Customer) 절차와 거래 데이터 분석을 통해 자금 세탁 방지 시스템을 구축합니다. 가상 자산 거래 분야에서는 거래 플랫폼들이 KYC 및 KYT 기술을 활용하여 각 거래를 관련된 주체와 연결하고, 거래 행위를 분석하며, 범죄 패턴을 식별하고, 체인 상의 분석 및 추적 도구를 사용하여 각 거래를 추적하고 프로파일링하여 사용자들을 평가함으로써 범죄자들이 가상 자산을 세탁하는 위험을 줄이는 데 도움이 됩니다.

Beosin KYT 는 사용자의 특정한 요구와 능력에 기반한 맞춤형 컴플라이언스 솔루션을 제공합니다. 블랙 어드레스 조회, 제재 목록 필터링, 어드레스/거래 위험 점수 산정, 어드레스 모니터링 및 알림, 추적 및 조사 기능과 같은 기능 외에도 Beosin KYT 는 맞춤형 리스크 전략 관리, 가상 자산 경로의 AI 기반 시각화 및 STR(의심스러운 거래 보고서) 익스포트 기능도 제공합니다. Beosin KYT 는 이미 여러 나라와 지역의 기관, 거래소, 지갑 회사 및 기타 업체에 서비스를 제공했습니다. Binance, OKX, HashKey Group 등과 같은 협력 고객도 있습니다.

8 . 도난자금흐름

도난된 자산의 45.5%가 회수되었습니다.

2023 년 상반기에 Beosin KYT 라는 가상 자산의 안티머니 로더링 컴플라이언스 및 분석 플랫폼에 따르면, 약 2 억 1,500 만 달러의 도난된 자산이 회수되었습니다. 이는 도난된 자산의 45.5%에 해당합니다. 그 반면, 2022 년에는 도난된 자산의 8%만이 회수되었습니다. 2023 년에는 자금 회수의 가능성이 크게 증가했습니다. 도난된 자산 회수를 위한 해커와의 협상 외에도, 보안 기업, 법 집행 기관 및 지역사회의 공동 노력을 통해 회수가 이루어지는 사례가 증가하고 있습니다. 게다가 전 세계적인 규제 체계의 개선과 강화된 집행 노력은 해커 활동에 대한 억제력으로 작용하고 있습니다.



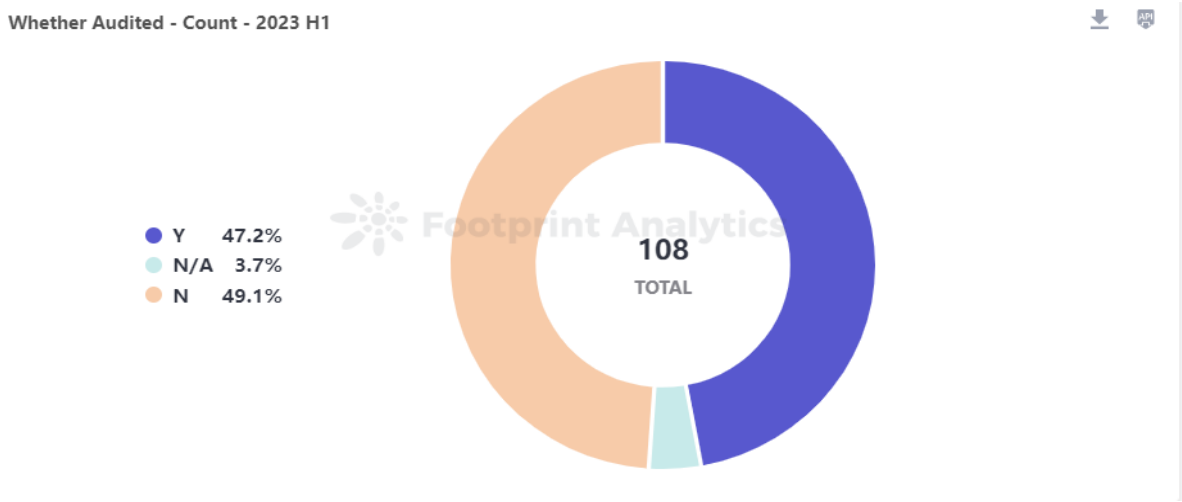
Stolen Fund Flow 2023 H1

도난된 자산 중 약 1 억 1,300 만 달러가 믹서로 이체되었습니다. 이 중 약 4,538 만 달러가 Tornado Cash 로 이체되었고, 약 6,814 만 달러가 다른 믹서 플랫폼으로 이체되었습니다. Tornado Cash 는 2022 년 8 월에 미국 외환자산청(OFAC)에 의해 제재를 받은 이후로 Tornado Cash 를 통해 혼합된 자금의 총액이 크게 감소했습니다. 그러나 FixedFloat 와 Sinbad 와 같은 다른 믹서 플랫폼의 사용은 현저히 증가한 것으로 나타났습니다.

9 감사 상태 분석

감사를 받은 프로젝트와 감사를 받지 않은 프로젝트의 비율은 거의 동일합니다.

108 개의 공격당한 프로젝트 중, 51 개는 감사를 받은 적이 있었고, 53 개는 감사를 받지 않은 상태였습니다. 이 비율은 2022 년과 거의 동일합니다.



Whether Audited by Count

51 개의 감사된 프로젝트 중 31 개(60%)가 계약 취약점으로 인해 공격을 받았습니다. 이 비율은 작년의 45%보다 높으며, 이는 전체 감사 시장의 품질이 여전히 낙관적이지 않음을 나타냅니다. 프로젝트 팀은 전문적인 보안 회사를 찾아 감사를 받아야 합니다.

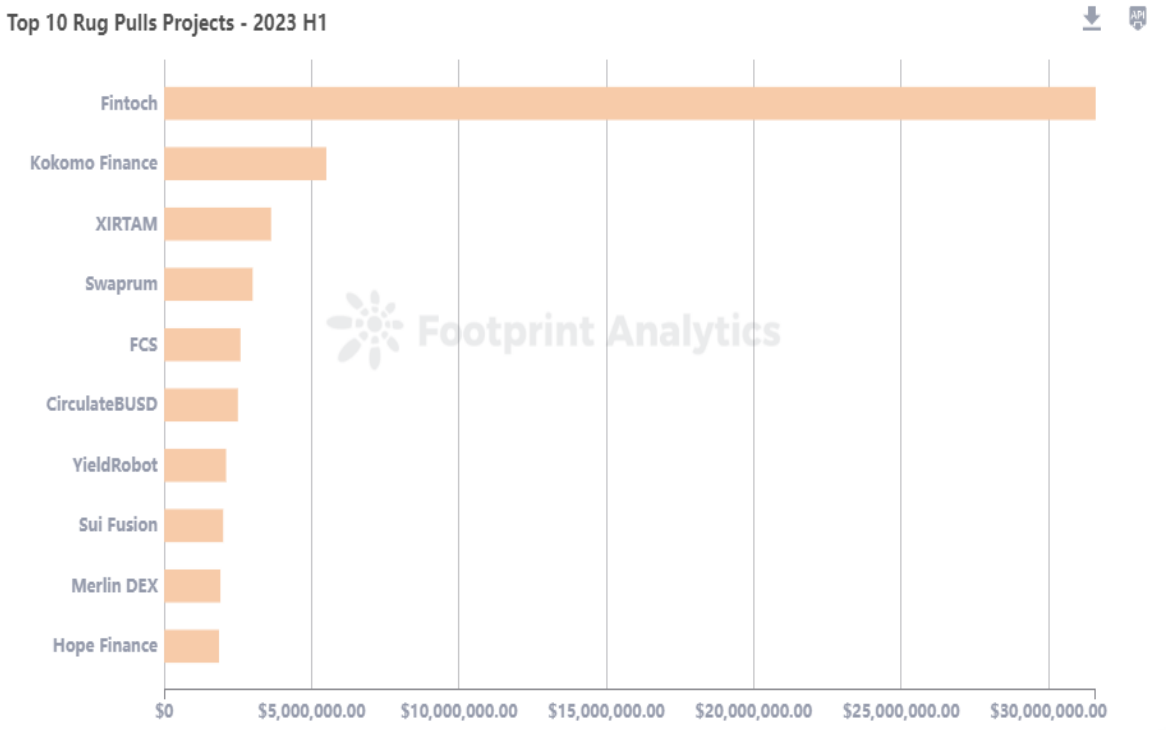
10 러그 풀

110 건의 러그 풀 사건으로 인해 7,587 만 달러가 손실되었습니다.

2023 년 상반기 웹 3 분야에서는 총 110 건의 주요한 러그 풀 사건이 발생하여 약 7,587 만 달러가 연루되었습니다.

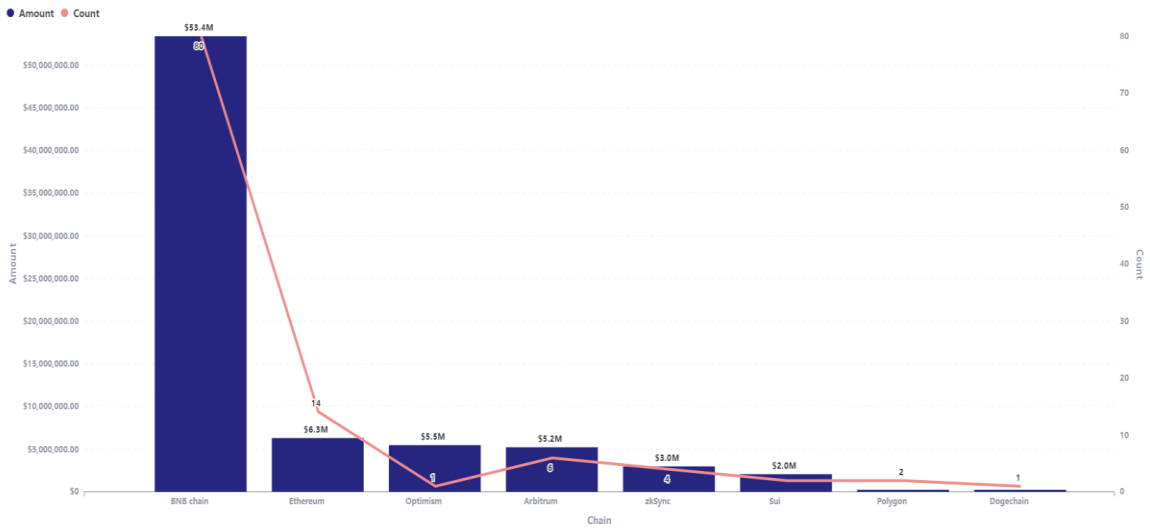
금액 기준으로 보면, 1 백만 달러를 초과하는 금액으로 발생한 러그 풀 사건은 14 건(12.7%)이었고, 10 만 달러에서 1 백만 달러 사이의 범위에서 발생한 사건은 41 건(37.3%)이었으며, 10 만 달러 미만의 금액으로 발생한 사건은 55 건(50%)이었습니다.

가장 큰 금액으로 발생한 러그 풀 사건은 Fintoch 프로젝트로, 약 3,160 만 달러의 자산을 약탈하였습니다.



Top 10 Rug Pulls H1 2023

블록체인 관점에서, BNB 체인은 80 건의 러그 풀 사건을 겪었으며, 이는 다른 공개적인 블록체인들보다 훨씬 높은 금액인 53.37 백만 달러에 이를 포함하고 있었습니다.



Rug Pulls by chain

11 요약

전반적으로, 웹 3 공간에서의 해킹으로 인한 총 손실은 2022 년에 비해 크게 감소했습니다. 2022 년 상반기에는 공격으로 인한 총 손실이 약 19 억 달러였으며, 이는 2022 년 하반기에 약 16.9 억 달러로

감소했습니다. 그러나 2023 년 상반기에는 이 값이 4 억 7,000 만 달러로 떨어지고, 약 2 억 1,500 만 달러의 훔친 자산이 회수되었습니다. 해킹 사례는 상당한 속도 감소를 보였으며, 이러한 현상에 기여한 주된 이유로는 전 세계적인 규제 체계의 점진적인 개선, 법 집행 기관의 노력 증대, 프로젝트들 사이의 보안 인식 개선, Tornado Cash 의 제재, 그리고 암호화폐 규정 준수 기술 및 절차의 개선이 있었습니다. 또한, 해커 신원을 식별하고 훔친 자금을 회수하기 위해 커뮤니티가 오프체인 정보에 의존하는 사례도 있었습니다.

해커 공격의 상당한 감소에도 불구하고, 스마트 컨트랙트 보안 문제는 무시할 수 없습니다. 2023 년 상반기에 가장 빈번하고 재정적 영향력이 큰 공격 유형은 스마트 컨트랙트 취약점을 이용한 공격이었습니다. 총 60 건의 스마트 컨트랙트 취약점 사례로 인해 2 억 6,400 만 달러의 손실이 발생했으며, 대부분의 취약점은 비즈니스 로직 결함과 관련이 있었습니다. 일부 복잡한 비즈니스 로직 취약점은 경험 많은 전문적인 감사 회사가 식별할 필요가 있습니다. Beosin 감사 팀은 모든 해킹 사례를 깊이 있는 분석을 통해 다루며 (트위터 @BeosinAlert), 이러한 사건에서 얻은 지식과 기술을 감사 과정에 적용하여 잠재적인 공격에 대응합니다.

해커 공격의 감소 추세와는 반대로, 일반 사용자를 대상으로 한 피싱 사기는 더욱 빈번해지고 있습니다. 2023 년 상반기에는 Venom Drainer 를 중심으로 한 일련의 지갑 강탈 그룹이 등장했습니다. 그들은 판매를 위해 악성 도구킷을 개발하며, 구매자들은 피싱 피해자를 성공적으로 유인한 후 수익을 공유합니다. 이러한 피싱 사기는 광범위한 사용자에게 영향을 미쳤으며, Venom Drainer 만으로도 최소 15,000 명 이상의 피해자가 있었습니다. 일반 사용자들에게는 보안 회사의 경보를 정기적으로 주시하고, 피싱 및 도난 방지 관행을 체계적으로 학습하고, 피싱 방지 플러그인, 거래 사전 실행 도구 및 기타 알림을 설치하는 것이 좋습니다 (그러나 도구에만 의존하지 않고, 스스로의 보안 인식을 강화하는 것이 항상 우선되어야 합니다).