Chainalysis

보고서

북한, 사상 최대 규모 20억 달러 암호화폐 절도 사건 발생... 누적 총액 67억 5천만 달러 기록

2025년 12월 18일 | CHAINALYSIS 팀 작성

요약

- 북한 해커들은 2025년에 20억 2천만 달러 상당의 암호화폐를 훔쳤는데, 이는 전년 대비 51% 증가한 수치이며, 공격 횟수는 줄었음에도 불구하고 누적 피해액은 67억 5천만 달러에 달합니다.

Chainalysis

도 사건 발생 후 45일 이내에 자금세탁이 완료되는 것으로도 나타났습니다.

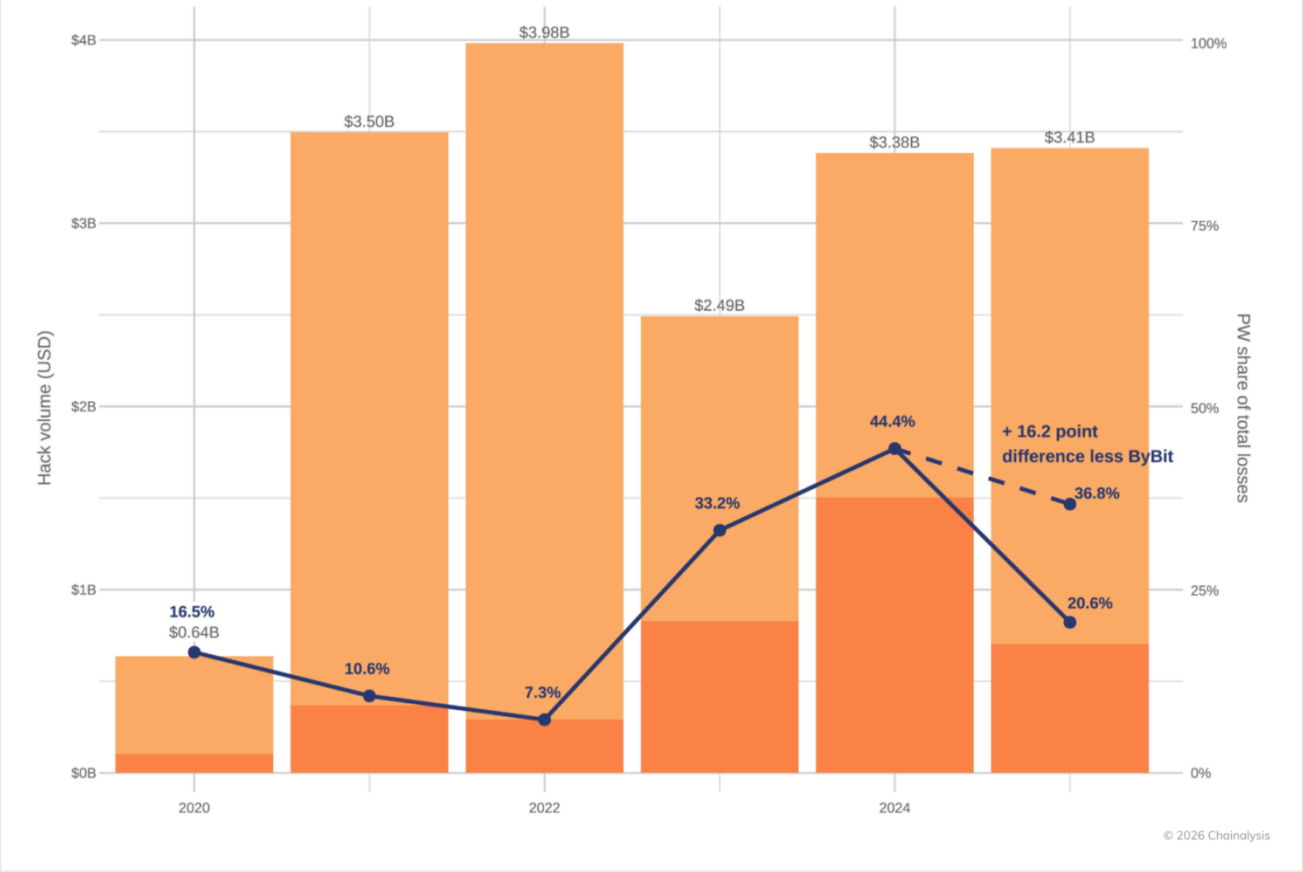
- 개인 지갑 해킹 사건은 2025년에 15만 8천 건으로 급증하여 8만 명의 피해자가 발생했지만, 도난당한 총액(7억 1천 3백만 달러)은 2024년보다 감소했습니다.
- 탈중앙화 금융(DeFi)에 예치된 총 자산(TVL)이 증가했음에도 불구하고, 2024-2025년 해킹 손실은 억제된 상태를 유지했는데, 이는 개선된 보안 관행이 의미 있는 효과를 내고 있음을 시사합니다.

2025년에도 암호화폐 생태계는 또 다른 어려운 한 해를 맞이했으며, 도난 자금은 계속해서 증가세를 보였습니다. 저희 분석에 따르면 암호화폐 도난 패턴에 변화가 나타났는데, 이는 네 가지 주요 특징으로 요약됩니다. 첫째, 주요 위협 행위자로서 북한(조선민주주의공화국)의 지속적인 존재, 둘째, 중앙 집중식 서비스에 대한 개인 공격의 심각성 증가, 셋째, 개인 지갑 해킹의 급증, 넷째, 탈중앙화 금융(DeFi) 해킹 추세의 예상치 못한 차이입니다.

이러한 패턴은 데이터에서 명확하게 드러나며, 다양한 플랫폼 유형과 피해자 유형에 걸쳐 암호화폐 도난이 발생하는 방식에 상당한 변화가 있음을 보여줍니다. 디지털 자산 사용이 확대 되고 가치가 최고치를 경신함에 따라, 이러한 진화하는 보안 위협을 이해하는 것이 점점 더 중요해지고 있습니다.

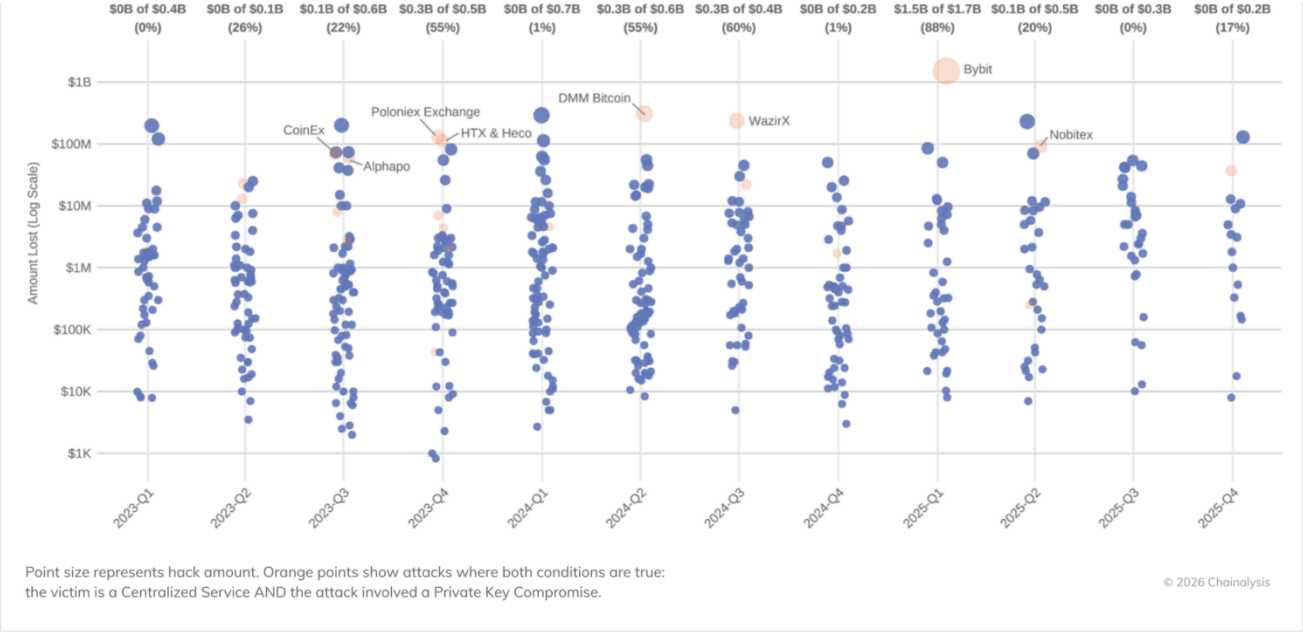
전체적인 상황: 2025년에 34억 달러 이상이 도난당할 것으로 예상됩니다.

암호화폐 업계에서는 2025년 1월부터 12월 초까지 34억 달러 이상의 도난 사건이 발생했으며, 그 중 2월에 발생한 바이비트(Bybit) 해킹 사건 만으로 15억 달러가량 손실되었습니다.



표면적인 수치 이면에 숨겨진 중요한 변화는 이러한 절도 사건의 구성에서 드러납니다. 개인 지갑 해킹은 크게 증가하여 2022년 전체 도난 금액의 7.3%에서 2024년 44%로 급증했습니다. 만약 바이비트(Bybit) 공격의 영향이 크지 않았다면 2025년에는 그 비율이 37%에 달했을 것입니다.

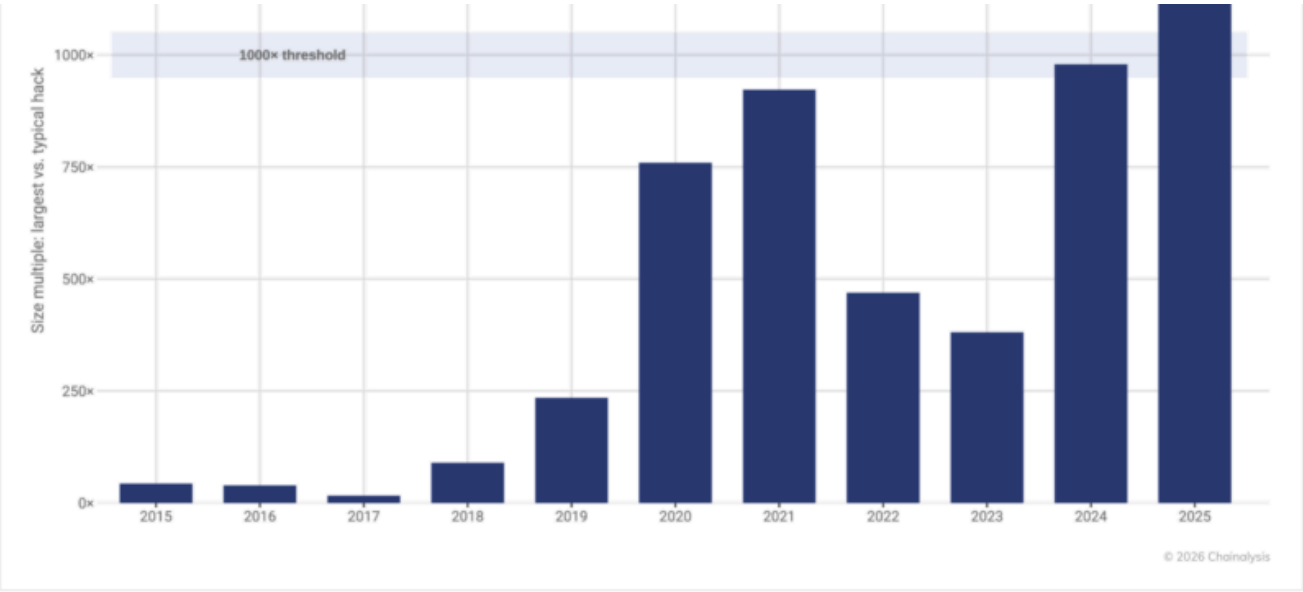
한편, 중앙 집중식 서비스는 개인 키 인프라 및 서명 프로세스에 대한 정교한 공격으로 인해 점점 더 큰 손실을 입고 있습니다. 이러한 플랫폼들은 막대한 기관 자원과 전문 보안팀을 보유하고 있음에도 불구하고, 콜드 월렛 제어를 우회할 수 있는 고도화된 위협에 여전히 취약합니다. 이러한 침해는 빈번하게 발생하지는 않지만(아래 차트 참조), 발생할 경우 그 규모가 엄청나서 전체 손실액의 88%를 차지할 것으로 예상됩니다. 많은 공격자들이 타사 지갑 통합을 악용하고 정당한 서명자를 속여 악성 거래를 승인하도록 유도하는 방법을 개발했습니다.



높은 수준의 데이터 유출이 지속되는 것은 암호화폐 보안 의 일부 영역은 개선되고 있을지라도 공격자들이 여전히 다양한 경로를 통해 공격을 감행하고 있음을 시사합니다.

상위 3개 해킹 유형이 전체 손실의 69%를 차지하며, 극단적인 경우는 중간값의 1,000배에 달하는 손실을 기록했습니다.

지금까지 자금 탈취 활동은 예외적인 사건에 의해 좌우되었으며, 대부분의 해킹은 비교적 소규모였지만 일부는 엄청난 규모였습니다. 그러나 2025년에는 놀라운 증가세가 나타났습니다. 가장 큰 해킹 사건과 전체 사건의 중간값 사이의 비율이 처음으로 1,000배를 넘어섰습니다. 가장 큰 공격으로 탈취된 자금은 이제 일반적인 사건에서 탈취된 자금보다 1,000배나 더 많으며, 2021년 강세장 최고치를 넘어섰습니다. 이러한 계산은 탈취 당시의 자금 가치를 기준으로 합니다.



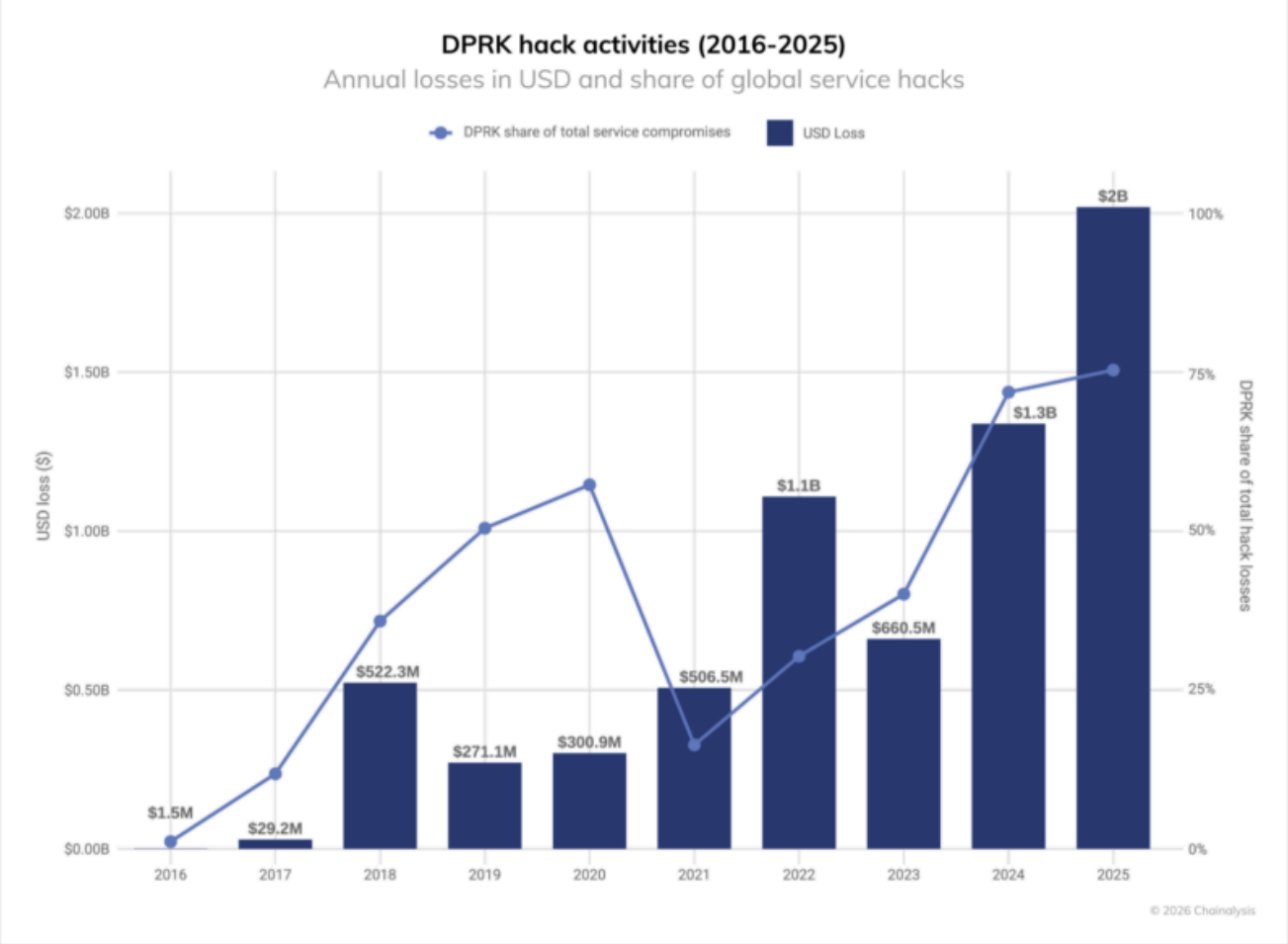
이러한 격차 확대는 손실을 극적으로 집중시키고 있습니다. 2025년 가장 큰 해킹 사고 세 건이 전체 서비스 손실의 69%를 차지할 것으로 예상되며, 이는 개별 사고가 연간 총 손실액에 엄청난 영향을 미치는 상황을 초래합니다. 사고 발생 건수는 변동이 있을 수 있고 자산 가격 상승에 따라 평균 손실액도 증가하지만, 개별 침해 사고로 인한 막대한 피해 가능성은 훨씬 더 빠르게 증가하고 있습니다.

북한은 확인된 사건 발생 건수는 줄었지만 여전히 주요 암호화폐 위협 행위자로 남아 있습니다.

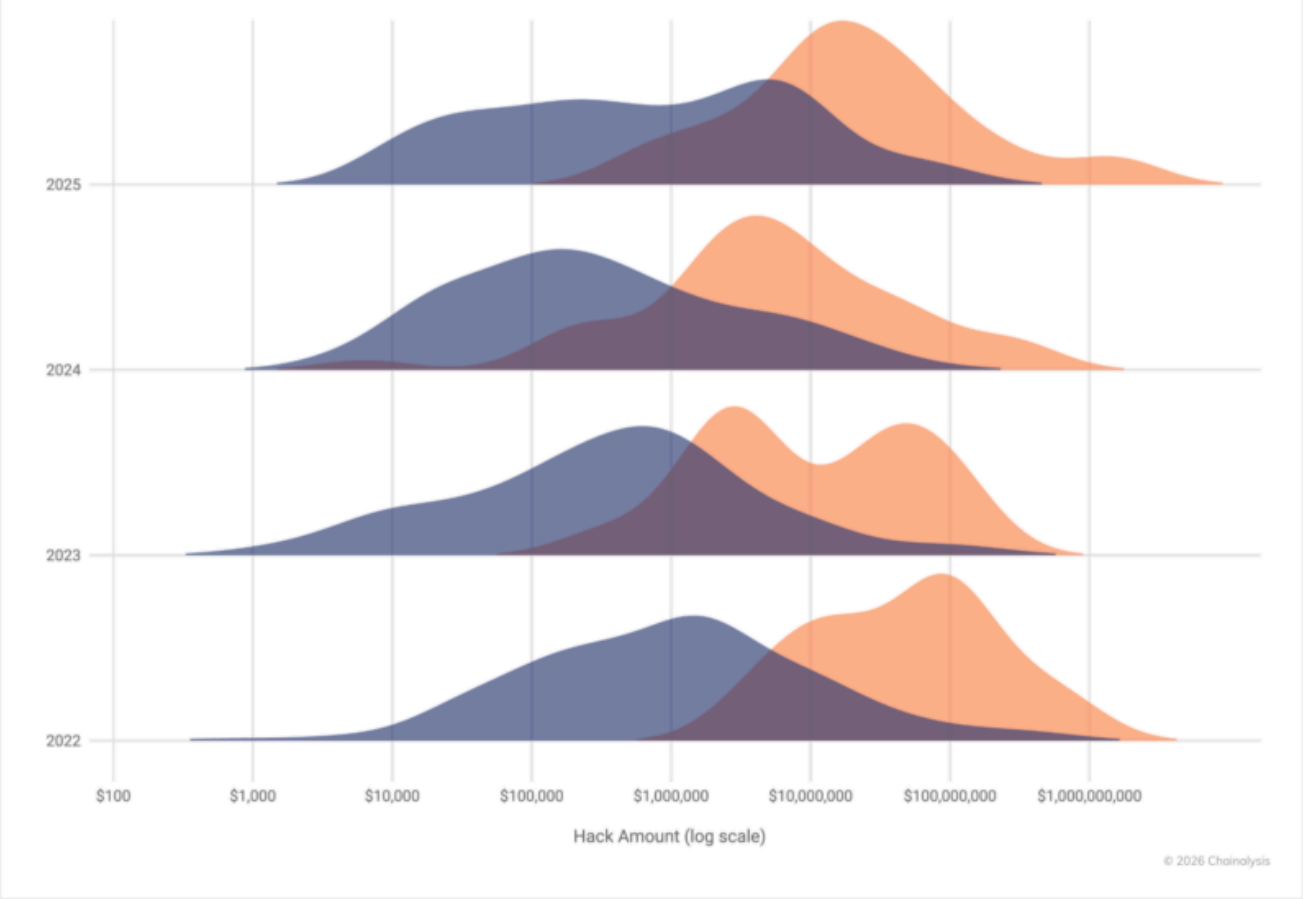
북한(조선민주주의공화국)은 암호화폐 보안에 대한 가장 심각한 국가 차원의 위협으로 남아 있으며, 공격 빈도가 급격히 감소했음에도 불구하고 탈취 금액 면에서 기록적인 한 해를 보냈습니다. 2025년 북한 해커들은 최소 20억 2천만 달러(2024년 대비 6억 8천1백만 달러 증가) 상당의 암호화폐를 탈취했으며, 이는 전년 대비 51% 증가한 수치입니다. 이는 탈취 금액 기준으로 북한의 암호화폐 탈취가 사상 최고치를 기록한 해이며, 전체 서비스 침해 사례 중 북한의 공격이 76%를 차지하는 기록적인 수치이기도 합니다. 2025년 수치를 종합하면 북한이 탈취한 암호화폐 자금의 누적 추정치는 최소 67억 5천만 달러에 달할 것으로 예상됩니다.

북한의 위협 행위자들은 IT 직원을 암호화폐 서비스 내부에 침투시켜 특권 접근 권한을 확보하고 대규모 침해를 가능하게 하는 주요 공격 방식을 점점 더 많이 사용하고 있습니다. 이는 북한의 주요 공격 경로 중 하나입니다. 올해 기록적인 공격 증가는 거래소, 수탁기관, 웹3 기업 등에 IT 직원을 침투시키는 방식에 대한 의존도가 높아진 것을 반영하는 것으로 보이며, 이는 대규모 해킹 공격에 앞서 초기 접근 및 횡적 이동을 가속화할 수 있습니다.

하지만 최근 들어 북한과 연계된 공격자들은 이러한 IT 직원 사기 모델을 완전히 뒤집고 있습니다. 단순히 채용 공고에 지원하여 직원으로 위장하는 대신, 유명 웹3 및 AI 기업의 채용 담당자를 사칭하여 가짜 채용 절차를 진행하고 있습니다. 이 과정은 "기술 심사"로 마무리되며, 피해자의 현재 고용주 계정에 접속하기 위한 자격 증명, 소스 코드, VPN 또는 SSO 접근 권한을 빼내는 것을 목표로 합니다. 임원급에서도 유사한 사회공학적 수법이 사용되고 있는데, 전략적 투자자 또는 인수자를 사칭



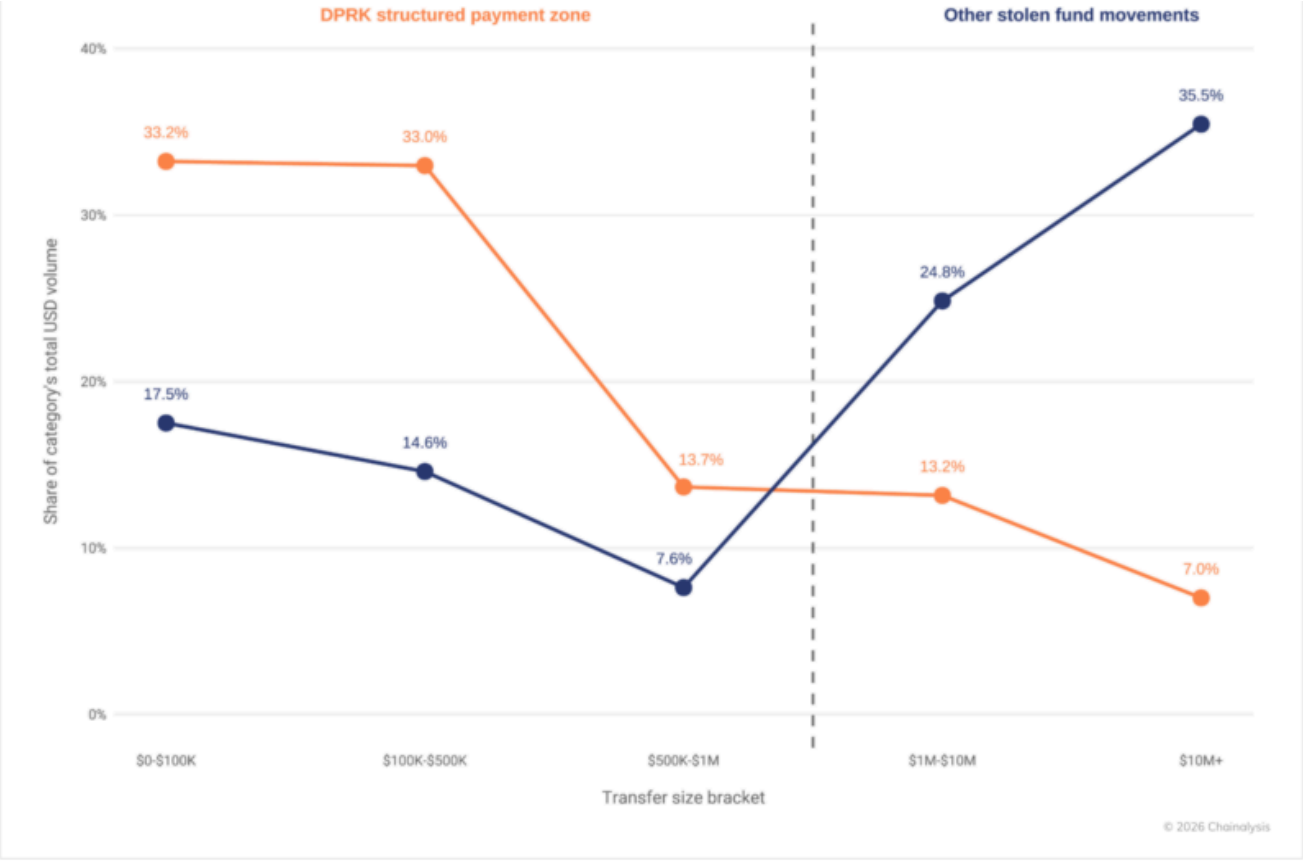
지난 몇 년간 보아왔듯이, 북한은 다른 위협 행위자들에 비해 훨씬 더 큰 규모의 공격을 지속적으로 감행하고 있습니다. 아래 차트에서 볼 수 있듯이, 2022년부터 2025년까지 북한 소행으로 추정되는 해킹 공격은 가장 높은 규모의 피해를 입힌 반면, 북한과 무관한 해킹 공격은 모든 규모의 피해액이 고르게 분포되어 있습니다. 이러한 패턴은 북한 해커들이 공격 시 대규모 서비스를 표적으로 삼아 최대의 피해를 입히는 것을 목표로 한다는 점을 다시 한번 보여줍니다.



올해 기록적인 수익은 작년보다 훨씬 적은 수의 사건에서 발생했습니다. 이러한 변화, 즉 적은 사건으로 훨씬 더 많은 수익을 올린 것은 2025년 2월에 발생한 대규모 바이비트(Bybit) 해킹 사건의 영향을 반영합니다.

북한의 독특한 세탁 방식

2025년 초에 발생한 대규모 도난 자금 유입은 북한 연계 세력이 어떻게 대규모로 암호화폐를 자금 세탁하는지 에 대한 전례 없는 통찰력을 제공합니다 . 이들의 수법은 다른 사이버 범죄자들과는 확연히 다르며 시간이 지남에 따라 진화하여 현재의 운영 선호도와 잠재적 취약점을 드러냅니다.



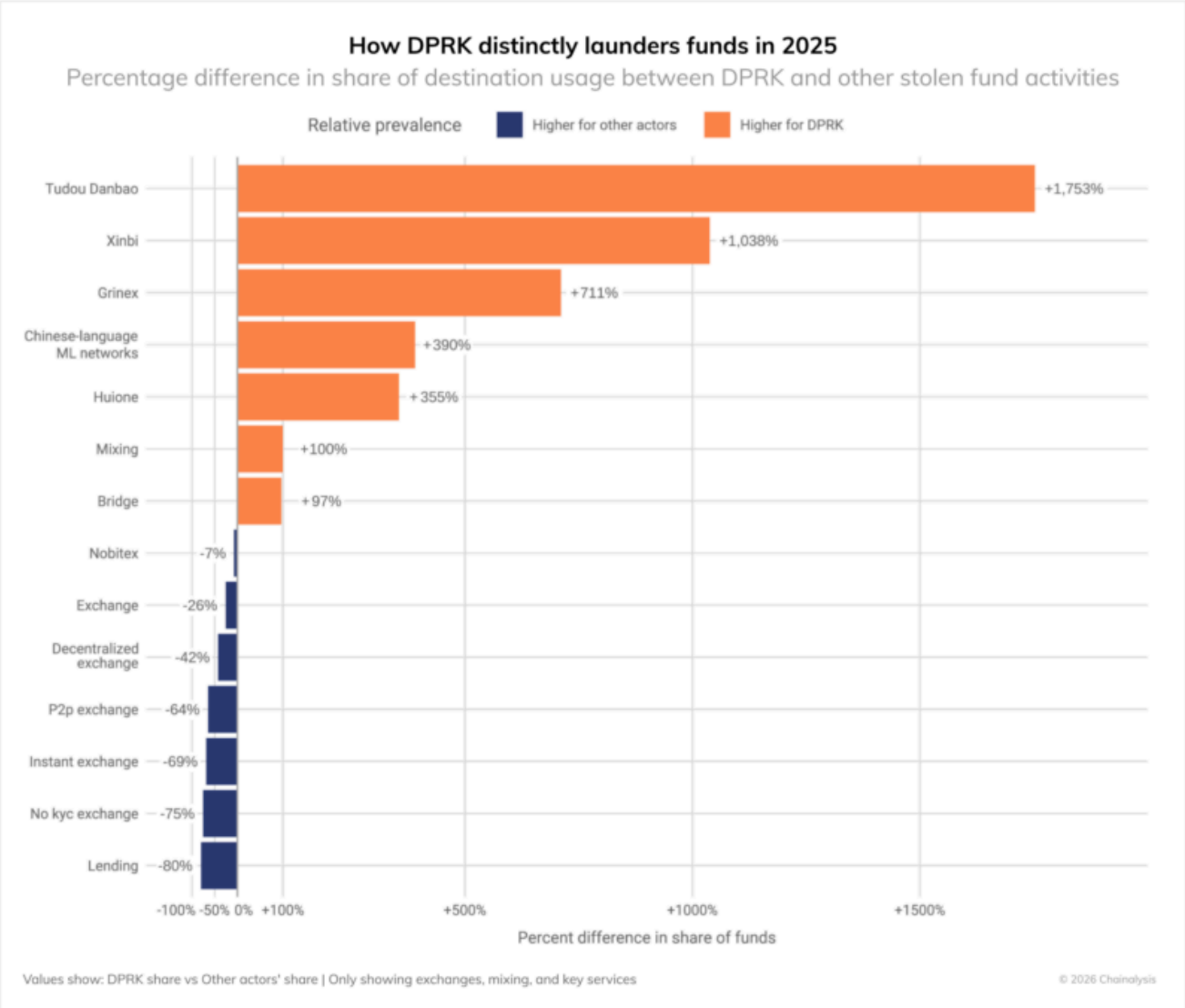
북한의 자금세탁은 뚜렷한 패턴으로 나타나는데, 전체 거래량의 60% 이상이 50만 달러 미만의 소액 이체에 집중되어 있습니다. 반면, 다른 자금세탁 관련자들은 전체 자금의 60% 이상을 100만 달러에서 1,000만 달러 이상에 이르는 소액으로 나누어 온체인에 이체합니다. 북한은 다른 자금세탁 위협 세력보다 훨씬 많은 금액을 훔치면서도, 온체인 결제를 소액으로 나누어 처리하는 정교한 수법을 사용하고 있습니다.

다른 자금 세탁 관련자들과 비교했을 때, 북한은 특정 자금 세탁 경로에 대한 뚜렷한 선호도를 보인다.

북한 해커들은 다음과 같은 것들을 매우 선호하는 경향이 있습니다:

- 중국어 기반 자금 이동 및 보증 서비스(+355%~+1000% 이상): 이들의 가장 두드러진 특징은 중국어 기반 보증 서비스와 자금 세탁 네트워크에 크게 의존한다는 점이며, 이러한 네트워크는 여러 세탁업자로 구성되어 있고 규제 준수 체계가 취약할 수 있습니다.
- 브리지 서비스(+97% 차이): 블록체인 간 자산 이동 및 추적을 어렵게 하기 위해 크로스체인 브리지에 크게 의존함
- 혼합 서비스 이용 증가(+100% 차이): 자금 흐름을 은폐하기 위해 혼합 서비스를 더 많이 이용함
- Huione과 같은 전문 서비스(+356%): 자금 세탁 작업을 용이하게 하는 특정 서비스를 전략적으로 활용

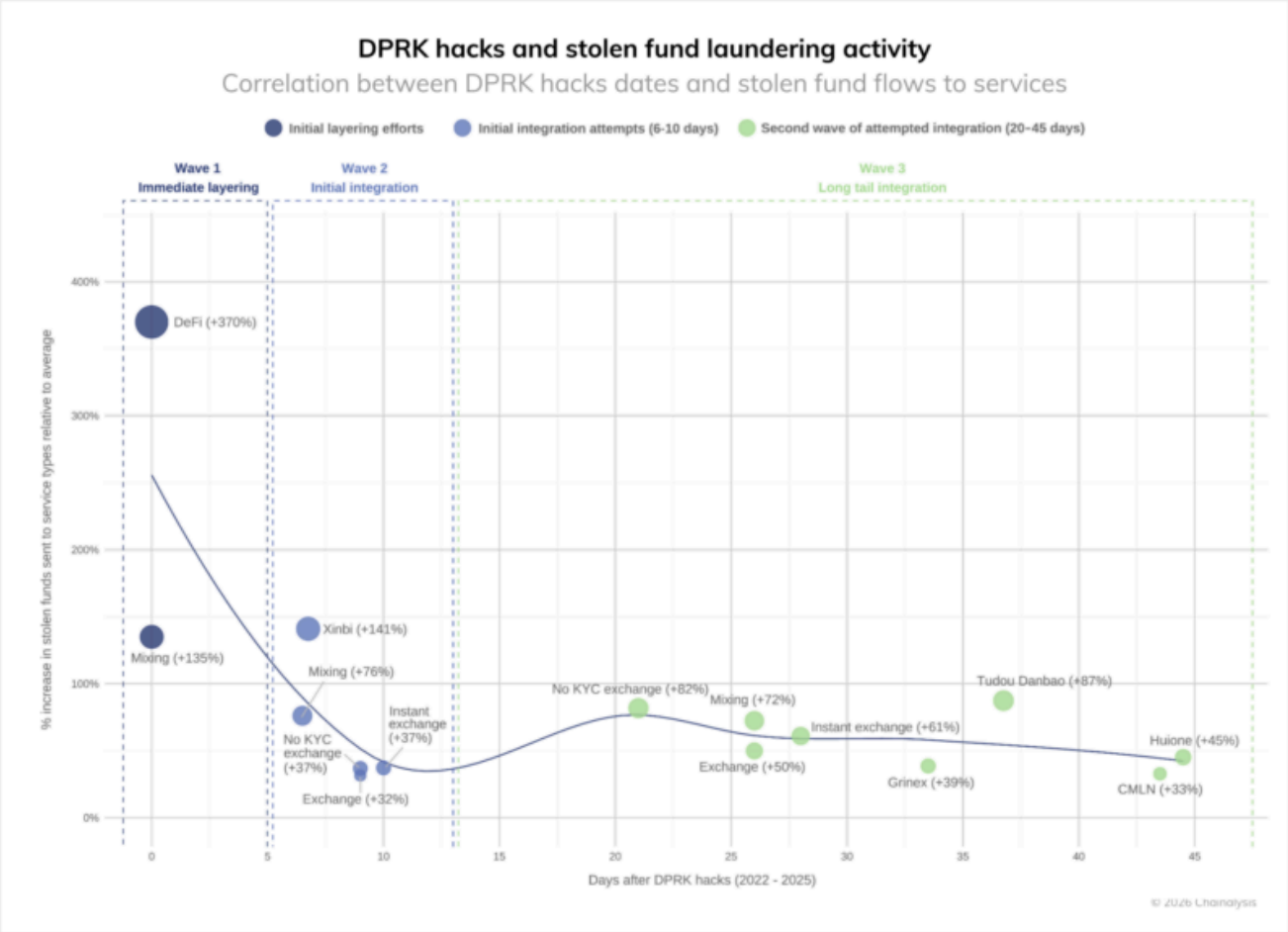
- KYC 없는 거래소 이용률 감소(-75% 차이): 놀랍게도, 다른 위협 행위자들이 북한보다 KYC가 필요 없는 거래소를 더 많이 이용하는 것으로 나타났습니다.
- P2P 거래(-64% 차이): 북한은 P2P 플랫폼에 대한 관심이 제한적인 것으로 나타났습니다.
- 중앙 집중식 거래(-25% 차이): 다른 범죄자들은 기존 거래 플랫폼과 더 직접적인 상호 작용을 보이는 것으로 나타났습니다.
- 탈중앙화 거래소(DEX)(-42% 차이): 다른 위협 행위자들은 유동성과 익명성 때문에 탈중앙화 거래소를 훨씬 더 선호합니다.



이러한 패턴은 북한이 국가 지원을 받지 않는 사이버 범죄자들과는 다른 제약 조건과 목표 하에서 활동하고 있음을 시사합니다. 북한이 중국어 전문 자금 세탁 서비스와 장외거래(OTC) 업체를 집중적으로 이용하는 것은 북한의 위협 행위자들이 아시아 태평양 지역 전반의 불법 행위자들과 긴밀하게 연계되어 있음을 나타내며, 이는 평양이 국제 금융 시스템에 접근하기 위해 중국 기반 네트워크를 역사적으로 이용해 온 것과 일맥상통합니다.

Chainalysis

[illegible] 세탁 경로를 거쳤습니다.



1차 단계: 즉시 레이어링(0~5일)

해킹 발생 후 초기 며칠 동안, 우리는 해킹 자금의 출처로부터 자금을 즉시 빼돌리려는 활동에 집중하는 이례적인 급증 현상을 관찰했습니다.

- 탈중앙화 금융(DeFi) 프로토콜은 도난 자금 유입이 가장 급증(+370%)한 주요 진입점입니다.
- 혼합 서비스 이용량이 크게 증가(+135~150%)하면서 1차적인 정보 은폐가 시작되었습니다.
- 이 단계는 최초 절도 사건으로부터 거리를 두기 위한 긴급한 "선제적 조치" 노력을 나타냅니다.

2차 단계: 초기 통합 (6~10일)

두 번째 주가 시작되면서 전략은 자금을 더 넓은 생태계에 통합하는 데 도움이 될 수 있는 서비스 중심으로 전환됩니다.

- KYC 절차가 간소화된 거래소(+37%)와 중앙 집중식 거래소(+32%)에서 자금 유입이 시작되었다.

- 이 단계는 자금이 잠재적인 유출입로로 이동하기 시작하는 중요한 전환기를 나타냅니다.

3차 파동: 장기 통합(20~45일)

최종 단계에서는 법정화폐 또는 기타 자산으로의 최종 전환을 용이하게 하는 서비스에 대한 선호도가 뚜렷하게 나타납니다.

- 본인 인증 절차가 필요 없는 거래소(+82%)와 투도우 단바오와 같은 보증 서비스(+87%)가 크게 증가했습니다.
- 즉시 환전(+61%)과 후이오네(Huione)와 같은 중국어 플랫폼(+45%)이 최종 환전 지점 역할을 합니다.
- 중앙 집중식 거래소(+50%) 또한 자금을 받는데, 이는 합법적인 자금 흐름과 섞으려는 정교한 시도가 있었음을 시사합니다.
- 중국어 자금세탁 네트워크(+33%) 및 Grinex(+39%)와 같은 플랫폼으로 대표되는 규제가 덜한 관할 지역이 이러한 패턴을 완성합니다.

자금세탁 활동이 일반적으로 45일이라는 기간 내에 이루어진다는 점은 법 집행 기관과 준법감시팀에 매우 중요한 정보를 제공합니다. 이러한 패턴이 여러 해에 걸쳐 지속된다는 것은 북한과 연계된 행위자들이 직면한 운영상의 제약, 즉 금융 인프라에 대한 접근성 부족과 특정 조력자와의 협력 필요성 등을 시사합니다.

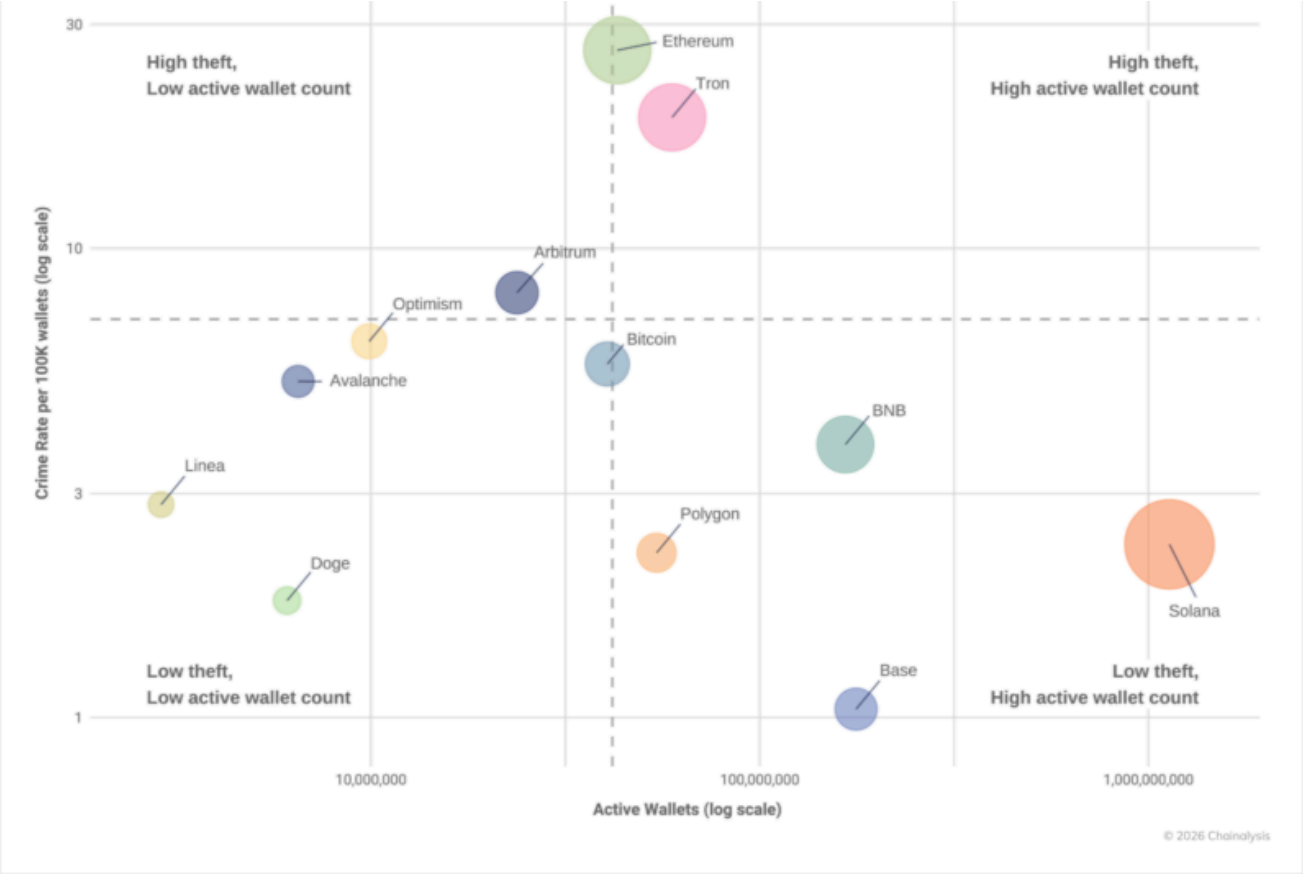
이러한 행위자들이 항상 정확히 이와 같은 시간표를 따르는 것은 아니지만(일부 도난 자금은 수개월 또는 수년 동안 휴면 상태로 남아 있기도 함), 이 패턴은 자금 세탁을 적극적으로 수행할 때 나타나는 일반적인 온체인 행동을 나타냅니다. 또한, 개인 키 전송이나 장외 암호화폐-법정화폐 거래와 같은 특정 활동은 추가적인 정보 보강 없이는 온체인에서 확인할 수 없으므로, 이러한 분석에는 잠재적인 사각지대가 존재할 수 있다는 점을 인지해야 합니다.

개인 지갑 보안 침해: 개인 사용자에게 점점 더 커지는 위협

온체인 패턴 분석과 피해자 및 업계 파트너의 보고를 통해 개인 지갑 해킹의 규모를 파악할 수 있지만, 실제 해킹 건수는 훨씬 더 많을 것으로 예상됩니다. 하한 추정치에 따르면, 개인 지갑 해킹으로 인한 전체 도난 금액은 2025년에 20%를 차지할 것으로 예상되며, 이는 2024년의 44%에서 감소한 수치로 규모와 패턴 모두에서 진화한 것입니다. 전체 도난 사건은 2025년에 15만 8천 건으로 급증하여 2022년의 5만 4천 건에 비해 거의 3배에 달할 것으로 전망됩니다. 피해자 수도 2022년 4만 명에서 2025년에는 최소 8만 명으로 증가할 것으로 예상됩니다. 이러한 급격한 증가는 암호화폐 사용 증가에 기인한 것으로 보입니다. 예를 들어, 활성 개인 지갑 수가 가장 많은 블록체인 중 하나인 솔라나(Solana)에서는 가장 많은 사건(약 2만 6천 5백 건)이 발생했습니다.

하지만 사건 발생 건수와 피해자 수는 증가했음에도 불구하고, 개별 피해자로부터 탈취한 총액은 2024년 최고치인 15억 달러에서 2025년 7억 1,300만 달러로 감소했습니다. 이는 공격자들이 더 많은 사용자를 표적으로 삼고 있지만, 피해자 한 명당 탈취하는 금액은 줄어들고 있음을 시사합니다.

네트워크별 피해 데이터는 암호화폐 사용자에게 가장 큰 위험을 초래하는 영역을 파악하는 데 추가적인 통찰력을 제공합니다. 아래 차트는 네트워크별 활성 개인 지갑 수를 기준으로 조정된 피해 데이터를 보여줍니다. 2025년 10만 개 지갑당 범죄율을 측정했을 때, 이더리움과 트론이 가장 높은 절도율을 보였습니다. 이더리움은 규모가 크기 때문에 절도율과 피해자 수가 모두 높으며, 트론은 활성 지갑 수가 적음에도 불구하고 절도율이 높은 것으로 나타났습니다. 반면, 베이스와 솔라나는 상당한 사용자 기반에도 불구하고 낮은 절도율을 보였습니다.



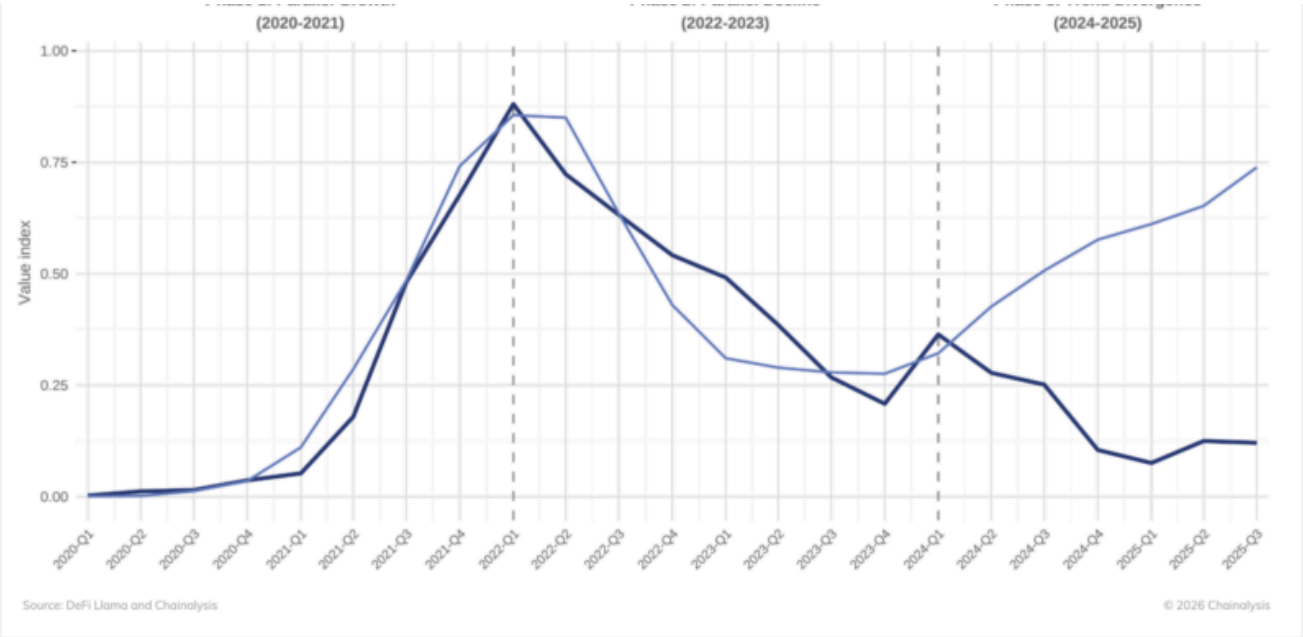
이러한 측정 가능한 차이는 개인 지갑 보안 위험이 암호화폐 생태계 전반에 걸쳐 균일하지 않다는 점을 강조합니다. 유사한 기술 아키텍처를 가진 블록체인 간에 피해 발생률이 차이가 나는 것은 기술적 요인 외에도 사용자 인구 통계, 인기 애플리케이션, 범죄 조직 인프라와 같은 요소들이 도난 발생률을 결정하는 데 중요한 역할을 한다는 것을 시사합니다.

디파이 해킹: 분기 패턴이 시장 변화를 예고한다

탈중앙화 금융(DeFi) 부문은 2025년 범죄 데이터에서 독특한 패턴을 보이며, 과거 추세와 뚜렷한 차이를 나타낼 것으로 예상됩니다.

데이터는 뚜렷한 세 단계를 보여줍니다.

- 1단계(2020-2021): DeFi 총 예치 자산(TVL)과 해킹 손실이 동시에 증가했습니다.
- 2단계(2022-2023): 두 지표 모두 함께 하락했습니다.
- 3단계(2024-2025): TVL은 회복세를 보였고 해킹 손실은 억제된 상태를 유지했습니다.



처음 두 단계는 직관적인 패턴을 따릅니다. 위험에 처한 가치가 클수록 훔칠 수 있는 가치도 커지고, 범죄자들은 고가치 프로토콜을 표적으로 삼아 더 많은 노력을 기울입니다. 악명 높은 은행 강도 윌리 서튼이 말했다고 전해지는 것처럼, "돈이 있는 곳이니까요."

이러한 점은 3단계가 과거의 전례와 크게 다르다는 것을 더욱 주목할 만하게 만듭니다. DeFi TVL은 2023년 최저치에서 상당히 회복되었지만, 해킹 손실은 그에 미치지 못했습니다. 수십억 달러가 이러한 프로토콜로 다시 유입되었음에도 불구하고 DeFi 해킹 발생률이 낮은 수준을 유지하고 있다는 것은 의미 있는 변화를 나타냅니다.

이러한 차이를 설명할 수 있는 두 가지 요인은 다음과 같습니다.

- ***보안 강화***: TVL이 증가했음에도 불구하고 해킹 발생률이 지속적으로 낮은 것은 DeFi 프로토콜이 2020-2021년 기간에 비해 더욱 효과적인 보안 조치를 시행하고 있음을 시사합니다.
- ***공격 대상 대체***: 개인 지갑 절도와 중앙 집중식 서비스 침해 사건이 동시에 증가하는 것은 공격자들이 다른 대상을 노리고 있을 가능성을 시사합니다.

사례 연구: 비너스 프로토콜의 보안 대응

2025년 9월에 발생한 비너스 프로토콜(Venus Protocol) 사건은 보안 강화가 실질적인 변화를 가져오는 대표적인 사례입니다. 공격자들이 해킹된 Zoom 클라이언트를 이용해 시스템 접근 권한을 획득하고, 사용자를 속여 1,300만 달러 규모의 계정에 대한 위임 권한을 얻어내려 했을 때, 그 결과는 재앙적이었을 수도 있습니다. 하지만 비너스 프로토콜은 사건 발생 한 달 전에 헥사게이트(Hexagate)의 보안 모니터링 플랫폼을 도입한 상태였습니다.

해당 플랫폼은 공격 발생 18시간 전에 의심스러운 활동을 감지했고, 악성 거래가 발생하자마자 추가 경고를 생성했습니다. 20분 이내에 Venus는 프로토콜을 일시 중단하여 자금 이동을 차단했습니다.

- **7시간 이내:** 공격자의 자금 동결 완료
- **12시간 이내:** 도난 자금 전액 복구 및 서비스 재개

가장 주목할 만한 점은 비너스가 공격자가 여전히 보유하고 있는 3백만 달러 상당의 자산을 동결하는 지배구조 제안을 통과시켰다는 것입니다. 공격자는 이익을 얻지 못했을 뿐만 아니라 오히려 손실을 입었습니다.

이번 사건은 DeFi 보안 인프라의 실질적인 개선을 보여줍니다. 사전 예방적 모니터링, 신속한 대응 능력, 그리고 결정적인 조치를 취할 수 있는 거버넌스 메커니즘의 결합으로 생태계는 더욱 민첩하고 탄력적으로 변모했습니다. 공격은 여전히 발생하지만, 이를 탐지하고 대응하며 심지어 복구까지 할 수 있게 된 것은 해킹 성공 시 영구적인 손실로 이어지던 초기 DeFi 시대와는 근본적으로 다른 변화입니다.

2026년 이후의 영향

2025년 데이터는 북한의 암호화폐 위협 행위자로서의 진화에 대한 복잡한 양상을 보여줍니다. 공격 횟수는 줄었지만 훨씬 더 큰 피해를 입히는 공격 방식을 구사하는 북한의 능력은 점점 더 정교해지고 인내심을 갖게 되었음을 시사합니다. 바이비트 사건이 연간 활동 패턴에 미친 영향은 북한이 대규모 해킹에 성공하면 공격 속도를 늦추고 해킹 수익금 세탁에 집중한다는 것을 보여줍니다.

암호화폐 업계에 있어 이러한 변화는 고가치 자금 세탁 대상에 대한 경계를 강화하고 북한 특유의 자금 세탁 패턴을 더욱 정확하게 탐지해야 할 필요성을 제기합니다. 북한이 특정 서비스 유형과 송금액을 일관되게 선호하는 행태는 탐지 기회를 제공하고, 다른 범죄자들과의 구별을 가능하게 하며, 수사관들이 온체인에서 그들의 행적을 파악하는 데 도움을 줄 수 있습니다.

북한이 국가 정책 자금 조달과 국제 제재 회피를 위해 암호화폐 탈취를 지속하는 가운데, 업계는 북한의 공격 방식이 일반적인 사이버 범죄자와는 다르다는 점을 인식해야 합니다. 북한의 2025년 공격 건수는 전년 대비 74% 감소하는 기록적인 수치를 달성했는데, 이는 우리가 북한 활동의 극히 일부만을 목격하고 있을 가능성을 시사합니다. 2026년의 과제는 북한과 연계된 공격자들이 바이비트(Bybit) 사태와 같은 대규모 공격을 다시 일으키기 전에 이러한 영향력이 큰 공격을 탐지하고 예방하는 것입니다.

Chainalysis

본 자료는 정보 제공 목적으로만 제공되며, 법률, 세무, 재정 또는 투자 자문으로 간주될 수 없습니다. 수신자는 이러한 유형의 결정을 내리기 전에 반드시 전문가와 상담해야 합니다. Chainalysis는 수신자가 본 자료를 활용하여 내린 결정이나 기타 행위 또는 부작위에 대해 어떠한 책임도 지지 않습니다.

Chainalysis는 본 보고서에 포함된 정보의 정확성, 완전성, 시의성, 적합성 또는 유효성을 보장하거나 보증하지 않으며, 해당 자료의 오류, 누락 또는 기타 부정확성으로 인해 발생하는 어떠한 청구에 대해서도 책임을 지지 않습니다.

바이빗 | 암호화폐 범죄 보고서 | 암호화폐 도난 | 디파이 | 북한 | 해킹 | 북한 | 도난당한 자금