암호화폐와 사이버 보안: **Bybit** 해킹을 중심으로

송영준

본 글은 2025년 바이비트 (Bybit) 거래소에서 발생한 대규모 암호화폐 탈취 사건을 중심으로, 암호화폐 및 블록체인 생태계에서의 보안 위협과 대응 방안을 논의한다. 블록체인 장부 상에서 관리되는 자산의 규모가 점점 커지고 있고, 탈중앙화와 같은 특성 때문에 이 자산에 대한 탈취 시도가 앞으로 꾸준히 증가할 것으로 예상한다. 국가 · 기업 · 개인 모두가 증가하는 보안 관련 문제를 인식해야 하고, 각 주체별로 취할 수 있는 방법을 기술한다.

지난 2025년 2월 21일, 세계에서 가장 큰 암호화폐 거래소 중 하나인 바이비트 (Bybit) 에서 역대 최대 규모의 암호화폐 탈취 사건이 발생하였다. 탈취 규모는 500,000 ETH로 약 1.5억 달러 (원화 기준 2조 원 이상) 에 달한다. 이는 전 세계적으로 발생한 역사상 단일 금융 탈취 사건 중 가장 많은 양에 해당한다. 해킹의 배후로는 북한이 지목되었는데, 이는 지난 몇 년간 암호화폐 업계에서 굵직한 탈취를 성공시킨 라자루스 그룹이 주로 사용해 온 자금 세탁 방식 및 지갑 주소와 동일한 점이 확인되었기 때문이다.

암호화폐 및 블록체인 분야는 수년간 해커들의 주요 타깃이었다. 2017년 이후 천문학적인 금액이 암호화폐 업계에 몰리면서, 자연스럽게 보안상의 약점을 포착하고 공격하려는 시도가 매우 빈번히 일어났다. 공격 대상은 크게 중앙화 거래소 (CEX) 와 스마트 컨트랙트 (smart contract) 로 구분할 수 있다. 중앙화 거래소는 단일 지갑에 수조 원의 자산을 보관한다는 점이 취약점으로 작용했고, 스마트 컨트랙트는 감사를 완전히 받지 않은 코드를 노려 컨트랙트 계정이 보유한 자산을 탈취하는 경우가 대부분이다. 특히 스마트 컨트랙트는 이더스캔 (etherscan.io) 과 같은 블록체인 익스플로러 서비스를 통해 바이트코드 (bytecode) 를 손쉽게 역번역 (decompile) 할 수 있고, 오픈소스로 운영되는 경우도 자주 있기 때문에 해커들이 집중적으로 공략해 왔다.

이번 바이비트 해킹 사건을 더 자세히 살펴보면, 해커들은 악성코드나 피싱 (phising) 을 통해 거래소 내부 권한 (핫월렛 (Hot-wallet), 다중서명 지갑 (Multi-sig wallet) 등)을 장악한 뒤, 짧은 시간 안에 자금을 여러 지갑으로 분산시키고 탈중앙화 거래소 (DEX) 와 브릿지 (Bridge: 서로 다른 블록체인 간 자산 이동 서비스) 등을 활용해 추적을 우회했다는 점이 특히 주목된다. 또한 트랜잭션 (transaction) 승인 절차 자체가 조작되었거나, 관리 콘솔 (API 키, 내부자 계정 등)에 침투해 송금 요청을 정상 승인으로 위장했다는 분석도 있다. 거래소 측에서는 신속하게 해킹 지갑 주소를 추적하고 일부 자산을 동결하려 했지만, 이미 상당량의 이더리움이 다른 체인이나 믹서 (Mixer: 자금 세탁 서비스) 로 옮겨져 추적이 어려워졌다. 결국 이번 사건을 통해 다중서명 지갑이나 콜드월렛 (Cold-wallet) 역시 완벽하게 안전하지 않다는 사실이 다시금 부각되었으며, 자금 세탁 과정에서 DEX와 브릿지를 총동원해 국가 간 규제 차이를 악용할 수 있다는 점 또한 확인되었다.

개인이 직접 비수탁 (non-custody) 지갑 을 통해 자산을 관리하다 해킹의 대상이 되는 사례도 많다. 대표적인 예로, 위조된 사이트에서 안전하지 않은 트랜잭션 요청에 서명한다거나, 지갑 복구 문구를 부주의하게 관리해 이 문구 자체가 노출됨으로써 문구가 연결된 계정들의 자산을 순식간에 탈취당하는 경우가 있다.

블록체인 분야에서 사이버 보안 이슈는 앞으로 더욱 중요해질 수밖에 없다고 본다. 첫째, 이미 상당한 자산이 블록체인 위에서 교환되고 있으며, 각국 규제 상황에 따라 실물 자산이 토큰화되어 거래될 전망이다. 예를 들어, 온도 파이낸스 (Ondo Finance) 는 미국 국채를 이더리움 상에서 토큰으로 발행하여 유동화를 시킨 바 있다. 이 밖에도 부동산, 예술품, 사모펀드 등의 자산을 토큰화하고자 하는 기업과 서비스가 다양하게 등장하고 있다. 더 많은 자산이 디지털화될수록 탈취 위험도 커질 것이다.

또한 블록체인은 탈중앙화라는 특성상 검열이 어렵고, 가용성 (Availability) 이 매우 높은 시스템이다. 이는 사용자 입장에서는 장점일 수 있으나, 보안적 관점에서 보았을 때는 위험 요소로 작용한다. 해킹 집단이 자체적으로 노드 (Node) 를 운영하고, 때마침 그 노드가 블록 생성 권한을

획득한다면, 시스템의 프로토콜 (Protocol) 을 위반하지 않는 선에서 악의적인 트랜잭션을 블록에 포함할 수도 있기 때문이다.

그렇다면 다가오는 위협에 우리는 어떻게 대비할 수 있을까. 먼저, 국가 차원에서의 대응이 필요하다. 각국 정부는 암호화폐 산업을 일정 수준 규제 범위에 두어야 한다. 해킹 사건 발생 시 해커 지갑 주소를 신속히 판별 · 추적하고, 법정화폐를 취급하는 거래소에 해당 지갑 주소를 동결하도록 요청하는 등 국내외 공조가 필수적이다. 또한 기업은 블록체인 서비스를 도입하기 전, 자금 탈취 위험이 있음을 인지하고 스마트 컨트랙트 작성 시 철저한 감사를 받아야 한다. 현재는 주로 보안 업체에 원본 코드 (source code) 를 전달해 보안 전문가들이 직접 검토하는 형태지만, 사람의 실수를 줄이기 위해 스마트 컨트랙트 언어 분석 도구를 개발 · 활용하고, 보안 전문가에 대한 지속적인 교육을 실시하는 등의 노력이 필요하다.

개인 또한 자신의 지갑을 관리할 때 언제든 자금이 탈취될 수 있다는 경각심을 가져야 한다. 이용하려는 서비스 도메인을 반드시 재확인하고, 지갑을 선택할 때 위험 사이트에 대해 한 번 더 확인을 요구하는 기능이 있는지 살펴봐야 한다. 복구 문구는 잘 보관하면 언제 어디서든 자산에 대한 관리 권한을 얻을 수 있다는 큰 장점이 있지만, 동시에 해커들의 주요 타깃이 되기도 하므로 평문 형태로 온라인에 저장하는 일은 절대 삼가야 한다. 대부분의 일반 사용자는 보안 인식이 높지 않으므로, 이들을 위한 기초 보안 교육 프로그램을 제공하는 것도 효과적인 방법이 될 것이다.

바이비트 사건은 암호화폐와 보안에 대한 중요한 경종을 다시금 울려주는 사례다. 피해 규모가 매우 크고 탈취 수법 또한 치밀하여, 현재까지도 구체적인 분석이 진행 중이다. 이 글에서 다루지 못한 개인 지갑 대상 범죄 역시 지금 이 순간에도 꾸준히 일어나고 있다. 앞으로 더 많은 자산이 블록체인 장부에서 관리될 것으로 예상되는 만큼, 이에 따른 보안 위험을 철저히 예방할 노력이 절실하다. 기관 · 기업은 더욱 거시적인 예방책과 해결책을 제시해야 하며, 서비스를 자유롭게 이용하는 개인도 위험성을 인식하고 기초적인 보안 지식을 차근차근 쌓아야 한다.