가상자산 탈취 예방을 위한 Chainabuse 기반 사기 주소 수집 프레임워크 제안

유민정[1], 정윤영[1], 박승현[1], 신미진[1], 김성민[2]
[1]성신여자대학교 융합보안공학과 학부생
[2]성신여자대학교 융합보안공학과 교수
20211079@sungshin.ac.kr, 20211097@sungshin.ac.kr, 20211058@sungshin.ac.kr,
20211073@sungshin.ac.kr, sm.kim@sungshin.ac.kr

Proposed Chainabuse-based Fraudulent Address Collection Framework to Prevent Virtual Asset Scam

Minjung Yoo[1], Yunyoung Jung[1], Seunghyun Park[1], Mijin Shin[1], Seongmin Kim[2]
[1, 2]Dept. of Convergence Security Engineering, Sungshin Women's University

요 약

가상자산은 온라인상에서의 투명성과 익명성을 통해 금융서비스 및 전자상거래 발전의 핵심으로 주목받아왔으나, 다크웹에서 사기(Scam) 및 랜섬웨어 등을 통한 자산 탈취의 대상이 되고 있다. 공격자는 익명성을 높이는 자금세탁 기법을 활용하여 탈취한 가상자산의 추적을 우회하며, 이로 인해 피해자에게 정상적인 피해보상이 어려운 실정이다. 본 연구에서는 가상자산 사기 주소에 대한 탈취를 목적으로 한 공격자의 사기 유형을 파악하고, 피해를 최소화하기 위해 대표적인 가상자산 피해 신고 사이트 Chainabuse의 사기 주소에 대한 Top Scammer 주소 수집 및 사기 동향 분석이 가능한 시스템을 제안한다.

1. 서론

가상자산은 온라인상에서 투명성과 익명성이 보장되므로 금융서비스 및 전자상거래 발전의 핵심으로 주목받아왔다. 그러나 블록체인 시스템상의 익명성 보장으로 인해 다크웹에서 불법 거래, 사기(Scam) 및 랜섬웨어 등에서 악용되고, 자산 탈취의 대상이 되고 있다[1]. 탈취된 가상자산은 공격자가 익명성을 강화하는 자금세탁 기법을 통해 추적을 우회하고, 대리인을 고용하여 현금화함으로써 신원 추적 및 피해보상도 어려운 실정이다. 이러한 문제점을 최소화하기 위해 머신러닝 기반 가상자산 자금세탁 경로 추적, 동일 주소 클러스터링 기법이 연구되어왔으나, 급변하는 사기 동향에 따른 사기 유형 체계화 및 동향 분석에 관한 연구는 미비하다[2]. 본 연구에서는 가상자산 탈취를 목적으로 한 공격자의 사기 및 랜섬웨어 유형을 파악하고, 피해를 최소화하기 위해서 대표적인 가상자산 피해 신고 사이트 Chainabuse[3]의 사기 주소에 대한 Top Scammer 주소 수집 및 사기 동향 분석이 가능한 시스템을 제안하고자 한다.

2. 관련 연구

현재까지의 가상자산 범죄에 관한 연구는 익명성을 보장하기 위한 토큰 혼합기법 및 도난자금 분산 기법과 같은 경험적 분석을 사용하고, 머신러닝 기반의 자금세탁 범죄율 탐지와 같은 불법 자금 추적의 정확도 향상에 주력하고 있다[2]. Yanan Gong 외 3인에 의하면[2] 불법 비트코인 주소를 수집하여 동일 주소 클러스터링 기법을 제안하고, 자금세탁을 시도하는 패턴을 식별하였다. 그러나 대부분의 연구는 가상자산 사고 원인 및 유형과 관계없이 범죄 그룹 추정 및 자금세탁 분석에 중점을 두고 있다. 따라서 탈취 동향의 변화와 거래 대상의 안전성 점검에 관한 연구는 아직 미흡하다.

3. 배경

3.1 Chainabuse

Chainabuse는 가상자산 탈취 피해 신고 사이트로, 블록체인 네트워크마다 카테고리화 하여 사기로 접수된 주소 및 사이트에 대한 코멘트를 제공한다. 그러나 보고되는 주소의 누적 신고 횟수를 알 수 없어

어떤 주소가 범죄 심각성이 높은지 알 수 없다.

3.2 가상자산 사기 유형

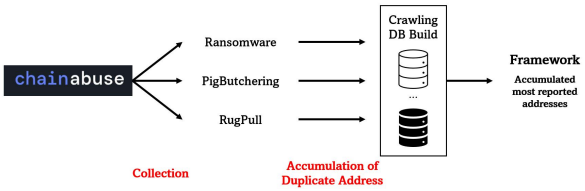
2023년에 발생한 가상자산 사기 피해액은 약 40억 달러로[1], 가상자산 불법 거래 중 두 번째로 큰 규모이다. 가상자산 사기는 직접적인 피해가 발생하기 전까지 피해자가 인지하기 어려우므로 사전 예방이 중요하다. 대표적인 사기 유형으로는 PigButchering, Rugpull, Ransomware 사기가 존재한다.

PigButchering은 피해자에게 의도적으로 접근하여 신뢰를 쌓은 뒤, 합법적이고 수익성이 있는 것처럼 보이는 사업에 투자하도록 유인하는 사기이다[1]. 최근 SNS를 통해 접근하여 투자를 유도하는 사례가 증가하고 있어 피해가 더욱 커질 것으로 예상된다.

Rugpull은 암호화폐나 NFT 개발자가 투자자들로부터 자금을 유치하기 위해 프로젝트를 홍보한 뒤, 투자금을 가지고 잠적하는 사기이다[1]. 프로젝트의 스마트 컨트랙트에 악성 백도어를 만들어 투자자의 토큰을 훔치는 'Hard Rug pull'과 과장된 마케팅으로 프로젝트의 가치를 부풀려 토큰을 가로채는 'Soft Rug pull'로 구분된다.

Ransomware는 컴퓨터 시스템을 암호화한 것처럼 가장하고 이를 해제하기 위해 금전을 요구하는 사기이다[1]. 피싱 이메일을 통해 불법 사이트 접속 및 피해자의 입금을 유도한다.

4. Chainabuse 기반의 가상자산 불법 사기 주소 누적 수집 프레임워크 제안



(그림 1) 가상자산 사기 주소 누적 수집 프레임워크

가상자산을 대상으로 하는 사기는 단기간에 큰 금액을 수입한 후 빠르게 인출하기 위해 동일한 지갑 주소를 여러 번 사용한다. 거래하고자 하는 주소가 공식적인 수사가 완료되기 전까지 계속해서 피해를 초래할 수 있으므로, 사용하는 주소의 신고 횟수 및 탈취 금액 규모를 조사한 후에 거래를 체결해야 한다. 가상자산 불법 주소 신고의 대표 사이트인 Chainabuse에서는 피해자들의 신고를 기록하고 피해 유형을 공유하지만, 이러한 정보를 단순 보고 형태로만 제공하여 실제 피해의 심각성을 파악하기 어렵다. 따라서 Chainabuse에 보고된 불법 사기 주소의 누적을 통해 거래하고자 하는 주소가 어느 정도 자금 탈취 사기와 연관되어 있는지 파악할 수 있는 가상자산 불법 사기 주소 누적 수집 프레임워크를 제안한다.

(그림 1)에서 제안하는 프레임워크는 Chainabuse에서 신고 횟수가 가장 많은 세 가지 사기 유형(Ransomware, PigButchering, RugPull)을 대상으로 하였으며, 분석하고자 하는 사기 유형에 따라 수집 대상을 변경할 수 있다. 수집과정에서는 중복으로 보고된 지갑의 신고 횟수 누적 및 피해 금액을 데이터베이스 상에 누적하고, 프레임워크의 프론트엔드 상에 나타냄으로써 현재 수사 협조가 가장 시급한 주소를 파악할 수 있다. 이를 통해 거래 대상의 위험성을 사전에 파악하여 PigButchering, RugPull 사기를 일으키는 잠재적인 피해자의 투자를 방지하고, 랜섬웨어 감염 여부를 재확인하도록 경고할 수 있다. 따라서 급변하는 사기 동향을 분석 및 체계화할 수 있으며, 사후 동결이 시급한 주소를 빠르게 파악함으로써 자금 수사에도 도움을 줄 수 있다.

5. 결론

가상자산 피해 금액이 급격히 증가함에 따라 피해 자금 추적 및 보안성 강화에 관한 연구가 이루어지고 있으나, 급변하는 사기 동향에 따라 사기 유형 체계화 및 동향 분석에 관한 연구는 부족하다. 따라서 본 연구에서는 사기 유형 거래 횟수 누적에 따라 동향을 파악할 수 있고, 거래하고자 하는 주소의 신고 횟수 및 피해 금액 누적을 확인할 수 있는 수집 프레임워크를 제안한다. 본 프레임워크를 통해 발전하는 자금 탈취 동향 파악이 가능하고, 사전 예방 및 신속한 지갑 동결에 도움이 되기를 기대한다.

참고문헌

[1] Chainalysis team, "The 2024 Crypto Crime Report", Chainalysis, Jan.2024

[2] Yanan Gong et al, "Analyzing the peeling chain patterns on the Bitcoin blockchain", DFRWS 2023 APAC, Singapore, Oct.2023

[3] Chainabuse team, "Report malicious crypto activity" [Online.]. Available: https://www.chainabuse.com/