https://doi.org/10.33778/kcsa.2024.24.3.023

공개출처정보(OSINT)를 활용한 가상화폐 범죄 추적 분석 기법: 방법(Methods) 및 프레임워크(Framework)의 통합 적용

서 병 완*, 김 원 웅**

요 약

가상화폐는 익명성과 탈중앙화 특성으로 인해 범죄에 악용될 가능성이 높으며, 이에 따라 효과적인 추적 기법의 개발이 요구된다. 공개출처정보는 공공 데이터, 소셜 미디어, 온라인 포럼 등 다양한 오픈 소스 데이터를 분석하여 범죄자의 신원 파악과 가상화폐 자금 흐름 추적에 유용한 정보를 제공할 수 있다. 본 논문에서는 공개출처정보의 활용 방안을 종합적으로 제시하고자 한다. 이를 위해 우선 가상화폐의 현황과 추세 및 관련 범죄 현황에 대해 살펴보고, 공개출처정보의 개념 및 방법에 대해 알아본다. 이후 가상화폐 관련 범죄의 추적 및 분석을 위한 공개출처정보의 5가지 방법과 7가지 프레임워크를 중점 분석하고, 공개출처정보 방법과 프레임워크를 적용하는 통합 기법을 제시한다.

Investigation of Cryptocurrency Crimes Using Open Source Intelligence (OSINT): focused on Integrated Techniques with Methods and Framework

Byung Wan Suh*, Won-Woong Kim**

ABSTRACT

The anonymity and decentralized nature of cryptocurrencies make them highly susceptible to criminal exploitation, requiring the development of effective tracking techniques. By analyzing various open source intelligence(OSINT), such as public data, social media, and online forums, open source intelligence can provide useful information for identifying criminals and tracking the flow of cryptocurrency funds. In this study, we present a comprehensive proposal for the utilization of open source intelligence. We will discuss the current status and trends of cryptocurrency and related crimes, and introduce the concept and methodology of open source intelligence. The paper then focuses on five methods and seven frameworks of open source intelligence for tracking and analyzing cryptocurrency-related crimes, and presents techniques for the integrated application of open source intelligence methods and frameworks.

Key words : Cryptocurrency, Cybersecurity, Blockchain, Digital Crime, OSINT

접수일(2024년 08월 16일), 수정일(1차: 2024년 09월 10일), 게재확정일(2024년 09월 19일)

* 산업정책연구원/연구교수(주저자)
** (주)페어스퀘어랩/기업부설연구소(공동저자)

1. 서 론

가상화폐(Cryptocurrency)가 금융 및 제도권에 진입하고 있지만 이를 이용한 범죄 행각은 끊이지 않고 있다. 가상화폐를 이용한 범죄는 시간 및 공간의 제약을 받지 않는다는 점에서 전 세계를 대상으로 하는 사이버 범죄이며, 국내에서도 관련 범죄는 이미 사회 문제로 등장한지 오래다. 특히, 사기, 자금세탁, 해킹 등 가상화폐를 수단으로 삼은 범죄들도 더욱 고도화되며 피해 규모는 갈수록 증가하고 있다.

2024년 7월 가상화폐 범죄 전문기업인 ㈜클로인트가 발간한 '가상화폐 해킹 사건에 대한 북한중심의 조사분석리포트'에 따르면, 전세계에서 가상화폐에 대한 범죄는 2022년부터 2024년 6월까지 약 30개월에 걸쳐 944건이 발생하였으며, 이는 하루에 한 번 꼴로 가상화폐 범죄가 발생하고 있다는 것이다[1]. 뿐만 아니라 가상화폐 범죄 규모도 커져가고 있는데, 2024년 1~6월 사이에 100만 달러 이상의 가상화폐 해킹범죄는 총 59건으로, 매월 100백만 달러 이상 규모의 가상화폐 범죄는 최소 5회 이상 일어나고 있다[2].

가상화폐의 거래 정보는 블록(Block)과 체인(Chain)의 형태로 존재한다. 블록체인(Blockchain)의 특성인 탈중앙화(Decentralization)와 익명성(Anonymity)을 고려할 때, 기존의 수사 기법으로는 불법 활동을 밝혀내기에는 현실적 및 기술적 어려움이 존재한다. 이런 측면에서 공개출처정보(OSINT, Open Source INTelligence)를 활용한 다각도의 범죄 수사 접근 방식은 블록체인 기반의 가상화폐 연구에서 필수 요소로 사용되어야 한다.

특히 가상화폐 범죄를 수사하는 수사관들은 OSINT 기술을 통해 공개적으로 접근 가능한 출처에서 정보를 얻고 범죄자 측면에서도 학습하여 사이버 범죄자를 식별하고 사기 활동을 추적할 필요가 있다. 즉, OSINT 기술을 활용하여 가상화폐 사용자들이 주로 사용하는 소셜 미디어 사이트, 온라인 그룹, 공개 포럼 등에서 정보를 얻을 수 있으며, 이를 통해 여러 주소에서 발생한 자금 이동을 추적하고 의심스러운 활동 패턴을 발견하여 가상화폐와 관련된 위험을 줄일 수 있을 것이다.

이러한 관점에서 본 논문에서는 소외되어 있는 가상화폐 범죄의 추적 및 분석 분야의 OSINT 활용 방법론 연구를 제시하기 위하여, 가상화폐와 OSINT의 정의 및 분류에 대해 알아보고 OSINT의 다섯 가지 방법과 프레임워크를 활용한 가상화폐 범죄 추적 분석의 적용 분야와 기법에 대해 상세히 분석한다.

2. 연구 배경 및 선행 연구

2.1 가상화폐

가상화폐(Cryptocurrency)는 블록체인 기반 분산 원장에 거래 내역이 기록되는 디지털 자산(Digital Asset)을 의미하며, 그 쓰임에 따라 가상자산 또는 암호화폐 등으로 불린다. 해외에서도 가상화폐에 대한 용어 및 정의가 일률적으로 사용되지 않으며, 가상화폐에 대한 국가별 또는 기관별 사용하는 용어 및 그 정의가 상이한 측면이 있다. 또한 비트코인과 같은 가상화폐의 경제적 가치는 인정하면서 공식 화폐로써의 법적 지위는 보장하지 않고 있다. 특히 암호화 기술을 적용한 가상화폐의 종류는 다양하지만 실제로 통용되는 대부분의 가상화폐는 해시함수(Hash Function)와 블록체인 등의 기술을 사용하며, 기존의 중앙관리 체계에 의한 거래 방식이 아닌 각 개인들이 거래 정보를 블록체인 구조로 공유함으로 상호 인증이 가능한 형태이다[3].

2.1.1 가상화폐 현황 및 추세

2024년 8월 14일 기준으로 전 세계 가상화폐는 10,000여 종이 넘는 것으로 추정된다. CoinMarket Cap에 따르면 전 세계 가상화폐 시장의 규모는 약 2.1 Trillion USD(한화 약 2,856조 원) 이며, 이 중 시가총액 1위는 Bitcoin (BTC), 2위는 Ethereum (ETH), 3위는 Tether USD(USDT)로 가상화폐 전체 시장 규모의 76.65%를 차지하고 있다[4].

(그림 1)은 가상화폐 시장에서 거래되는 1만여 가지의 가상화폐 중 다빈도의 거래는 빨간색, 그렇지 않은 것은 녹색 등으로 표기하고, 거래 금액의 크기에 비례하여 직사각형의 크기를 조절하여 보여주고 있는 열지도(Heat Map)이다. 특히, 2017년 최초 등장한 Bitcoin과 Ethereum 두 종류의 가상화폐 점유율은

전체의 71.22%를 차지하고 있어, 가상화폐 범죄 측면에서도 두 종류의 가상화폐에 집중되고 있다.

(그림 1) 가상화폐의 종류 및 열지도(Heat Map)

반면 2020년 7월 전 세계 가상화폐는 1,000여 종이었고 0.272 Trillion USD 규모였으나, 현재 약 4년 만에 그 종류는 10배 이상 증가하였고, 규모는 7.6배 이상 증가하였다[5]. 이렇듯 가상화폐의 종류와 규모는 해를 더해감에 따라 빠르게 증가하고 있다.

2.1.2 가상화폐 범죄

가상화폐 시장의 성장과 함께 가상화폐 범죄도 빠르게 증가하고 있고, 관련 범죄는 다양한 형태로 나타난다. 또한 가상화폐 범죄에는 사기, 해킹, 자금세탁(Money Laundry) 등이 포함된다.

사기는 가장 흔한 형태의 가상화폐 범죄 중 하나이며, 가짜 투자 기회를 제공하거나 실체가 없는 가상화폐를 판매하는 등의 방법으로 투자자들을 속이는 것이다. 해킹은 거래소 또는 개인의 가상화폐 저장소의 보안을 뚫고 가상화폐를 훔쳐 가는 것이다. 자금세탁은 가상화폐의 익명성을 악용한 범죄로, 불법적으로 취득한 자금을 가상화폐를 이용하여 세탁하는 행위이다. 이러한 범죄를 방지하기 위해 각국의 정부나 기관을 가상화폐 거래소 대상으로 일정한 자금세탁 방지 규정을 정하여 적용하고 있다. 더불어, 가상화폐를 수단으로 하는 주요 범죄 형태로는, 마약 거래 및 도박, 탈세 및 편법 증여, 불법 외환거래 등이 있다.

2022년 경찰청이 국회에 제출한 자료에 살펴보면, 2017년부터 2021년까지 최근 5년간 가상화폐 불법행위 검거 건수는 총 774건, 검거 인원은 총 1천976명이었으며, 연도별 피해액은 2017년 4천674억원, 2018년 1천693억원, 2019년 7천638억원, 2020년 2천136억원에서 2021년에는 3조1천282억원으로 급증했다. 이는 2020년과 비교하면 피해 규모가 15배가량 폭증한 셈이다. 또한 검거 인원은 2017년 126명, 2018년 139명, 2019년 289명, 2020년 560명에서 2021년에는 862명으로 전년 대비 53.9% 늘었다. 검거 건수는 2017년 41건, 2018년 62건, 2019년 103건, 2020년 333건, 2021년 235건으로 집계됐다. 2021년에는 약 2조2천400억원 규모의 피해를 낸 브이글로벌 사건으로 인해 피해액이 대폭 증가하였다[6].

가상화폐에 대한 범죄는 국내에서만 발생하지 않고 해당 국가를 넘어 국제 범죄로 이어지는 경우가 다수이다. 가상화폐에 대한 해킹 범죄는 2022년부터 2024년 6월까지 약 30개월 동안 944건의 사고가 있었으며, 이 중 100 Million USD (한화 약 13억원) 이상인 사건만 244건이며, 이는 하루에 한 번꼴로 가상화폐 범죄가 발생하고 있다고 볼 수 있다[1].

그뿐만 아니라, '북한 사이버 공격 전략의 진화: 대북 제재 회피를 위한 외화벌이 수단으로서 사이버 전략'에 따르면 북한의 사이버 공격 사례가 지속해서 이루어짐을 확인할 수 있다. 2017년 7월 국내 가상화폐 거래소인 빗썸(Bithumb)을 대상으로 700만 달러 상당의 가상화폐 탈취가 되었으며, 같은 해 12월에는 2차 공격을 포함하여 유빗(Youbit)을 대상으로 약 225억 원 상당의 가상화폐가 탈취되었다. 또한 한미 양국은 북한이 이러한 사이버 공격을 통해 2022년 한 해 동안 약 1조 7천억 원 상당의 가상화폐를 탈취했다고 밝혔으며, 북한의 사이버 공격의 경우 2014년 12월 소니픽처스 해킹과 같은 보복성 해킹이 아닌 외화벌이의 수단으로서 기능하고 있다는 사실을 파악할 수 있다[7].

2.2 공개출처정보 (OSINT)

공개 출처 정보(OSINT)란 것은 쉽게 접근할 수 있는 공개된 정보를 수집, 분석하여 유용한 정보를 도출하는 방법을 의미한다. OSINT는 군사, 정보기관, 법 집행 기관뿐만 아니라 민간 분야에서도 활용되며, 특히 보안, 사이버 범죄 추적, 정보, 수집 및 분석 등에 광범위하게 사용된다.

2006년 발표된 미국 국방수권법(National Defense Authorization Act)에 따르면, Open Source Information과 Open Source Intelligence는 엄연히 구분하고 있는데, Open Source Information은 공개적으로 이용 가능한 정보로, 누구나 합법적으로 요청, 구입 또는 관찰을 통해 얻을 수 있는 정보라 정의하고, Open Source Intelligence는 공개적으로 접근 가능한 출처로부터 체계적으로 수집, 분석 및 활용되는 정보로, 공개된 자료를 전략적으로 활용하여 생성된 지식 체계를 의미한다. 또한 OSINT는 해당 정보의 적절한 배포와 전달도 포함하며, 공개된 정보의 가치를 극대화하여 의사결정과 전략 수립에 기여하는 중요한 정보 자산으로 인식되고 있다.

이러한 사이버수사 관련 OSINT의 중요성을 국내 학문적 연구 측면에서 살펴보면, 2016년 이후 DBpia에서 검색된 학술연구 논문은 총 8건밖에는 검색되지 않았으며 이렇듯 OSINT 관련 보안 분야의 연구는 매우 희소하다. 8건의 연구 논문은 주로 OSINT 정보 수집 방법, 유사도 분석 연구, 그리고 데이터베이스 구축 방안에 대한 연구가 주를 이룬다.

<표 1> 국내 OSINT 관련 학술 논문(2016년~)

연구 제목	저자	년도
중국 해킹그룹 샤오치잉 사이버 무기체계 대응 방안 연구	유도진	2023
사이버위협인텔리전스와 공개출처 지능정보에 대한 서지학적 연구	신상민 외 2명	2023
안보 관점에서의 OSINT와 SOCMINT 조사 분석업무의 한계와 극복방안을 위한 요구사항 연구	나가진 외 1명	2021
공개정보 기반 타임라인 프로파일링을 위한 확정된 워크플로우 개발	권희원 외 6명	2021
Automating OSINT as Decision Support System to Address Attribution Problem in Cyber Investigation	A. Onche 외 2명	2021
OSINT기반의 활용 가능한 사이버 위협 인텔리전스 생성을 위한 위협 정보 수집 시스템	김경한 외 3명	2019
실시간 사이버 위협 지능형 분석 및 예측 기술	임창완 외 5명	2019
단어 조합 검색을 이용한 불법 유해 정보 탐지 기법	한병우 외 1명	2016

3. 가상화폐 범죄에서 OSINT 활용분석

가상화폐 범죄의 증가와 범죄 기술의 고도화, 그리고 범죄의 복잡성과 은밀성이 증가함에 따라, 기존의 단편적인 OSINT 활용 방식으로는 효과적인 대응에 한계가 있다. 이에 본 연구에서는 이러한 문제의 해결 방안 중 하나로 OSINT 방식과 프레임워크(Framework)를 활용한 통합 추적 기법을 제안함으로, 가상화폐 범죄 추적 및 분석의 효율성과 정확성을 항상 시킬 수 있는 체계적인 접근 기법을 제시한다.

3.1 OSINT 방법 (Method)

전통적인 OSINT 방법은 오랫동안 사이버 보안 분야에 활용되어 온 것이 사실이다. 수동 웹 검색, 키워드 분석 및 기본적인 데이터 수집 기법이 활용되기도 하였으나, 최근에 사용되는 OSINT 방법은 Red Team Reconnaissance, Google Dorking and Advanced Search Techniques, Digital Footprint Analysis, Geospatial OSINT, Deep Web and Dark Web Analysis의 5가지로 분류할 수 있다[8].

3.1.1 Red Team Reconnaissance

Red Team Reconnaissance는 공격자(Red Team) 관점에서 사이버 공격 시뮬레이션을 수행하여 결과를 보여주고, 실제 환경에서 방어자(Blue Team)를 위한 효과적인 전략을 보여줌으로써 기업의 사이버 보안을 강화하는 방법이다. 이를 가상화폐 범죄 추적에 적용할 경우, 가상화폐 거래소나 지갑 서비스의 취약점을 분석, 잠재적 공격 시나리오를 예측하여 대응 전략을 수립할 수 있다. 또한, 새로운 가상화폐 탈취 기법을 선제적으로 파악하는 데 활용될 수 있다.

3.1.2 Google Dorking and Advanced Search Techniques

Google Dorking and Advanced Search Tech-niques는 Google 검색 엔진을 활용하여 일반적으로 접근할 수 없는 정보를 추출하는 고급 검색 기법이다. 이 기법은 특정 가상화폐 주소와 연관된 정보를 수집하거나 의심스러운 거래소 및 서비스에 대한 심층 정보를 탐색하는 데 효과적이다. 또한, 가상화폐 관련 문서나 포럼 게시물 등을 효율적으로 검색하여 범죄 활

동의 흔적을 찾는 데도 도움을 줄 수 있다.

3.1.3 Digital Footprint Analysis

Digital Footprint Analysis는 온라인상에서 디지털 흔적을 분석하여 개인이나 조직의 활동을 추적하는 방법이다. 이를 통해 가상화폐 공격자의 온라인 활동을 모니터링하고 이에 대해 평가할 수 있다. 가상화폐 범죄 추적에 있어서는 의심스러운 가상화폐 주소 소유자의 온라인 활동을 분석하거나 가상화폐 범죄 조직의 커뮤니케이션 패턴을 파악하는 데 활용될 수 있다. 또한, 소셜 미디어를 통한 가상화폐 사기 홍보 활동을 모니터링하는 데에도 유용하다.

3.1.4 Geospatial OSINT

Geospatial OSINT는 지리적 데이터를 활용하여 위협 인텔리전스(Threat Intelligence)를 강화하는 방법이다. 이 방법은 특정 지역의 가상화폐 범죄 동향을 분석하는 데 적용될 수 있다. 또한, 국가별 가상화폐 규제 및 법 집행 현황을 매핑(Mapping)하여 글로벌 차원의 범죄 추적에 도움을 줄 수 있다.

3.1.5 Deep Web and Dark Web Analysis

Deep Web and Dark Web Analysis는 일반 검색 엔진으로는 접근할 수 없는 웹 영역을 분석하는 기법이다. 검색 엔진을 통해 흔히 접하는 부분은 Surface Web이라고 하며, Deep Web은 검색 엔진에 의해 인덱싱(Indexing)되지 않고 특정 액세스 권한이 필요한 콘텐츠를 포함하는 영역을 의미한다. 개인 데이터베이스 또는 암호로 보호된 페이지 및 학술 자료가 포함된다. Dark Web은 Tor Search와 같은 특정 소프트웨어를 통해서만 접근할 수 있는 Deep Web의 하위 집합을 의미한다. 사용자가 암시장, 포럼 및 불법 서비스와 같은 익명의 빈번한 불법 활동에 참여할 수 있는 플랫폼을 제공한다. 이 방법은 Dark Web 상에서의 불법 가상화폐 거래를 모니터링 하거나 가상화폐를 이용한 자금세탁 네트워크를 분석하는 데 활용될 수 있다. 또한, 새로운 가상화폐 관련 범죄 수법을 조기에 탐지할 수 있다.

<표 2> OSINT 5가지 방법(Methods) 및 특징

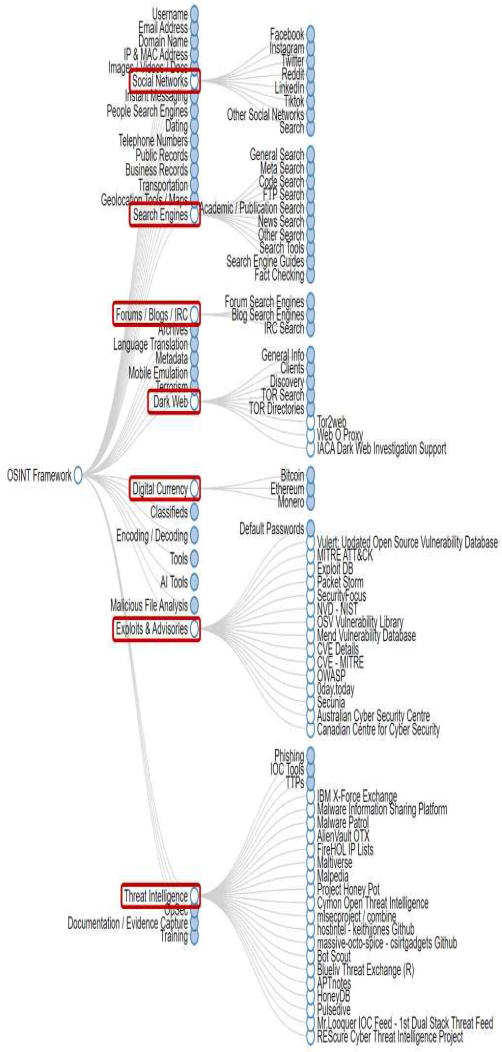
방법	상세 설명
Red Team Reconnaiss-ance	Active Scanning, Collecting Data about the Targeted Host, Collecting Victim Identity Information, Collect Victim Network Information, Collect Target Organization Information, Phishing for Information, Conducting Closed Source Research, Conduct Searches on Publicly Accessible Technical Databases, OSINT on Public Websites, Analysing Target-Owned Websites
Google Dorking and Advanced Search Techniques	Same as Google hacking, using advanced search operators and specific search queries to extract information from the Google search engine
Digital Footprint Analysis	Web Crawling & Scraping, Social Media Intelligence
Geospatial OSINT	Geolocation Data, Mapping & Visualization
Deep Web and Dark Web Analysis	Deep web is not indexed by search engine such as Google and requires certain access permissions. Dark Web is a subset of the deep web that can only be accessed with the use of specialized software, such as Tor.

3.1.6 고려 사항

더불어, <표 2>와 같이 OSINT의 다섯 가지 방식을 활용한 가상화폐 범죄 추적에는 한계와 윤리적 고려 사항이 존재한다. 우선, 개인정보 보호와 합법적 정보 수집 사이의 균형을 유지하는 것이 중요하다. 특히 Dark Web 분석 시에는 법적, 윤리적 문제가 발생할 가능성이 있으므로 신중한 접근이 필요하다. 또한, OSINT를 통해 수집된 정보의 신뢰성과 정확성을 검증하는 과정이 필수적이다. 이를 위해 다양한 출처의 정보를 교차 검증하고 전문가의 검토를 거치는 등의 절차가 요구된다. 마지막으로, OSINT 기술의 오용을 방지하기 위한 명확한 가이드라인을 수립하고 준수하는 것이 중요하다[9].

3.2 OSINT 프레임워크 (Framework)

OSINT 프레임워크는 무료 도구 또는 정보의 원천으로 해당 정보를 수집하는데 중점을 둔 프레임워크이다. 이는 일반인들이 무료 OSINT 리소스를 찾을 수 있도록 돕는 것이 목적이며, OSINT의 프레임워크 총 33개 중 가상화폐 범죄 추적을 위한 항목은 Social Network, Search Engine, Forum/Blog /IRC, Dark Web, Digital Currency, Exploit & Advisory, Threat Intelligence의 7가지가 해당한다 [10].



(그림 2) OSINT 프레임워크(Framework)

3.2.1 Social Network

Social Network는 다양한 정보들이 사용자들에 의해 실시간으로 공유되는 플랫폼으로, 가상화폐 범죄 추적에 있어 중요한 역할을 한다. 이는 탈취된 가상화폐의 소유자가 직접 대중에게 경고를 하기 위한 용도로 사용되기도 하며, 분석가들에 의해 정제된 정보가 공유되기도 한다. 대표적으로 X(구 Twitter), Reddit 그리고 LinkedIn과 같은 주요 Social Network Media를 통해 가상화폐 탈취 사건의 실시간 모니터링, 피해 규모 파악, 범죄 수법 분석 등이 가능하다.

3.2.2 Search Engine

Search Engine은 가상화폐와 관련된 광범위한 정보 수집에 핵심적인 도구이다. 대표적으로 Google과 같은 검색 엔진을 통해 가상화폐 관련 뉴스, 거래소 정보, 규제 동향 등을 효과적으로 수집할 수 있다. 의심스러운 거래나 대규모 자금 이동과 관련된 주소를 추적에 활용된다. 또한 특정 거래나 지갑과 연관된 개인이나 단체의 정보를 수집할 수 있으며, Social Network나 Forum/Blog/IRC와 같은 다른 OSINT 도구로의 연결점 역할을 수행하기도 한다.

3.2.3 Forum/Blog/IRC

Forum/Blog/IRC는 가상화폐 전문가들의 심층적인 시장 분석과 기술적 견해를 얻을 수 있는 정보원이다. Forum은 특히 Bitcoin Talk, Reddit의 cryptocurrency subreddit 등과 같은 대형 포럼에서는 가상화폐 거래, 신기술, 그리고 보안 이슈 등에 대한 광범위한 토론이 이루어지며, 이러한 Forum을 모니터링 하여 새로운 사기 수법이나 해킹 기술에 대한 정보를 조기에 파악할 수 있다. 또한, 피해자들의 게시물을 통해 실제 범죄 사례와 수법을 분석할 수 있으며, 때로는 범죄자들의 실수로 인한 정보 유출을 포착할 수도 있다. Blog는 가상화폐 전문가, 보안 연구자, 그리고 업계 종사자들이 심층적인 분석과 견해를 공유하는 공간이며, Medium, Steemit 등의 플랫폼에서 발행되는 블로그들은 최신 가상화폐 범죄 동향, 취약점 분석, 그리고 예방 기법 등에 대한 상세한 정보를

제공한다. 특히 보안 전문가들의 블로그는 새로운 해킹 기법이나 악성코드에 대한 기술적 분석을 제공하여 범죄 수법의 진화를 추적하는 데 도움을 준다. 또한, 일반 사용자들의 블로그를 통해 소규모 사기나 피싱 시도 등 일상적인 범죄 사례를 수집할 수 있다. IRC는 실시간 커뮤니케이션 도구로, 익명성을 선호하는 사용자들이 모이는 장소가 되어 불법적인 활동에 대한 논의가 이루어지기도 한다. 보안 연구자들은 이러한 IRC 채널을 모니터링하여 새로운 범죄 계획이나 기법에 대한 정보를 수집할 수 있다. 특히 Dark Web이 관련된 IRC 네트워크는 더욱 은밀한 범죄 활동의 온상이 될 수 있어 주의 깊은 관찰이 필요하다.

3.2.4 Dark Web

Dark Web은 익명성과 암호화된 통신을 제공하는 특성으로 인해 디지털 범죄가 발생하기에 최적의 환경을 제공하는 공간으로, 가상화폐를 이용한 다양한 불법 활동의 온상이 되고 있다. Dark Web에서의 OSINT 활용은 익명성과 접근의 어려움으로 인해 일반적인 웹에서의 활용과는 다른 접근 방식과 도구가 필요하며, 일반 검색 엔진과는 다른 Tor Search와 같은 특수한 검색 엔진들이 존재한다. 또는 Reddit Deep Web, Reddit Darknet과 같은 Forum 틀을 통해 지속적으로 모니터링하여 Dark Web에 대한 포괄적인 정보를 수집하고 분석할 수 있다. 이를 통해 불법 거래 모니터링, 새로운 범죄 수법 파악, 가상화폐 세탁 경로 추적 등이 가능하다.

3.2.5 Digital Currency

Digital Currency는 가상화폐 추적에 있어 가장 직접적이고 핵심적인 프레임워크 중 하나이다. Bitcoin이나 Etherum 또는 알트코인 등 가상화폐별로 존재하는 Block Explorer를 활용하여 블록체인상의 트랜잭션을 분석할 수 있다.

이를 통해 가상화폐의 흐름을 지갑 주소와 해당 거래에 따라 추적할 수 있고, 범죄와 연관된 주소를 식별하며, 자금세탁 패턴을 파악하는 등 다양한 분석이 가능하다.

3.2.6 Exploit & Advisory

Exploit & Advisory는 가상화폐 관련 보안 취약점과 공격 기법에 대한 정보를 제공한다. Phishing이나 Malware를 이용한 개인 키(Key)나 패스워드 탈취 등의 수법을 분석할 수 있다. 이러한 정보는 가상화폐 범죄의 예방과 대응 전략 수립에 중요한 역할을 한다.

3.2.7 Threat Intelligence

Threat Intelligence는 조직을 대상으로 하는 사이버 보안 위협을 예방하고 이에 대응하기 위한 상세하고 실행 가능한 위협 정보를 제공한다. PhishTank, Malpedia와 같은 OSINT를 활용하여 가상화폐 관련 사이버 공격을 조기에 탐지하고 대응할 수 있다. 이는 Phishing, Malware 등 다양한 형태의 가상화폐 범죄를 예방하는 데 중요한 역할을 한다.

이러한 7가지 OSINT Framework는 각각의 특성과 장점이 있으며, 이들을 종합적으로 활용하여 가상화폐 범죄 추적의 효과성을 크게 높일 수 있다.

3.3 OSINT 방법과 프레임워크의 통합 기법

Red Team Reconnaissance는 공격자의 관점에서 시스템의 취약점을 탐색하는 방법으로, Exploit & Advisory, Threat Intelligence, Dark Web 프레임워크와 밀접하게 연관된다. Exploit & Advisory 프레임워크를 통해 가상화폐 거래소나 지갑의 알려진 취약점을 파악하고, 이를 Red Team 시뮬레이션에 활용할 수 있다. Threat Intelligence 프레임워크는 최신 사이버 동향과 공격 기법에 대한 정보를 제공하여 Red Team의 공격 시나리오를 현실적으로 구성하는데 기여한다. 또한, Dark Web 프레임워크를 활용하여 실제 사이버 범죄자들이 사용하는 최신 기법과 도구를 파악하고, 이를 Red Team 활동에 반영함으로써 보안 체계의 실효성을 높일 수 있다.

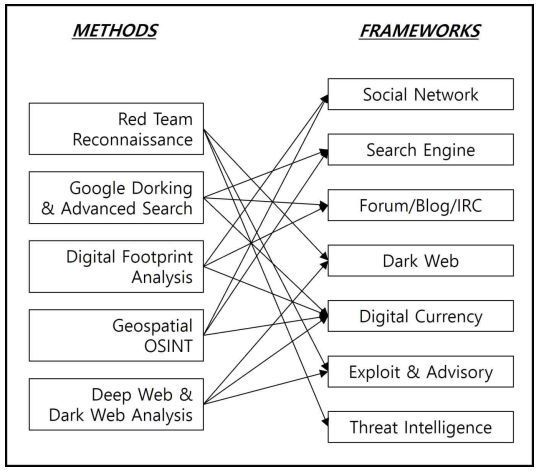
Google Dorking과 Advanced Search Techniques 방식은 Search Engine, Forum/Blog/IRC, Digital Currency 프레임워크와 연계하여 활용될 수 있다. 이러한 방식을 통해 특정 가상화폐 주소나 거래와 관련된 숨겨진 정보를 효과적으로 탐색할 수 있다. 예를

들어 Bitcoin 주소와 연관된 웹 페이지나 문서를 Search Engine 프레임워크를 통해 찾아낼 수 있으며, Forum/Blog/IRC 프레임워크를 활용하여 가상화폐 범죄나 사기 사례에 대한 피해자 또는 전문가의 상세한 경험담을 수집할 수 있다. 또한 Digital Currency 프레임워크와 결합하여 특정 거래 ID, 주소, Forum 게시물 또는 소셜 미디어 언급을 추적, 의심스러운 거래의 배경이나 관련자에 대한 추가 정보를 확보할 수 있다.

Digital Footprint Analysis 방식은 Social Network, Forum/Blog/IRC, Digital Currency 프레임워크와 긴밀히 연관된다. Social Network 프레임워크를 통해 가상화폐 범죄자의 온라인 활동 패턴, 연관 관계, 선호하는 거래소 등의 정보를 파악할 수 있으며, 특정 해시태그 추적을 통해 가상화폐 사기 홍보 활동을 모니터링 할 수 있다. Forum/Blog/IRC 프레임워크는 범죄자나 피해자가 운영하는 Forum /Blog/IRC 분석을 통해 그들의 활동, 지식수준, 연관 관계 등을 파악하는 데에 활용될 수 있다. Digital Currency 프레임워크와 결합하여 블록체인상의 거래 이력을 다른 디지털 흔적과 연계 분석하여 범죄자의 활동 패턴을 더욱 포괄적으로 이해할 수 있다.

Geospatial OSINT 방법은 Social Network, Search Engine, Digital Currency 프레임워크와 연계하여 지리적 정보를 활용한 범죄 활동 분석을 가능하게 한다. Social Network 프레임워크를 통해 소셜 미디어 게시물의 위치 정보를 분석하여 가상화폐 범죄 조직의 활동 지역을 파악할 수 있으며, Search Engine 프레임워크를 활용하여 특정 지역과 관련된 가상화폐 활동을 검색하여 지역별 범죄 동향을 파악할 수 있다. Digital Currency 프레임워크는 거래의 IP 주소 분석을 통해 가상화폐 활동의 지리적 분포를 이해하는 데 도움을 준다.

마지막으로, Deep Web & Dark Web Analysis 방법은 Dark Web, Digital Currency, Exploit & Advisory 프레임워크와 밀접하게 연관된다. Dark Web 프레임워크를 통해 Tor 네트워크 등에서 운영되는 불법 마켓플레이스 또는 포럼을 분석하여 새로운 범죄 수법이나 거래 동향을 파악할 수 있다. Digital Currency 프레임워크와 결합하여 Dark Web 상의 가상화폐 거래를 추적하고 분석하여 자금 세탁 경로나 불법 거래의 규모를 파악할 수 있으며, Exploit & Advisory 프레임워크를 활용하여 Dark Web에서 거래되는 해킹 도구나 제로데이 취약점 정보를 수집하여 잠재적인 가상화폐 관련 사이버 공격을 예측할 수 있을 것이다.



(그림 3) OSINT 방법과 프레임워크를 적용한 통합 기법

(그림 3)은 가상화폐 범죄 추적 분석을 위한 OSINT 5가지 방법(Methods)과 7개의 프레임워크를 가상화폐 범죄 특성에 맞추어 통합한 분석 기법이며, 기존의 OSINT 관련 연구가 정보 출처에 따른 수집 방법에 대한 설명과 정보 수집 절차에 관한 연구, OSINT에서 수집한 정보의 유사도 분석 연구, 그리고 OSINT를 통하여 수집한 데이터를 지속적으로 데이터베이스화하여 이를 구축하는 방법에 대한 연구가 주를 이룬 것과 차이가 있다. 즉, 기존 연구들은 주로 OSINT 측면에서의 정보 분석에 중점을 둔 반면, 본 연구는 이러한 OSINT를 활용하여 수집되어 진 정보의 출처들과 프레임워크가, 가상화폐 범죄의 조사에 활용될 수 있는 실질적 방법론과 기법 측면에서 종합 분석하였다.

4. 결 론

본 논문에서는 가상화폐와 OSINT의 정의 및 분류

에 대해 알아보고, OSINT 방법과 프레임워크를 활용한 가상화폐 범죄 추적 분석의 적용 분야와 기법에 대해 상세히 분석하였다. 가상화폐의 익명성에도 불구하고 OSINT는 가상화폐 범죄 추적 분석에 있어 매우 효과적인 도구로 활용되며, 다양한 오픈 소스 데이터를 통합적으로 분석하여 범죄와 연관된 활동을 효과적으로 추적할 수 있게 한다. 특히 법 집행 기관 및 사이버 보안 전문가들이 이러한 OSINT를 활용한 추적 분석 기법을 적극적으로 도입하고 활용하여, 가상화폐를 이용한 사이버 범죄를 더욱 효율적으로 억제할 수 있을 것으로 기대할 수 있다.

더불어 향후 다양한 방법론의 적용을 통한 관련분야의 지속적인 정량적 및 정성적 연구와 OSINT 정보 저장 및 분석의 자동화 도구의 개발 및 향상 등을 통을 통해 가상화폐 범죄의 추적 효율성 및 범죄 활동 탐지의 정밀도 향상이 가능할 것이며, 국제적 협력과 법적 규제를 병행함으로 가상화폐를 통한 범죄를 더욱 체계적으로 억제할 수 있을 것을 기대한다.

참고문헌

[1] ㈜클로인트, “가상화폐 해킹 사건에 대한 북한 중심의 조사 분석 리포트‘, 2024.

[2] CertiK Alert[@CertiKAlert]. (2024, August 9). In 2024 there have been at least 5 incidents with initial losses of over $1m, per month. X. https://x.com/CertiKAlert/status/1821893299352825867.

[3] 이기영, 김익한, ”기록관리시스템 블록체인 기술 적용 방안 연구“, 기록학연구, 제60호, pp.317-358, 2019.

[4] CoinMarketCap. n.d.: https://coinmarketcap.com/.

[5] 정승원, 서병완, ”가상화폐 조사를 위한 블록체인 기반의 온체인 데이터 분석 기법 연구“, 디지털포렌식연구, 제17권, 제3호, pp.93-105, 2023.

[6] 더불어민주당 양경숙의원. 2022. 7. 18. "가상자산 불법행위 피해액 작년 3조 넘어. 검거인원도 증가". 언론 속의 양경숙. https://blog.naver.com/jongroyang/222817114583.

[7] 이승열, ”북한 사이버 공격 전략의 진화: 대북 제재 회피를 위한 외화벌이 수단으로서 사이버 전략“, 한국통일정책연구논총, 제32권, 제1호, pp.323-353, 2023.

[8] Gioti, Angeliki. Advancements in Open Source Intelligence (OSINT) Techniques and the role of artificial intelligence in Cyber Threat Intelligence, 2024.

[9] 앤소니 온체, 럭슨 즈비리쿠제, 장윤식, “사이버 수사에서 귀속문제 의사결정을 위한 공개출처 정보 처리 자동화”, 디지털포렌식연구, 제15권, 제2호, pp.86-98, 2021.

[10] OSINT Framework. n.d.: https://osintframework.com/.

〔저자소개〕

서 병 완 (Byung Wan Suh)
1993년 7월 미국 일리노이주립대학 학사
1995년 12월 미국 조지워싱턴대학교 석사
2013년 8월 서울종합과학대학원 박사
2017년 9월~현재 산업정책연구원
2023년 1월~현재 ㈜페어스퀘어랩 기업부설연구소장
email : byungwan.suh@gmail.com

김 원 웅 (Won-Woong Kim)
2022년 2월 한성대학교 IT융합학과 학사
2024년 2월 한성대학교 IT융합학과 석사
2024년 5월 ~ 현재 ㈜페어스퀘어랩 기업부설연구소
email : woong@fairsquarelab.com