AI 기반 크립토재킹 스크립트 삽입 검증 프레임워크

*이찬영, *강요한, *민준홍, *조하선
*네이버 클라우트 캠프, 이스트 소프트
dhzmehd1703@gmail.com, kangyohan040@naver.com, minjunhong95@gmail.com, hasunien@gmail.com

AI-based Framework for Verifying Cryptojacking Script Injection

*Lee Chan Young, *Kang Yo Han, *Min Jun Hong, *Jo Ha Seon
*Naver cloud camp, EST soft

요 약

크립토재킹(CryptoJacking)의 범죄율은 암호화폐 시장의 성장에 따라 지속적으로 증가하고 있다. 특히 보안성이 취약한 웹사이트를 대상으로 XSS나 서버 데이터 변조 등을 통해 마이닝 코드를 삽입하는 형태의 공격이 늘어나면서, 검증된 사용자의 서비스도 개인 사용자들에게는 크립토재킹 여부를 확인해야 하는 대상으로서 자리 잡고 있다. 이러한 공격의 가장 큰 피해자는 일반 사용자로, 피해를 사전에 방지하기 위해 URL 주소를 검증할 수 있는 AI(Artificial Intelligence) 기반 크립토재킹 스크립트 삽입 검증 프레임워크(Framework)를 제안한다. AI 기반 프레임워크 모델은 기존 시그니처 탐지(Signature-based Detection) 방식과 상용 LLM(Large Language Mode)을 결합해 코드 난독화를 해제하고 시그니처(Signature) 및 암호화폐 네트워크 패턴을 시뮬레이션 탐지하는 방식이며, 웹 통한 프레임워크 제작으로 일반 사용자들의 접근성을 높였다. 이러한 연구는 빠르게 확산하는 크립토재킹 피해 대응에 실무적 및 학문적 기여를 할 것으로 기대된다.

Ⅰ. 서 론

최근 암호화폐 시장의 성장과 함께 크립토재킹 공격의 비율이 증가하고 있다[1]. 특히 의료 분야에서는 700% 증가했고, 교육 기관은 2023년 대비 320배나 많은 공격을 받았다[2]. 이렇듯 크립토재킹은 일반 웹 사이트뿐만 아니라 검증된 기관성 웹 사이트에서도 감염 피해가 발생할 가능성이 존재하며, 감염된 페이지에 접근하는 개인 사용자들이 크립토재킹의 실질적인 피해 대상이 된다.

본 연구는 이러한 개인 사용자들의 피해를 줄이고자 AI 기반 크립토재킹 검증 프레임워크 제작을 목표로 한다. AI 기반 프레임워크는 기존 시그니처 탐지 방식의 난독화 및 소형화된 변종 위협이라는 한계를 보완하고 높은 탐지율을 보이며, 웹 프레임워크 제작을 통해 개인 사용자들의 접근성을 높여 크립토재킹 피해를 사전에 방지할 수 있는 방안을 제시하고자 한다.

Ⅱ. 이론적 배경

2.1 크립토재킹의 개념 및 동작 원리

크립토재킹은 CryptoCurrency 와 Hijacking을 합친 용어로 다른 사용자들의 PC 리소스를 이용해 크립토마이닝(Cryptomining)을 수행하는 행위들을 통칭하는 공격이다[3]. 주로 사용자의 브라우저 단에서 동작하며, 사용자가 웹 사이트에 방문하면 공격자가 삽입한 자바스크립트(JavaScript) 크립토마이닝 코드가 로드되어 실행된다. 이렇게 실행된 코드는 웹 사이트 방문자의 동의 없이 방문자의 자원을 암호화폐 채굴에 이용하며 채굴에 의한 보상은 공격자에게 지급된다.

이에 따라 사용자는 리소스 자원 부족 현상으로 인해 운영체제 오류나 사용상의 문제를 야기할 수 있고, 하드웨어 수명 단축 문제가 발생할 수도 있다.

2.2 기존 탐지 방식의 방법 및 한계

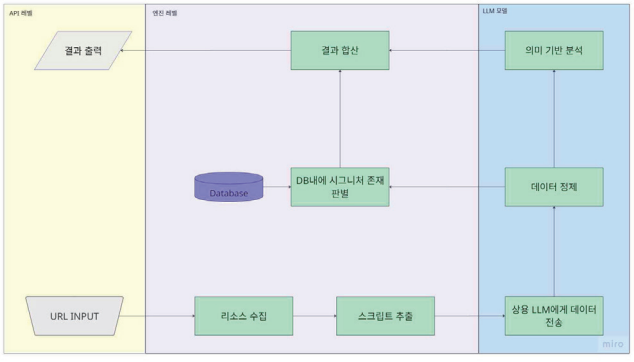
크립토재킹 탐지에서 가장 많이 사용되는 정적 탐지 방식인 시그니처 탐지 방식은 패턴을 찾아 위협을 식별하는 방법으로, 미리 정의된 패턴들이 데이터베이스에 저장되어 탐지 시스템이 대상 데이터와 비교하여 탐지한다[3]. 따라서 시그니처 탐지 방식은 데이터베이스 내부에 있는 패턴은 정확한 탐지가 가능하지만, 난독화나 소형화된 변종 패턴에 대해서는 탐지가 불가능하고 데이터베이스를 갱신하지 않으면 실시간성이 떨어진다는 한계가 있다.

즉, 공격자가 다양하고 쉽게 구현할 수 있는 난독화 및 소형화 기법을 사용해서 시그니처 탐지를 쉽게 우회할 수 있다.

Ⅲ. 기술적 배경

3.1 프레임워크 구조

본 연구의 프레임워크 구조는 데이터를 수집/정제하고 나온 데이터를 가지고 크립토재킹을 탐지하여 나온 결과를 웹에 출력하는 형태이다.

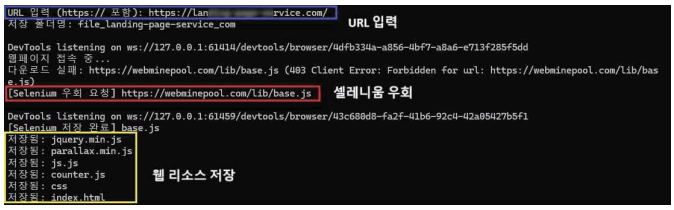


[그림 1] 프레임워크 모식도

3.1.1 데이터 수집 및 정제

AI 기반 프레임워크 모델은 분석을 위해 입력 URL에 대한 사이트의 리소스 데이터를 수집한다. 일반적으로 크립토재킹 스크립트는 HTML 내부 또는 외부에 자바스크립트 형태로 존재하며, 의도적으로 스크립트 파일을 감추기 위해 확장자를 명시하지 않고 서버에 업로드되어 있거나, 페이지 로드 이후에 일정 시간 지난 후 외부에서 악성 스크립트가 로드되는 등 다양한 가능성이 존재한다. 따라서, 셀레니움(Selenium)과 같은 포터블 오픈 소스 프레임워크를 사용하여 대상 접근 시점부터 페이지 로드 이후까지의 전체 리소스를 수집한다.

이렇게 수집된 데이터는 클라이언트 브라우저 레벨에서 실행되는 마이닝 코드를 찾기 위해 전체 리소스에서 실행할 수 있는 스크립트 부분을 모두 추출하고 나머지 영역의 소거를 진행한다. 이 과정에서 스테가노그래피 기법과 같이 리소스 내에 은닉된 실행 가능 코드 영역도 추출되며, 수집된 실행 가능한 코드 영역은 하나의 파일로 병합된다. 이후 상용 LLM을 활용해 난독화 및 소형화를 해제하는 데이터 정제 과정이 진행되며, 이러한 정제 작업은 AI및 시그니처 탐지 과정의 분석 효율이 크게 개선된다.



그림[2] 데이터 수집

[그림 3] 데이터 정제

3.1.2 AI 기반 스크립트 검증

정제된 데이터 기존 방식인 시그니처 기반의 패턴 탐지와 상용 LLM을 사용한 문맥 기반 분석을 진행한다. 문맥 기반 분석은 코드의 문맥과 실행 흐름을 종합적으로 분석하고 악성여부를 판단 하는 것으로, 크립토재킹과 관련된 CPU의 사용률을 설정하는 Throttle 설정값, 암호화폐 지갑 주소 형식의 문자열, 그리고 start(), setInterval() 등 반복 실행 함수가 코드 내에 존재하는지에 대해서 중점적으로 분석한다. 이로써 본 연구의 탐지는 기존 시그니처 탐지 방식을 개량한 교차 검증 형태로 더욱 정확한 악성여부 탐지가 가능해지며, 상용 LLM을 통한 실시간 분석으로 변종 위협에 대응할 수 있는 구조를 갖게 된다.

3.1.3 프레임워크 결과 출력

본 연구에서 만들어진 프레임워크는 시그니처 탐지와 AI의 문맥 기반 분석을 통한 결과를 합쳐 일반 또는, 변종 크립토재킹을 탐지한다. 이러한 탐지 결과를 웹에 연동하여 사용자들이 식별하기 편하게 값을 출력하므로, 일반 사용자도 크립토재킹을 탐지할 수 있게 접근성을 높였다.

[그림 4] 웹 화면

[그림 5] 웹 결과 출력 화면

Ⅳ. 결론

본 연구에서 제안하는 크립토재킹 검증 프레임워크는 웹을 이용하는 탐지 프레임워크로 개인 사용자들의 피해 확산을 방지한다. 또한 상용 LLM을 시그니처와 결합한 탐지는 단순한 스크립트 내 시그니처 매칭에 의존하지 않고, 코드의 구조적 특성과 실행 패턴을 분석함으로써 다양한 형태의 변종 공격에도 유연하게 대응할 수 있다.

그 결과, 이 연구는 보안 지식이 부족한 사용자들이 점차 늘어나고 있는 크립토재킹과 변종 크립토재킹 공격을 감지할 수 있으며, AI와 시그니처 탐지 방식을 결합한 교차 검증 형태라는 발전된 방향성을 제시하였고 본 연구의 시스템을 웹에 연동시킴으로써 사용자들의 접근성을 높였다. 향후 연구로는 더 발전된 AI를 이용한 성능 강화와 크립토재킹의 새로운 변종 기법에 대한 대응 방안 마련이 필요할 것으로 제안된다.

참 고 문 헌

[1] 사이버보안팀, “크립토재킹 (Miner) 공격 시나리오”, 한국재정정보원 보안동향 및 통계 September, 2021. (https://www.fis.kr/ko/major_biz/cyber_safety_oper/attack_info/notice_issue?articleSeq=1998&utm_source)

[2] Sean Blanton “90+ 2024 Cybersecurity Statistics and Trends”, October, 2024

[3] 고동현, 정인혁, 최석환, 최윤호, “크립토재킹 사이트 탐지를 위한 동적 분석 프레임워크”, Journal of The Korea Institute of Information Security & Cryptology, vol. 28, no.4, pp. 963-974, Aug. 2018.