LLM 기반 웹 콘텐츠 분석을 통한 암호화 압축파일의 악성코드 차단 자동화 기술 개발

정대영, 이성훈*, 김정환**

네이버 클라우드 캠프, 이스트소프트

hidae0az@gmail.com, only4clovers@gmail.com*, kkim60260265@gmail.com**

Development of automated technology for blocking malware in encrypted compressed files through LLM-based web content analysis

Jeong Dae Young, Lee Sung Hoon, Kim Jeong Hwan

Naver Cloud Camp in Est Soft

요 약

기존의 엔드포인트 보호 솔루션이나 웹 보안 솔루션은 주로 웹 소스코드 정적 분석 또는 사용자 입장에서의 실행 이후 탐지 및 차단에 집중되어 있어, 암호화 압축과 같은 간단한 방법으로 우회가 가능한 한계점이 존재한다. 이러한 웹 콘텐츠의 파일 전송 환경 내의 위협을 해결하기 위해 상용 대규모 언어 모델(LLM)을 기반으로 웹 콘텐츠를 분석하여 암호화 압축을 해제하고 온라인 위협 탐지 서비스 기반의 분석을 통해 압축 파일 내 악성코드 감염 여부를 검증하는 시스템을 제안한다. 본 논문은 웹 소스코드의 LLM기반 암호화 압축 내부 분석으로 웹 콘텐츠에 포함된 압축파일의 악성 여부를 검증하는 브라우저 확장 프로그램을 제안하며, 공공 보안 측면에서 중요한 기여를 할 것으로 기대된다.

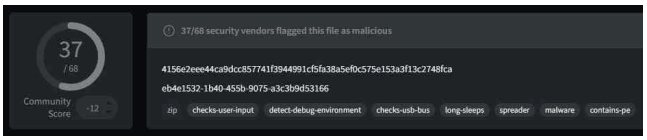
I. 서 론

웹 보안 서비스로는 대표적으로 Google Safe Browsing과 같은 기본 브라우저 서비스나 Avira, Avast와 같은 보안기업의 브라우저 확장 프로그램 등이 사용되고 있으나, 기술적 한계로 인해 암호화 압축 파일 악성여부 감지를 지원하지 않는다. 이는 브라우저의 암호화 파일을 일반적인 정적 분석만으로는 실시간 탐지할 수 없다는 데에서 비롯된다[1]. 따라서 암호화 압축파일은 대표적인 악성파일 운반책으로 사용되고 있으며, 해킹 사례들의 사용자 접근 단계에서 각종 보안 솔루션들을 우회하는 데에 집중적으로 활용되기 때문에 압축파일의 세부적인 검증에 대한 필요성이 강조되고 있다. 특히 웹 서비스에서 공유되는 파일들은 대부분 압축파일로 공유되고 있으며, 사용자는 악성 파일 노출로부터 IT 자산을 보호하기 위해 백신을 포함한 엔드포인트 보호 솔루션의 악성코드 검사에 한정하여 의존하고 있는 실태이다. 본 연구에서는 암호화 압축 내부 파일이 기존 엔드포인트 보호 솔루션의 검증 제외 대상이라는 특징에 집중하여, 대규모 언어 모델(LLM)을 활용한 웹 콘텐츠 분석을 통해 암호화 압축을 자동 해제하고, 격리 환경에서 악성 여부를 진단하는 브라우저 확장 프로그램을 개발하여 보안성을 확보하는 시스템을 제안한다.

II. 본 론

2.1. 기존 암호화 압축파일 분석 과정

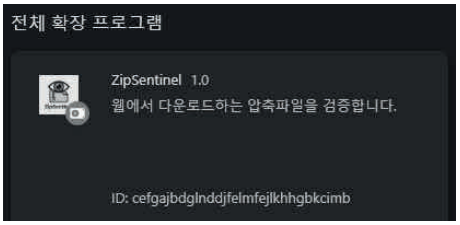
<그림 1>는 37개 안티바이러스 엔진에서 악성 진단을 받은 파일의 분석 보고서 표본이다. 해당 표본의 파일 전송은 Google Safe Browsing 서비스가 적용된 다운로드 환경에서 진행되었으며, 일체의 경고 없이 파일 전송이 완료되었다. 암호화 압축파일은 데이터가 비밀번호를 기반으로 암호화되어있기 때문에 엔드포인트 보안 솔루션이 적용된 브라우저도 내부 위협 요소를 식별할 수 없다[2]. 이에 따라 파일 전송 환경에서 악성코드가 존재하는 대상의 위협을 탐지하지 못하고 다운로드가 진행되어 버리는 한계를 보여준다. 이에 본 논문은 기존의 한계점을 극복하기 위해 암호화 압축 파일을 격리 환경에서 해제하여 직접 분석하는 보안 기법 개발을 핵심으로 한다.



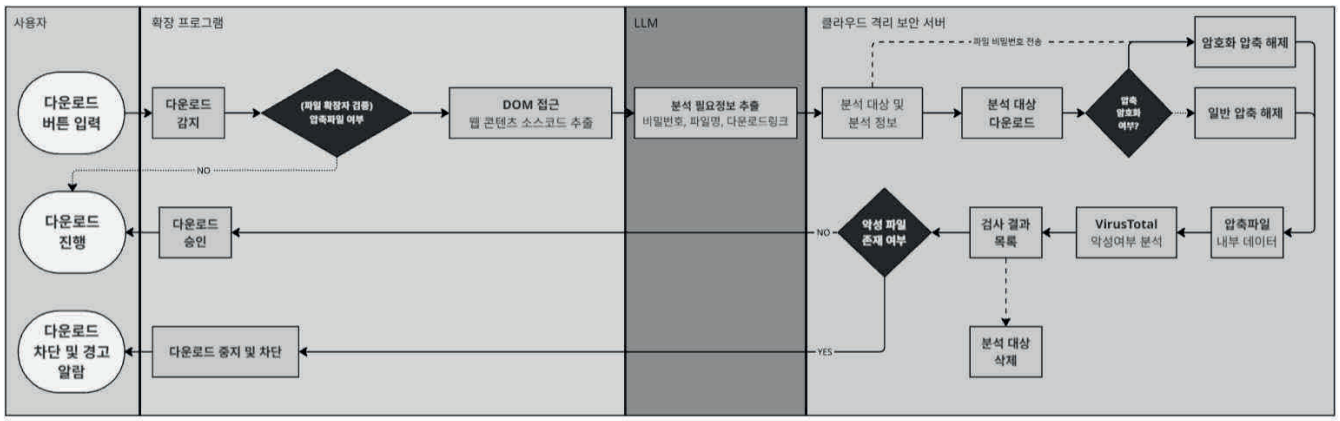
〈그림 1〉 악성 압축파일 분석 보고서

2.2. 브라우저 기반 확장 프로그램 개발 환경

본 논문에서 제안하는 시스템은 범용성과 접근 방향성을 고려하여 Manifest V3기반으로 제작되었다. Manifest V3는 Google Chrome을 비롯한 Chromium 기반 브라우저에서 통용되는 브라우저 확장 플랫폼으로, 사용자가 접근중인 웹 페이지의 DOM(Document Object Model)에 직접 접근할 수 있으며, 이를 통해 콘텐츠 내 HTML 소스코드와 자바스크립트와 같은 주요 데이터를 분석할 수 있다[3]. 또한 Manifest V3 내부 API를 사용하여 다운로드 이벤트를 감지할 수 있으며, 다운로드 직전 웹 페이지 정보를 기반으로 사전 경고, 차단 시스템을 구현할 수 있다. 콘텐츠의 분석과 다운로드 감지는 확장 프로그램 내에서 처리되며, 암호화 압축파일 해제 및 분석은 외부 격리 서버에 연동되어 이루어진다. 이하 내용은 개발한 확장 프로그램의 시스템 구성 요소를 설명한다.



〈그림 2〉 Google Chrome에 적용된 확장 프로그램



〈그림 3〉 시스템 구성 요소 흐름도

2.3. 콘텐츠 내 데이터 추출

암호화 압축 내부를 직접 분석하기 위해 파일 정보를 추출하는 과정이 필요하다. 일반적인 웹 콘텐츠 환경에서 압축파일의 암호화는 출처에 대한 간접적 인지의 목적으로 이루어지기 때문에, 비밀번호가 본문 내에 포함되는 경우가 대부분이다. 이에 다운로드가 이루어지는 웹 페이지를 분석하기 위한 적절한 도구의 채택이 필수적이다. 상용 LLM은 웹 콘텐츠에서 문맥에 따라 정보를 추출하는 데 특화된 모델로, 콘텐츠 정보를 본문에서 추출하는 방식에 있어 패턴 기반 분석 방법인 정규표현식과 비교하여 그 성능이 탁월하다[4]. 본 논문은 상용 LLM인 GPT-4o모델을 활용하여 파일명, 다운로드 링크, 압축파일 비밀번호를 .JSON 데이터셋으로 가공한다. 해당 데이터셋은 압축 해제 자동화로 연계되어 암호화 압축파일 분석에 사용된다.

2.4. 압축 해제 자동화

다운로드 이벤트가 발생하여 웹 페이지 내 정보가 데이터셋으로 산출되면, 다운로드 링크를 바탕으로 격리 환경에서 직접 다운로드한다. 이후 데이터셋 내 비밀번호를 이용해 자동으로 압축을 해제한다. 중첩으로 압축된 파일은 추가 압축 형태가 감지되지 않을 시점까지 반복하여 추출된 모든 파일을 분석 대상에 포함시킨다. 해당 과정은 일반 압축파일의 확장자(.zip, .rar, .7z, .tar.gz)를 포괄하도록 설계되었다.

2.5. 악성코드 감염 여부 분석

압축파일 내부 데이터 악성 여부 탐지는 온라인 위협 탐지 서비스를 활용하는 방식으로 이루어진다. VirusTotal은 다양한 안티바이러스 엔진의 분석 기능을 통합 제공하는 온라인 위협 탐지 서비스로, 업로드 된 파일에 대해 다양한 보안 엔진을 기반으로 정적 및 동적 분석을 수행한다. 본 논문에서 암호화가 해제된 압축파일 내부 데이터의 악성 여부 판단에는 VirusTotal API가 탑재되어 작성된 Python 코드가 사용되며, 시스템 내에서 다운로드 환경의 파일을 전반적으로 검증한다. 압축이 해제된 파일은 Hash만을 일차적으로 검증하여 빠르게 악성여부 탐지를 진행한다. Hash가 감지되지 않을 경우에는 파일 전체를 VirusTotal API에 업로드하여 정밀하게 분석한다[5]. 악성 여부가 검출된 파일은 실행 권한을 제거하는 방식으로 임시 격리조치 시키며, 확장 프로그램 상에서 사용자의 다운로드 이벤트를 취소하여 위협을 차단한다.

Ⅲ. 결 론

본 연구는 AI 기반 웹 콘텐츠에 포함된 암호화 압축 파일 분석을 자동화하여 기존 웹 보안 솔루션과 차별화된 브라우저 확장 프로그램을 제시한다. 분석 과정에서는 보안 격리 환경을 구축하여 임의의 사용자가 데이터를 조작하지 못하도록 설계하여 분석 결과에 대한 무결성을 확보하였다. 결론적으로 기존 엔드포인트 보안 솔루션의 한계를 해당 확장 프로그램으로 해결할 수 있다는 가능성을 제시하며, 나아가 일반 사용자의 권익을 보호하는 방향성을 통해 공공 보안 차원의 연구·실무적으로 크게 기여할 것으로 기대된다.

참 고 문 헌

[1] De Gaspari, Fabio, et al. "Encod: Distinguishing compressed and encrypted file fragments." Network and System Security: 14th International Conference, NSS 2020, Melbourne, VIC, Australia, November 25 - 27, 2020, Proceedings 14. Springer International Publishing, 2020.

[2] 박종인, 손익영, 송주석. "통신효율과 보안을위한 자료압축과 암호화의 결합." 한국정보과학회 학술발표논문집 18.2 (1990): 581-584.

[3] Google. "Overview of the Chrome Extension Manifest V3." *Chrome for Developers*, 22 Feb. 2023, https://developer.chrome.com/docs/extensions/mv3/intro/mv3-overview.

[4] Luitjens, Pieter. “Natural Language v. Regex: The Context Wars.” *Private AI*, 3 Feb. 2021, “https://www.private-ai.com/en/2021/02/03/1412/”.

[5] VirusTotal, How it works, VirusTotal, “https://docs.virustotal.com/docs/how-it-works”.