# 콘텐츠 무해화 및 재조합 기술 연구 분석 및 고찰

오소현[1], 아비르[2], 박종혁[2,*]
[1]서울과학기술대학교 행정학과
[2,*]서울과학기술대학교 컴퓨터공학과
{dipelz, abir.el, jhpark1}@seoultech.ac.kr

# An analysis of Content Disarm and Reconstruction

Sohyeon Oh[1], Abir EL Azzaoui[2], Jong Hyuk Park[2,*]
[1]Department of Public Administration, [2]Department of Computer Science and Engineering, Seoul National University of Science and Technology

요 약

비대면 활동 및 원격 작업 증가에 따라 문서 파일을 이용한 사이버 공격 빈도가 증가하고 있으며, 별도의 실행 파일 대신 문서 내의 기본적인 기능을 악용하는 문서 공격은 기존의 악성코드 탐지 메커니즘을 우회할 수 있기 때문에 큰 문제가 되고 있다. 이러한 문제에 대응하기 위한 여러 기술 중 CDR 기술은 악성 행위에 이용될 가능성이 있는 액티브 콘텐츠를 제거하거나 비활성화하여 사전에 악성코드로 탐지되지 않았던 파일에 대한 보안성을 제공하지만, 문서의 내용을 분석하고 안전하게 재조합하는 과정에서 오류가 발생하여 전달하고자 했던 내용을 제대로 표현할 수 없게 되거나, 파일을 사용할 수 없게 되는 문제가 발생할 수 있다. 본 논문에서는 파일을 후처리하는 방식으로만 CDR을 적용하는 것이 아니라, 확장 프로그램이나 가상 환경 등을 이용해 문서의 작성 단계에서부터 CDR 처리 과정을 거치게 하는 방법을 제안하여 파일 손상이나 내용 누락 문제를 완화하고 사용자의 업무 효율을 높이는 동시에 강화된 보안성을 제공한다.

## 1. 서론

현재 우리는 4차 산업혁명 시대를 맞이하고 있기도 하지만 한편으로 포스트 코로나 시대에 적응해 가는 중이기도 하다. 예기치 못한 전염병의 출현은 우리 사회를 비대면 친화적인 모습으로 변화시켰다. 재택근무 및 온라인 수업 등에 관한 수요가 높아짐에 따라 인터넷 접속을 통한 원격 작업 및 자료 공유도 그만큼 활발해진 바 있다. 업무상 자주 접근할 수밖에 없는 이메일이나 문서 파일을 통한 공격의 경우 비대면 작업이 빈번해진 환경에서 영향력을 발휘할 가능성이 크며, 특히 문서형 악성코드 공격은 문서 내의 정상적이고 기본적인 기능을 이용하기 때문에 기존의 악성코드 탐지 방식을 우회할 수 있어 더욱 위협적이다.

이러한 문서형 악성코드 공격에 대응하기 위한 기술로 Content Disarm and Reconstruction (CDR)이 있다. CDR은 문서 파일이 사용자에게 전달되기 전에 파일을 미리 분석하여 문서 내 매크로, 하이퍼링크, 템플릿, 이미지 등 악성코드가 삽입될 수 있는 액티브 콘텐츠들을 제거하거나 비활성화한다. 사용자는 의심스러운 외부 문서를 다운로드 및 열람할 때 CDR을 적용하여 안전하게 재구성된 파일을 받을 수 있다. 그러나 CDR은 파일 처리 과정에서 공격에 이용될 위험이 있는 모든 요소를 일방적으로 제거하므로, 문서의 내용을 의도하지 않은 방향으로 변경하거나 업무에 필수적인 액티브 콘텐츠를 비활성화하여 사용자에게 불편을 줄 수 있다는 문제점이 있다. 문서를 조작하여 안전한 요소로 내용을 재조합하는 것이 가독성 저하 및 파일 손상으로 이어질 가능성도 존재한다.

본 논문에서는 사용자가 문서 작성 단계에서 보는 모습과 CDR 처리를 거친 후의 모습이 달라질 수 있고 액티브 콘텐츠를 사용하여 완성한 문서에 CDR을 적용하는 과정에서 파일이 손상될 수 있다는 점을 보완하기 위해 문서 공유 단계가 아닌 작성 단계에서부터 CDR로 무해화된 요소만을 이용해 문서를 작성하는 방안을 제안한다.

### 2-1. 문서를 이용한 악성코드 공격

악성코드를 탐지하는 방법에는 크게 정적 분석과 동적 분석이 있다. 정적 분석은 파일의 종류나 헤더

정보와 같은 파일의 고유 속성에 초점을 맞추어 악성 여부를 판단하고, 동적 분석은 파일이나 프로그램의 행위에 초점을 맞추어 파일의 동작을 보고 악성 여부를 탐지한다[1]. 그러나 문서를 이용한 공격은 이러한 탐지 방식을 우회할 수 있는 특성들을 지니고 있다. 문서형 악성코드를 이용하는 공격자는 문서 내의 정상적 기능인 하이퍼링크, 매크로, 메타데이터, 스크립트 등을 이용해 악성코드를 은닉한다. 그리고 이를 정상적인 문서인 것처럼 배포한 뒤, 사용자가 부주의하게 문서를 열람하거나 악성코드를 활성화하도록 유도한다[2]. 이러한 공격은 별도의 실행 파일을 동작시키는 것이 아니라 문서 자체의 기능을 이용하는 것이므로 데이터베이스와 패턴 매칭을 이용한 방식에 탐지되지 않을 가능성이 있고[3], 사용자가 문서를 어느 정도 읽거나 특정 액티브 콘텐츠를 활성화할 때까지 기다렸다가 악성 행위를 수행하도록 공격을 설계한 경우 샌드박스와 같은 가상 환경에서 파일을 실행시키는 동적 방법으로도 탐지되지 않을 가능성이 크다.[4] 그리고 이러한 문서형 악성코드는 다양한 경로를 통한 접근이 용이하고, 사회공학적 기법을 통해 쉽게 유포될 수 있다[5].

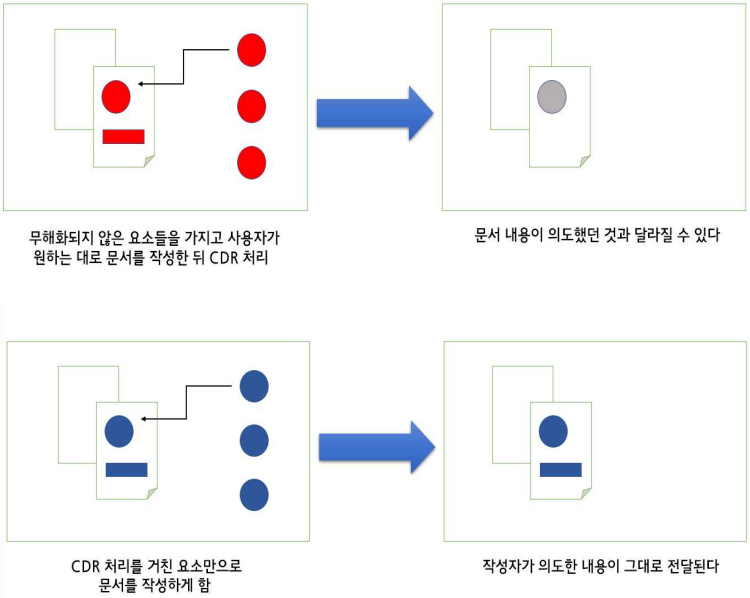
### 2-2. Content Disarm and Reconstruction (CDR)

CDR 기술은 파일 내에서 액티브 콘텐츠들을 제거한 뒤 안전한 요소들만을 가지고 파일을 다시 구축하는 기술을 말한다. CDR은 문서에 포함된 의심스러운 요소를 비활성화 및 제거하거나 대체한 뒤 안전한 파일을 사용자에게 전달함으로써 문서 안에 있을지 모르는 악성코드의 실행을 막는다. 즉, 모든 파일을 잠재적 위협으로 간주하고 악용될 가능성이 있는 콘텐츠를 전부 차단하여 파일에서 악성 행위가 실행될 가능성을 사전에 방지하는 것이다. 이 기술이 완성도 있게 적용되기 위해서는 대상이 되는 문서 형식에 대한 수준 높은 이해가 필요하다. 악성코드가 삽입될 가능성이 있는 요소 및 해당 요소의 위치를 파악하고 있어야 하며, 위협적 콘텐츠를 제거한 문서를 원본과 거의 동일한 모습으로 재조합하여 출력할 수 있어야 한다[6].

그러나 다양한 형태로 작성된 문서 내용 중에서 어떤 것이 악의적 데이터이고 어떤 것이 업무를 위한 필수적 데이터인지 가려내기는 쉽지 않다. 또한, 문서를 재조합하는 과정에서 문서의 내용이 변형되어 원본 문서에서 의도했던 것과 다르게 전달되거나 정합성에 문제가 생겨 파일이 제대로 동작하지 않을 수 있다. 외부 폰트 등 특이한 데이터를 이용한 경우 문서가 악성코드를 포함한 것으로 오인되어 열람이 제한될 가능성도 존재한다[7].

### 3. 제안 기법

문서 재조합 단계에서 발생할 수 있는 손상 및 사용자가 의도했던 내용의 누락 문제를 보완할 방법으로, 문서가 처음 작성될 때부터 CDR의 무해화 기준을 충족하는 환경에서 작성되도록 하는 방법을 제안하고자 한다. 다시 말해 CDR의 처리 순서를 앞당기는 것이다. (그림 1)은 제안 기법을 간략하게 나타내고 있다. 사용자는 문서를 공유 및 열람하는 단계가 아닌 작성하는 단계에서부터 CDR 기술을 적용하여, 후에 제거되지 않을 만한 요소들로 문서 내용을 표현한다. 이후 임의의 다른 사용자가 해당 문서에 대해 추가로 CDR 처리를 진행하더라도 문서 작성 단계에서 보는 문서와 CDR 적용 이후 보는 문서는 동일하다.




(그림 1) CDR 처리 순서 변경

제안 기법은 CDR 기술이 적용된 가상 환경을 제공하거나 확장 프로그램과 같은 형식으로 문서 작성 툴 자체에 CDR 솔루션을 적용하여, 사용자가 문서를 작성하며 첨부하는 요소들이 곧바로 무해화 과정을 거친 뒤 삽입될 수 있도록 한다. 이렇게 할 경우 문서가 의도한 형태로 전달되지 않는 문제나 정합성

문제를 방지할 수 있다. 기존의 악성코드 탐지 기술과 연동해 문서 작성 중 의심스러운 스크립트나 기능의 삽입 자체를 차단하는 기능을 추가하여 보안성을 강화하는 것도 가능하다.

또한, 외부에서 들어오는 문서가 이러한 CDR 환경에서 작성된 것인지 확인하여 수신자가 승인 여부를 결정할 수 있도록 한다. 공문이나 이력서 등 업무를 위한 문서 공유가 필요할 경우 작성자에게 CDR 환경에서 작성된 문서만을 제출하도록 요구하고 일반 환경에서 작성된 문서는 차단함으로써 위협적 요소의 유입을 봉쇄할 수 있다.

## 4. 결론

본 논문에서는 문서를 이용한 악성코드 공격 수법, 그에 대응하는 CDR 기술의 효과와 한계 등을 분석하고, 문서 재조합 단계에서 일어날 수 있는 문제점 해결을 위한 방안을 제시하였다.

CDR 기술은 무해화한 콘텐츠에 관한 데이터를 축적하여 분석용으로 사용하거나, 다른 악성 코드 탐지 기술과 결합하여 기존 백신을 보조하거나, 내부로 들어오는 파일뿐 아니라 외부로 나가는 파일의 안전성을 확보하는 등 다양하게 응용할 수 있다. 근래에는 CDR 기술을 웹 및 데스크톱 버전으로 이용할 수 있게 하는 연구[8], 국내에서 사용하는 문서 형식 및 이메일 환경에 적용할 수 있는 브라우저 확장 프로그램 개발 등의 시도가 있었다[9]. 이러한 연구가 계속되어 CDR 기술에 대한 접근성이 개선되면 보다 많은 사람에게 해당 기술을 보편적으로 사용하도록 권장할 수 있을 것이고, 무해화를 거치지 않은 파일을 경계하는 풍조를 형성하여 사회공학적 공격에도 어느 정도의 대응성을 갖출 수 있을 것으로 사료된다.

## Acknowledgment

This research was supported by the National Research Foundation of Korea(NRF) funded by the Ministry of Science and ICT(2022K1A3A1A61014825).

## 참고문헌

[1] "효율적인 보안시스템 구축을 위한 분석기술의 통합." 컴퓨터월드. https://www.comworld.co.kr/news/articleView.html?idxno=49618, 2019.

[2] 강아름, 정영섭, 김세령, 김종현, 우지영, 최선오. "문서 구조 및 스트림 오브젝트 분석을 통한 문서형 악성코드 탐지." 한국컴퓨터정보학회논문지 23 no.11, 85-93, 2018.

[3] 박현수, 강아름. "CNN 기반 MS Office 악성 문서 탐지." 한국정보보호학회논문지 32 no.2, 439-446, 2022.

[4] 이상준. "표적형 악성코드 대응 CDR 기술 동향." 주간기술동향 no.1939, 12-24, 2020.

[5] 최민지, 신강식, 정동재. "HWP 문서형 악성코드 위협인자 추출 및 분석 연구." 한국정보과학회 학술발표논문집 874-876, 2021.

[6] Simon Wiseman. "Content security through transformation." Computer Fraud & Security 2017 no. 9, 5-10, 2017.

[7] 한재혁, 윤영인, 허지민, 이재연, 최정인, 홍석준, 이상진. "망분리 환경에서 파일형식 변환을 통한 안전한 파일 전송 및 포렌식 준비도 구축 연구." 한국정보보호학회논문지 29 no.4, 859-866, 2019.

[8] 서민정, 고희수, 양현지, 강민주, 김관영. "오픈소스 기반 문서형 악성코드 차단 프로그램의 개발." 한국정보처리학회 학술대회논문집 27 no.2, 859-866, 2020.

[9] 김희은, 손태식, 김두원, 한광석, 성지훈. "오픈소스 기반 APT 공격 예방 Chrome extension 개발." 온라인 추계학술발표대회 논문집 9 no.3, 2021.