

# 오픈소스 기반 문서형 악성코드 차단 프로그램의 개발

서민정\*, 고희수\*\*, 양현지\*\*\*, 강민주\*\*\*\*, 김관영\*\*\*\*\*

\*경희대학교 응용수학과

\*\*인천대학교 정보통신공학과

\*\*\*우석대학교 정보보안학과

\*\*\*\*성신여자대학교 융합보안공학과

\*\*\*\*\*Open UP

[mathmjseo@khu.ac.kr](mailto:mathmjseo@khu.ac.kr), [kohs116@naver.com](mailto:kohs116@naver.com), [tkrk1090@stu.woosuk.ac.kr](mailto:tkrk1090@stu.woosuk.ac.kr), [20180886@sungshin.ac.kr](mailto:20180886@sungshin.ac.kr),  
[gy741.kim@gmail.com](mailto:gy741.kim@gmail.com)

## Development of an open source-based malicious code blocking program

Minjeong Seo\*, HuiSu Ko\*\*, Hyeonji Yang\*\*\*, Minju Kang\*\*\*\*, GwanYeong Kim\*\*\*\*\*

\* Dept. of Applied Mathematics, KyungHee University

\*\* Dept. of Information and Computer Engineering, In-Cheon University

\*\*\* Dept. of Information Security, Woosuk University

\*\*\*\* Dept. of Convergence Security Engineering, Sungshin Women's University

\*\*\*\*\*Open UP

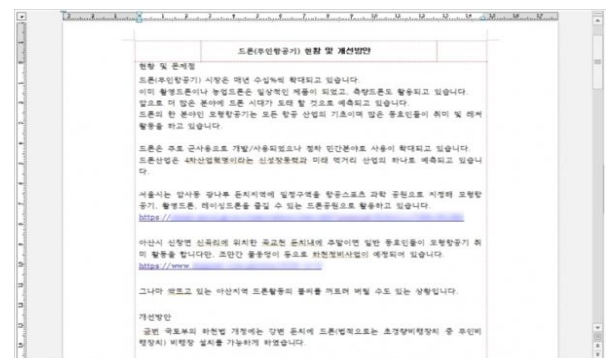
### 요 약

인터넷의 활발한 이용으로 인해 악성코드의 유포 경로가 다양해지고 있다. 그 중, 문서형 악성코드 감염 사례가 증가하고 있다. 문서형 악성코드는 이메일, 온라인에서 다운로드 받는 PDF, DOCX 파일의 취약점을 통해 유포되고 있다. 이로 인해 우리는 쉽게 바이러스에 감염될 수 있다. 그러므로 문서형 악성코드의 예방은 매우 중요하다. 우리는 악성코드로 의심되는 문서 파일을 안전한 PDF 파일로 변환해 주는 오픈 소스 프로그램인 Dangerzone<sup>1</sup>을 활용하여 개인과 기업에서 프로그램을 쉽고 편리하게 사용할 수 있도록 웹, 데스크톱 형태로 확장 개발한다.

### 1. 서론

#### 1.1 개발 배경

최근, 문서로 위장한 악성 코드 유포 사례가 발생하고 있다. 2020년 6월 3일, 안랩은 ‘국내 드론 현황 및 개선 방안 관련 보고서’로 위장한 악성 문서 파일을 발견하고 이에 따른 피해가 발생하지 않도록 사용자에게 각별한 주의를 당부하였다.



(그림 1) '드론 현황 및 개선방안'으로 위장한 문서 파일 [이미지=안랩].

문서형 악성 코드에 대한 연구는 여전히 지속하고 있다. 더불어 감염 여부를 자동적으로 판단하기 위한 시스템 또한 각계에서 다양하게 연구되고 있다. [1]

문서형 악성 코드는 불가피하게 문서를 열어봐야

<sup>1</sup>Dangerzone. (n.d.). Retrieved September 27, 2020, from <https://dangerzone.rocks/>

하는 기자나 특수성을 가진 직업의 경우 보안에 매우 취약하다. 따라서 이러한 공격에 효율적으로 대처하기 위한 방안과 관련 프로그램의 필요성이 증가하고 있다.

## 1.2 관련 연구

Dangerzone은 First Look Media가 Nullcon 2020 hacker conference에서 발표한 문서형 악성 코드를 탐지하여 안전한 파일로 변환해주는 오픈소스 프로그램이다. 작동 원리는 먼저 PDF 파일의 페이지를 RGB 비트맵으로 렌더링하고, 악성코드를 사용할 수 있는 공간이 남지 않게 하여 최종 파일이 반환되도록 한다. 또한 Linux Container를 사용하여 위험한 문서를 샌드박스 이동시켜 안전한 파일로 변환한다.

Dangerzone의 상세 작동 원리는 그림 2와 같다.



(그림 2) Dangerzone 작동 원리

## 1.3 개발의 필요성

Dangerzone은 개인 클라이언트별로 설치하여 구동해야 한다는 한계가 있다. 따라서 다수의 클라이언트가 이용하는 기업 환경에서는 사용하기에 어려움이 있다.

본 프로젝트에서는 Dangerzone을 웹 애플리케이션 및 데스크톱 S/W으로 확장하여 기업 엔터프라이즈 환경에서 유저들이 사용할 수 있도록 개발하고자 한다.

## 2. 본론

### 2-1. 시스템 개요

오픈소스 Dangerzone을 이용하여 문서형 악성코드를 예방한다. 특히, 사용자의 OS 환경에 의존하지 않고 이용할 수 있도록 웹 애플리케이션과 데스크톱 S/W 버전으로 확장 개발하는 것을 목표로 한다.

### 2-2. 기능 설계 - 웹 애플리케이션

사용자가 변환할 파일을 전달하였을 때, 어떠한 악성코드들이 발견되었는지 여부를 확인할 수 있도록 VirusTotal API2를 활용한다. 또한 변환된 파일의 보안

을 위해 1 회 다운로드로 제한하고, 프로그램 내 DB에서 삭제한다.

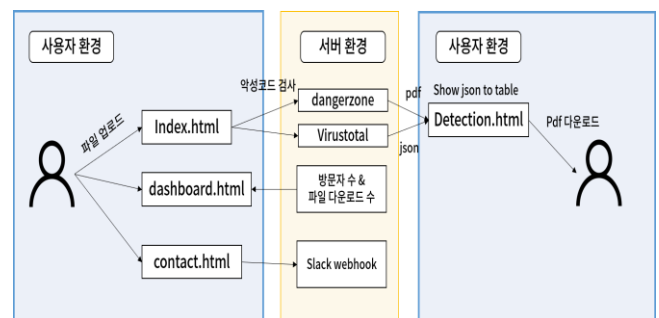
또한 대시보드를 통해 최근 15 일의 방문자 추이 및 파일 변환 현황을 나타낸다. 프로그램에 대한 지속적인 이용자들의 피드백을 위해 Contact 페이지를 개설하여 Slack으로 전달될 수 있도록 한다.

### 2-3. 기능 설계 - 데스크톱

프로그램은 Electron, NodeJS를 활용하였고 기존의 웹 애플리케이션과 별도로 데스크톱에 특화되어 있는 웹을 추가로 개발하였다. 사용자는 우클릭 실행 혹은 프로그램 직접 실행 두 가지 방법으로 파일을 반환받을 수 있다.

변환할 파일에서 우클릭을 실행하면 바로 데스크톱 프로그램으로 연결되어 안전한 PDF 파일로 반환된다. 또한 자체적으로 실행하여 파일을 변환한 후 로컬에 자동으로 저장되도록 한다.

### 2-4. 서비스 구성도 설계



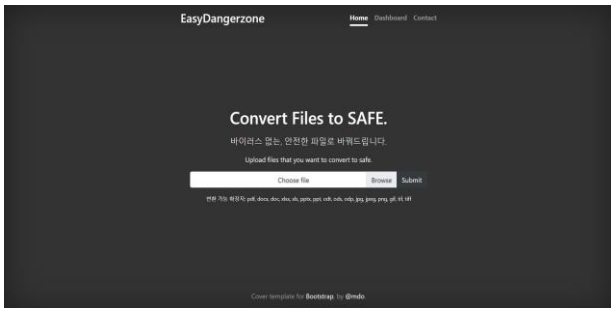
(그림 3) 서비스 구성도 설계.

## 3. 구현 결과

### 3-1. 웹 애플리케이션

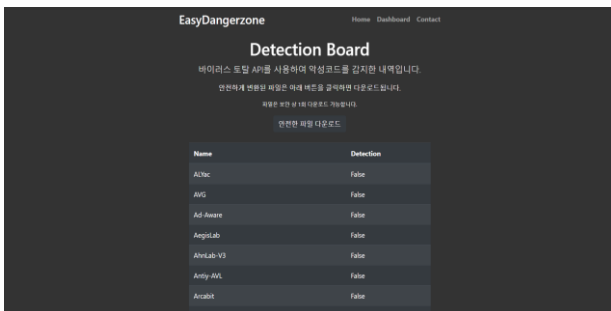
Django를 활용하여 서버와 전반적인 프로그램을 구성하였다.[2] 각 페이지를 구성하기 위해 Bootstrap을 활용하여 디자인하였다. 특히, Dangerzone 프로그램을 실제 서버에서 실행시키기 위해 GUI로 구현된 Dangerzone을 CLI 명령어로 변환하여 실행하는 과정을 거쳤다. 또한 CLI로 인해 중복되어 생성되는 파일들을 일정 주기로 삭제하여 이전 사용자들의 파일을 다음 사용자가 받아볼 수 없도록 구현하였다.

<sup>2</sup> VirusTotal. (n.d.). Retrieved September 27, 2020, from <https://www.virustotal.com/gui/home>



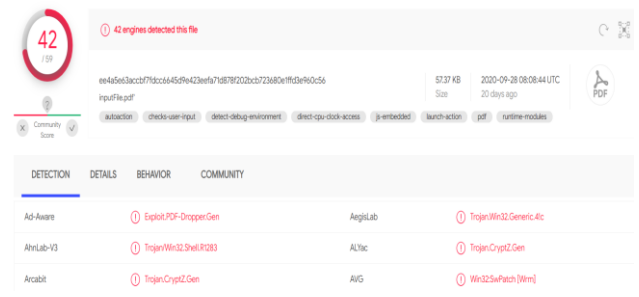
(그림 4) 웹 페이지 메인 화면(이하 EasyDangerzone)

웹 페이지는 EasyDangerzone 이라는 명칭으로 구현되었다. EasyDangerzone 의 핵심 기능인 파일 변환과 악성코드 검출 여부는 그림 5 와 같이 구현되었다. 사용자가 파일을 올릴 시, VirusTotal API 를 이용하여 파일을 전달하고 각종 바이러스 검출 프로그램을 거친 결과를 Detection Board 페이지에 별도 표시하도록 구현하였다. 또한 추가적으로 URLhaus 의 ClamAV signatures 파일 중 md5 해시키를 MySQL 데이터베이스에 저장하여, 업로드 된 파일의 해시키와 데이터베이스에 저장된 해시키 중 일치하는 것이 있다면 알람을 띄워주도록 구현하였다.

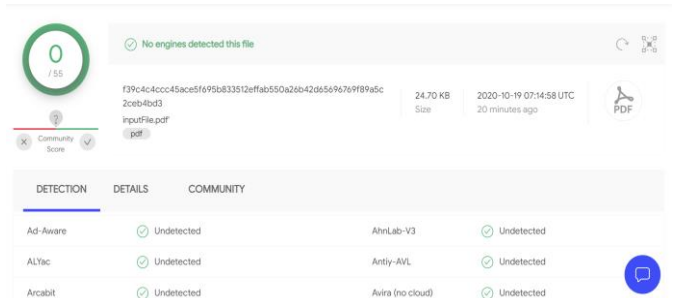


(그림 5) Detection Board

실제 EasyDangerzone 의 작동을 확인해보기 위해 악성코드에 감염된 파일을 이용하여 테스트 해 보았다. 그림 6 에서 볼 수 있듯, 우리가 사용한 파일은 트로이목마 악성코드에 감염된 파일임을 VirusTotal 을 통해 확인하였다. 이 파일을 EasyDangerzone 웹 애플리케이션에서 변환한 뒤 다시 VirusTotal 에서 분석해본 결과, 그림 7 과 같이 악성코드가 발견되지 않았다. EasyDangerzone 을 통해 안전성이 분명하지 않은 파일도 안전한 PDF 파일로 변환할 수 있음을 확인하였다.



(그림 6) 악성코드가 검출된 파일



(그림 7) EasyDangerzone 에서 변환된 파일의 바이러스 검출 여부

### 3-2. 데스크톱 프로그램

데스크톱 프로그램은 Flask 를 활용하였으며, 최소한의 기능만을 구현하였다. 사용자가 안전한 PDF 로 변환할 파일에서 그림 8 과 같이 우클릭하면 프로그램에서 Docker 를 실행하여 자동으로 변환되고, 이 후 로컬에 자동 저장되며 PDF 뷰어를 통해 오픈 된다.



(그림 8) 데스크톱 프로그램 우클릭 실행화면

또는, 사용자가 자체적으로 프로그램을 실행하면 그림 9 과 같이 올린 후에 PDF 파일을 반환 받도록 구현하였다.



(그림 9) 데스크톱 프로그램 실행 화면

### 참고문헌

- [1] 이창용/강홍구/이태진/정현철/원유재, 문서형 악성 코드 행위 분석 및 악성여부 탐지 시스템, 한국경영정보학회 2012 년 추계학술대회, 2012, 532-537
- [2] 김석훈, “파이썬 프로그래밍: Django(장고)로 배우는 쉽고 빠른 웹 개발, 한빛미디어, 2015

## 4. 결론 및 향후 연구

최근에도 문서형 악성코드에 대한 다양한 연구가 진행되고 있다. EasyDangerzone 시스템은 그의 일환으로 사용자들이 편리하게 접근하여 문서형 악성코드의 감염 여부를 판단하고, 예방하는 데 도움을 줄 수 있을 것이라 기대한다.

또한 웹 페이지의 이용으로는 어려운 보안 문서의 경우에 데스크톱 버전을 활용하여 기업 환경에서의 여러 유저들이 편리하게 사용할 수 있으리라 기대된다.

표 1 을 통해 Dangerzone 과 EasyDangerzone 의 차이를 확인할 수 있다.

	Dangerzone	EasyDangerzone
Docker 설치	PC 개별 설치	서버 설치
악성코드 검출의 확인	X	O
사용자의 피드백 전송	X	O
개발 형태	데스크톱	웹/데스크톱

(표 1) Dangerzone 과 EasyDangerzone 의 비교

향후 개발한 웹 애플리케이션 및 데스크톱 버전의 지속적인 개선이 이루어질 것이다. Detection board 의 개선을 통해 한눈에 바이러스 감염 여부를 알아볼 수 있도록 한다. 또한 Dangerzone 프로그램을 적극 활용하여 동시에 여러 개 파일을 변환할 수 있도록 하는 것을 목표로 한다. 그리고 개발된 프로그램을 오픈소스로 공개하여 다양한 개발자들의 적극적인 기여를 유도할 것이다.

[본 논문은 과학기술정보통신부 정보통신창의인재양성사업의 지원을 통해 수행한 ICT 멘토링 프로젝트 결과물입니다]