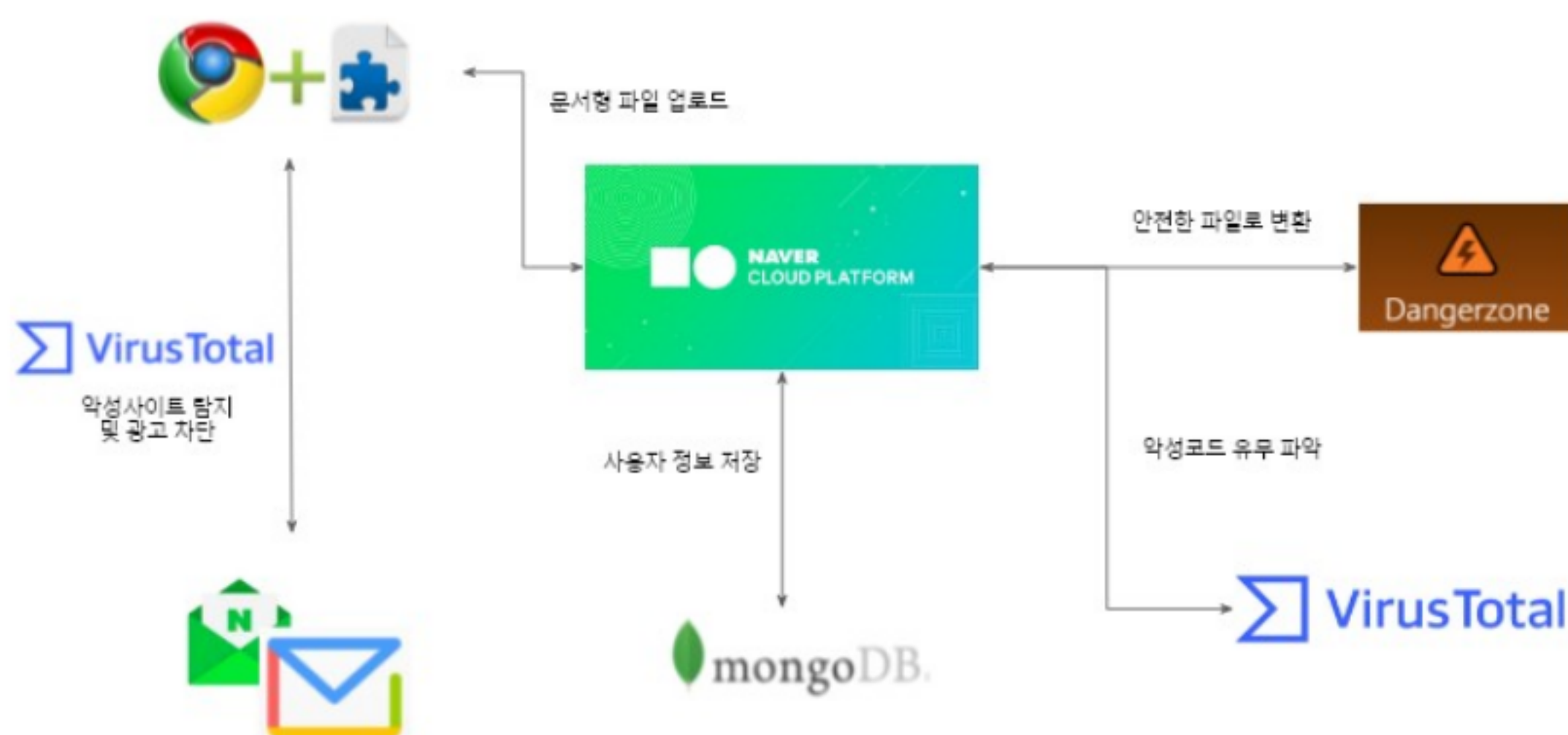


APT 멈춰!

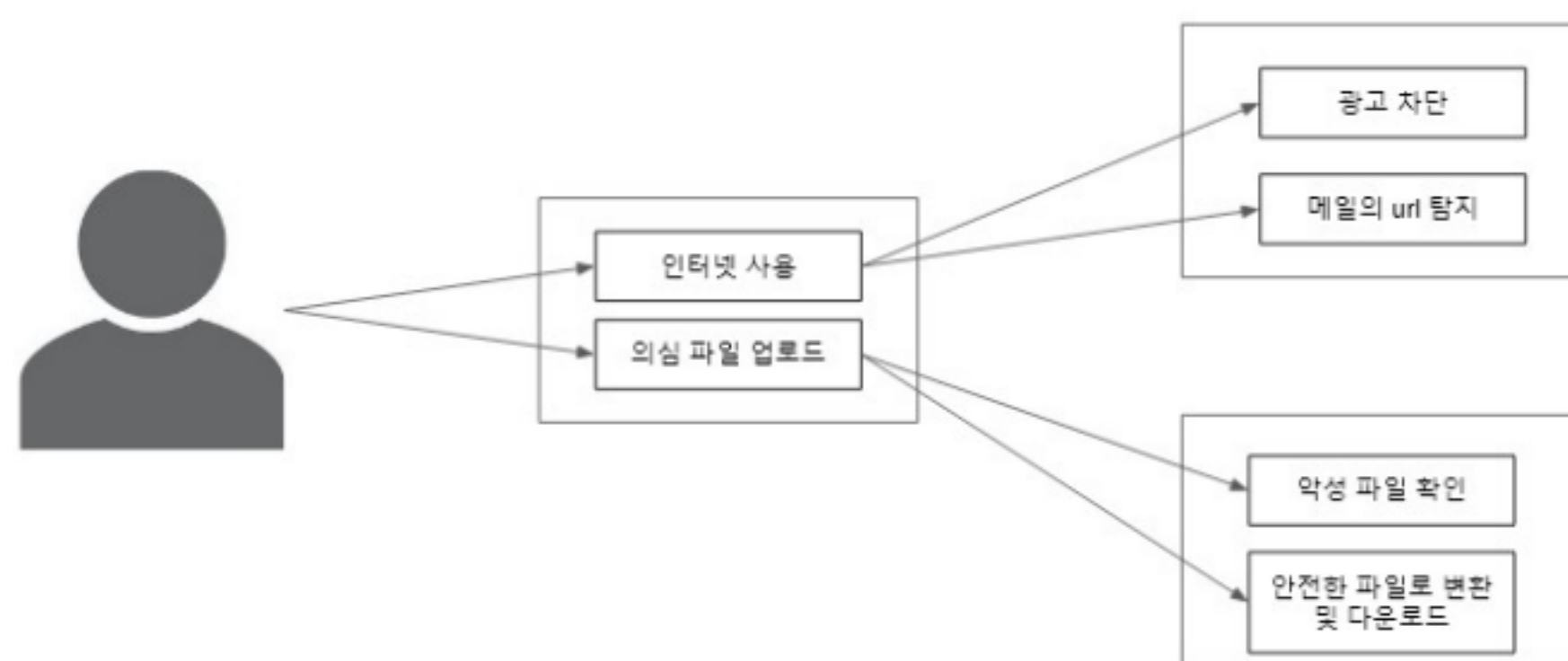
Team name	그만부르시조	
Professor	손태식	
Project Manager	김두원	201620630
Team Member	김희은	201821533
	성지훈	201620650
	한광석	201620643

The table of contents


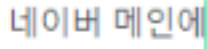
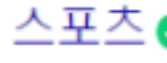

1. 요약[단원제목, 맑은 고딕, 16, 굵게].....	5
2. 개발 목표.....	6
3. 동기 및 기대효과.....	7
4. 기술 동향.....	8
4.1. 제품.....	8
가 지란지교시큐리티: SaniTOX.....	8
나 Dangerzone.....	9
다 McAfee WebAdvisor.....	9
4.2. 차별성.....	10
5. 예상 결과물 및 요구조건 분석.....	11
5.1. 시스템 구현 범위.....	11



.....	11
5.2. 사용자 서술.....	11
- 예상 사용자 : CHROME 을 사용하는 모든 사용자.....	11



.....	12
5.3. 입출력.....	12
1. 사용자가 CHROME EXTENSION 에 문서형 파일 업로드.....	12
□ 출력 : 사용자가 업로드한 파일의 내부데이터만을 뽑은 안전한 PDF 파일 생성.....	12
2. 사용자가 NAVER, DAUM 등의 이메일에서 특정 URL 에 ONMOUSEOVER(MOUSEHOVER) 이벤트가 발생할 경우.....	12

□ 출력 : VIRUSTOTAL API 와 EASYLIST 기반의 URL 분석을 바탕으로 한 알고리즘으로 해당 URL의 위험도 제공.....	12
    <div> 안전한 링크입니다 • 포털 사이트 사이트 보고서 보기 </div>	12
5.4. 기능적 요구사항.....	12
- HWP 파일 변환.....	12
□ HWP 파일 변환 시 HWP 파일의 악성 매크로 부분을 제외하고 그림 및 글만을 사용자가 확인할 수 있도록 해야 함.....	12
- 악성파일 탐지.....	12
□ 악성파일 탐지 시 안전한 파일인지, 안전하지 않은 파일이라면 어떤 악성 매크로가 포함되어 있는지 사용자가 확인할 수 있도록 해야 함.....	12
- 악성 URL 탐지.....	12
□ URL 분석기능 사용시 사용자가 브라우저 또는 이메일에서 URL에 접속하기 이전에 해당 URL에 대한 위험도를 확인할 수 있도록 해야 함.....	12
- 기록 저장.....	13
□ 기록 저장기능의 경우 사용자가 어떤 URL을 완전히 차단시키고자 하는 경우 해당사용자가 해당 URL에 대한 정보를 입력하여 완전히 차단될 수 있도록 해야 함.....	13
- 통합 기능.....	13
□ 통합 기능의 경우 파일업로드 기능과 URL 분석 및 차단 기능을 하나의 CHROME EXTENSION에서 모두 사용할 수 있도록 해야 함.....	13
5.5. 비기능적 요구사항.....	13
6. 개발 방법.....	14
7. 프로젝트 관리.....	15
7.1. 위험 요소 및 대처 방안.....	15
프로젝트를 진행하면서 발생할 수 있는 위험요소에는 악성 파일을 관리하면서 악성 코드 샘플에 감염될 위험이 있고, HWP 를 제외한 확장자 기능은 기존에 존재하는 DANGERZONE 에서 사용하기 때문에 해당 기능을 유지해야 하며, 정상 사이트를 차단하거나 위험 사이트를 오탐지 할 수 있다. 이를 해결하기 위해 최대한 고립된 환경인 SANDBOX 환경에서 기능 구현을 테스트하고, DANGERZONE 코드를 분석하고 해당 코드에서 HWP 변환을 추가하였으며, 최대한 많은 URL 테스트를 통해 여러 알고리즘을 테스트 해 보고 최대한 정확한 알고리즘을 설계할 것이다.	15
7.2. 역할 분담.....	15
7.3. 개발 일정.....	15
8. 참고 자료.....	18

1. 요약[단원제목, 맑은 고딕, 16, 굵게]



Figure 1. 2021년 2월 첫째 주 악성코드 통계[자료 = 보안뉴스]

APT(advanced persistent threat) 공격이란 잠행적이고 지속적인 컴퓨터 해킹 프로세스들의 집합으로 특정 실체를 목표로 행해지는 공격이다.¹ 이러한 APT 공격은 대개 스팸 메일과 위장된 배너 광고 등 다양한 방식을 통해서 이뤄진다. 대부분 송장, 선적 서류(Shipment Document), 구매 주문서(P.O.-Purchase Order) 등으로 위장한 스팸 메일을 통해 유포되기 때문에 파일 이름도 동일하게 위와 같은 이름이 사용된다. 그리고 이러한 정보탈취형(Infostealer) 공격이 가장 2020년 2월 첫째 주 가장 많이 발견된 악성 코드였다.²

Content Disarm & Reconstruction(이하 CDR)은 백신, 샌드박스에서 막아내지 못한 보안 위협에 대하여 파일 내 잠재적 보안 위협 요소를 원천 제거 후 안전한 파일로 재조합하여 악성코드 감염 위험을 사전에 방지할 수 있는 '콘텐츠 무해화 & 재조합' 기술이다. 글로벌 IT 자문기관 '가트너(Gartner)'에서는 첨부파일 형태의 공격에 대한 솔루션으로 CDR을 추천하고 있다.³

Open source로 공개된 CDR 기법을 사용하는 프로그램으로 'Dangerzone'이 있다. 해당 프로그램은 대부분의 문서 파일의 확장자를 지원하지만, 한국에서 많이 사용되는 HWP 파일의 확장자를 지원하지 않고 있다. 그리고 Gmail은 악성 URL을 1차적으로 차단해주지만 Naver, Daum 등의 메일 시스템에서는 악성 URL을 차단하지 않아 손쉽게 악성 URL을 유포할 수 있다.

이러한 문제점에서 착안하여 APT 공격을 예방하기 위한 HWP 확장자를 지원하는 'Dangerzone' 프로그램, Naver, Daum 메일 내 URL 검사, 배너형 광고 차단 기능을 수행하는 Chrome extension을 개발하는 프로젝트를 진행했다.

2. 개발 목표

Naver, Daum 메일을 통해 유포되는 URL 검사 및 알림 기능, 공격 벡터로 사용될 수 있는 배너형 광고 차단 기능, Dangerzone을 이용한 악성 문서 파일 변환 기능을 갖춘 Chrome extension 개발과, Dangerzone에 HWP 확장자 변환 기능을 추가하는 것을 개발 목표로 한다.

¹ 위키백과 “지능형 지속 공격”

² 보안뉴스 “2월 첫째 주 가장 많이 발견된 악성코드, 1위 정보탈취형 ‘AgentTesla’”

³ 지란지교시큐리티 SaniTOX

URL 위험도 알림



악성 파일 검사 및 안전한 파일 변환

Browse and Upload

Detection Board	
바이러스 토탑 API를 사용하여 악성코드를 감지한 내역입니다.	
안전하게 변환된 파일은 아래 버튼을 클릭하면 다운로드됩니다.	
파일은 보안 상 1회 다운로드 가능합니다.	
안전한 파일 다운로드	
Name	Detection
AlYac	False
AvG	False
Ad-Aware	False
AvastLab	False
AhnLab-V3	False
Antiy-AVL	False
Arcabit	False
Avest	False
Avira	False
Baidu	False

Figure 2. 예상 결과물

3. 동기 및 기대효과

사용자가 쉽게 접할 수 있는 메일에서 송장, 구매주문서 등으로 위장한 악성파일 및 스팸메일에 포함된 사이트, 그리고 공격 벡터로 사용될 수 있는 수많은 배너형 광고들은 일반 사용자들이 쉽게 접할 수 있다. 또한 우리나라의 정부 기관, 민간 기업에서 많이 사용하는 HWP, MS office의 문서형 악성코드가 아직도 많다는 뉴스를 보고 DangerZone 기반의 악성파일 변환, 메일 검사 및 광고차단의 기능을 가진 APT 방어를 위한 Chrome extension을 기획하게 되었다.

이 프로젝트로 인한 기대효과는 기술적, 경제적, 사회적 이득으로 나눌 수 있다. 먼저 기술적 기대효과로는 악성코드를 지닌 문서 내부 데이터를 확인할 수 있다는 점, HWP, Ms office 등 다양한 확장자 변환 기능을 제공한다는 점, 악성사이트 차단 및 사이트별 위험도 확인 기능을 제공한다는 점이 있다. 경제적으로는 Chrome extension 상용으로 사용자에게 높은 접근성과 편의성을 제공하여 많은 사용자들을 위험으로부터 지킬 수 있고 오픈소스로 무료로 사용 및 편의에 따라 개량도 가능하다. 마지막으로 사회적 기대효과는 APT 공격 예방을 해준다는 기대효과가 있다.

[보안뉴스 권 준 기자] 설날 연휴를 앞두고 있던 2021년 2월 첫째 주에는 인포스틸러(정보탈취) 유형의 악성코드가 가장 많이 발견된 것으로 집계됐다.

보안전문 업체 안랩의 ASEC 분석팀이 ASEC 자동 분석 시스템 'RAPIT'를 활용해 2월 1일부터 7일까지 발견된 악성코드를 분석한 결과, 인포스틸러 악성코드인 'AgentTesla'가 1위를 차지했고, 2위와 3위도 인포스틸러 악성코드인 'Formbook', 'Lokibot'이었던 것으로 드러났다.

Figure 3. 보안뉴스 최근 악성코드 유형

4. 기술 동향

4.1. 제품

지능화된 악성위협이 증가함에 따라 샌드박스 회피 및 우회하는 기술이 증가하고 있는 세로 샌드박스만으로는 지능화된 위협에 대응하는데 한계를 나타내고 있다. 이에 가트너(Gartner)가 발표한 회피성이 높은 공격으로부터 보호하기 위한 5 가지 핵심 보안 패턴 중 하나로 CDR 기법이 있다. APT 공격을 방지하기 위해 많은 백신 프로그램이 존재하지만 CDR 기능을 지원하고 메일을 통해 유포되는 URL을 검사하는 기능을 지원하는 경우는 드물다. 현재, 실제로 운영되고 있는 CDR 기법을 지원하는 프로그램과 URL 검사를 지원하는 프로그램에 대한 분석은 다음과 같다.

가 지란지교시큐리티: SaniTOX

지원 환경 및 파일형식					
 지원 운영체제 • CentOS 6, 7/64bit • Python 2.6 / 2.7		 지원 파일 • MS Office 2003 / 2007+ • 한글(HWP) • PDF • RTF • 압축파일(ZIP) • Image(JPG, JPEG, BMP, PNG, TIF, TIFF)			
콘텐츠 \ 파일형식	MS Office 2003	MS Office 2007+	HWP	PDF	
JavaScript	-	-	○	○	
Embeddedfiles	○	○	○	○	
Macro(VBA script)	○	○	-	-	
OLE Package	○	○	○	-	
DDE	○	○	-	-	
Link	○	○	-	○	
Media	○	○	○	○	
Attach files	○	○	○	○	

Figure 4.지란지교 시큐리티 SaniTOX 지원 환경 및 파일형식

국내에서 CDR 기법을 지원하는 대표적인 프로그램은 지란지교시큐리티의 SaniTOX이다. 지란지교시큐리티의 SaniTOX는 파일 내 실행 가능한 액티브 콘텐츠를 원천 제거 후 안전한 파일로 재조합해 알려지지 않은 보안 위협에 대응할 수 있는 콘텐츠 악성코드 무해화 솔루션이다. Web 형식으로 이용이 편리하고 HWP, MS Office, PNG 등 많은 확장자를 지원한다. 그렇지만, linux에서 사용되는 odt 등의 확장자를 지원하지 않고 모든 기능을 사용하기 위해선 요금을 지불해야 한다.

나 Dangerzone

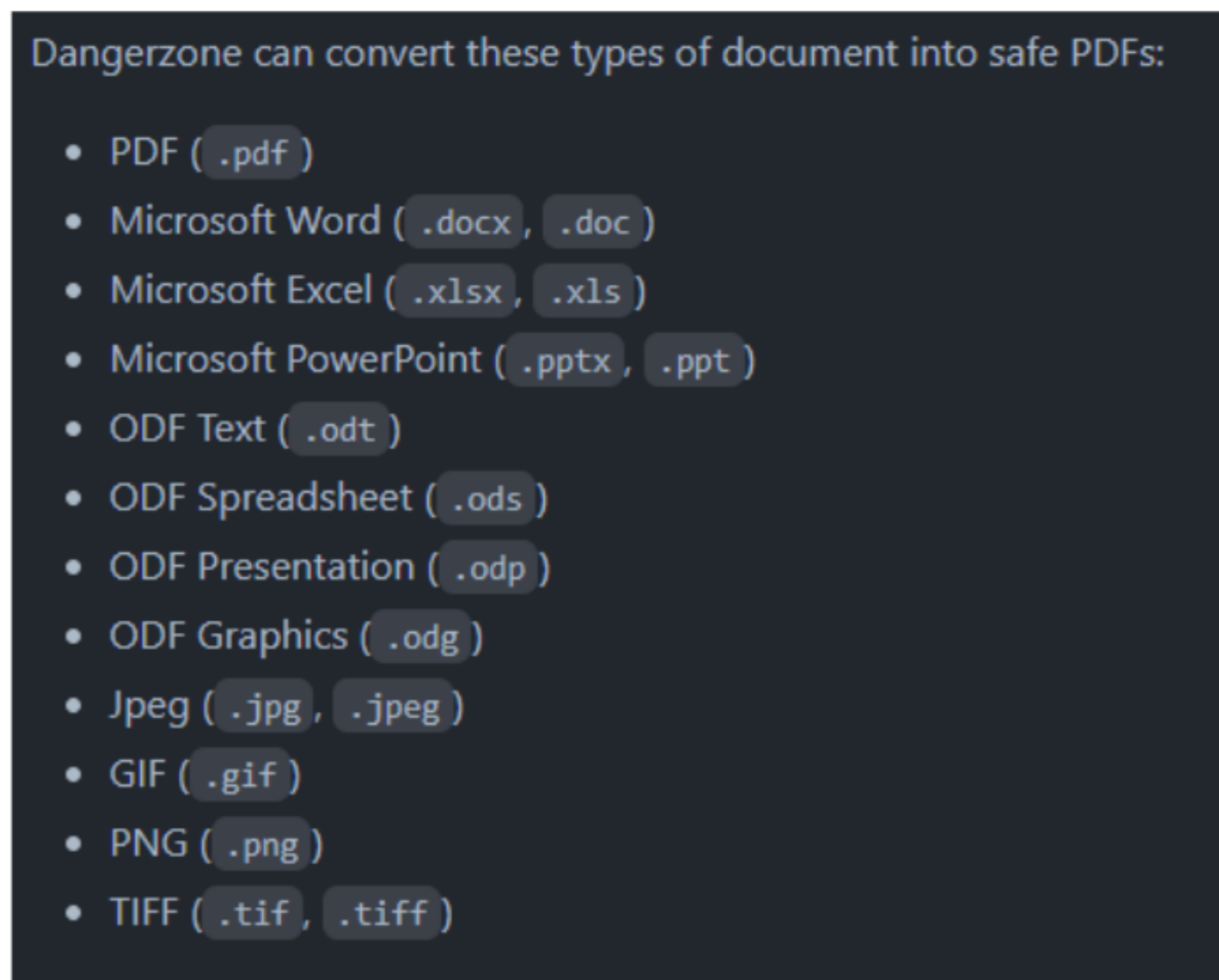
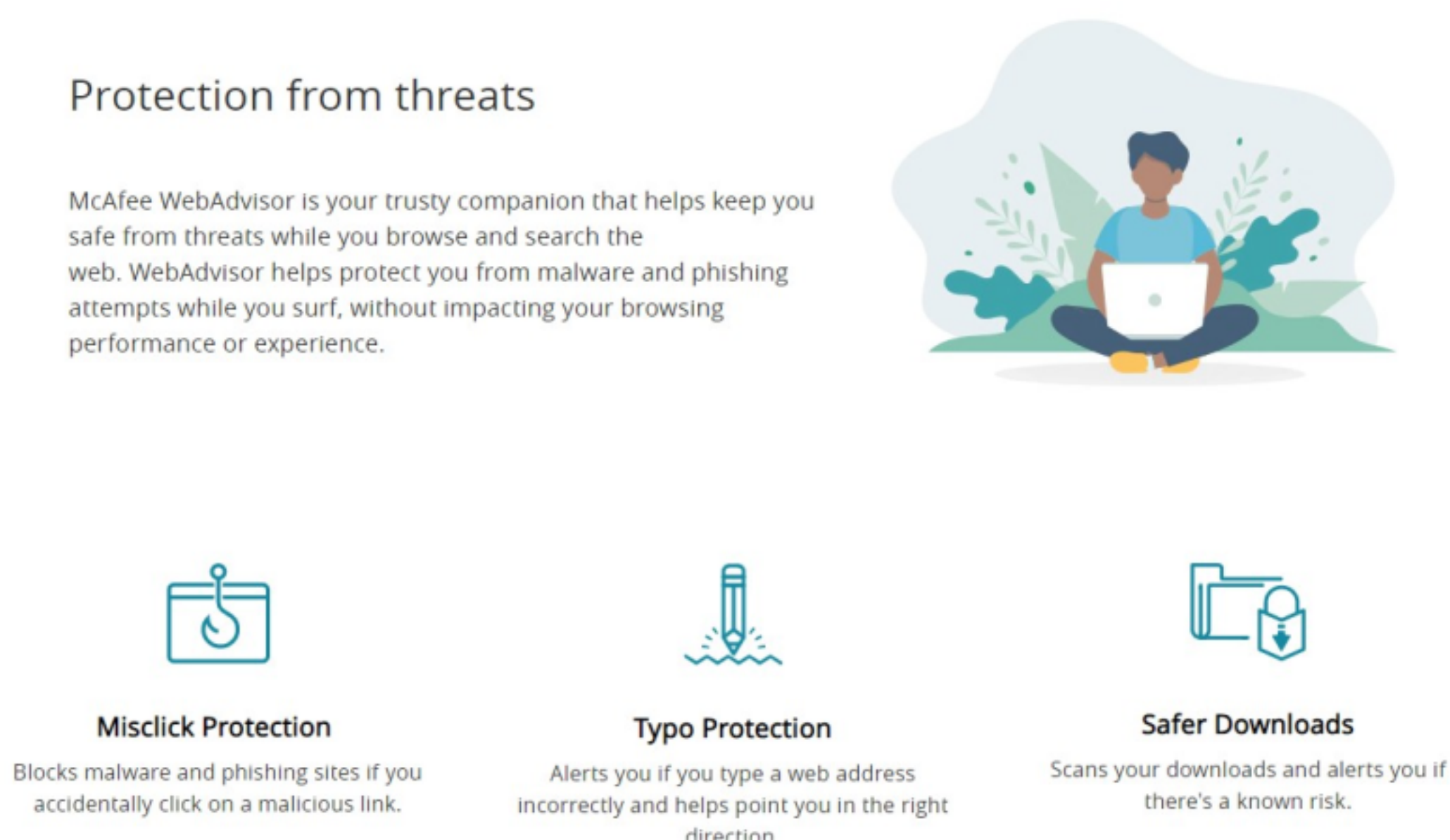


Figure 5. Dangerzone 지원하는 확장자

현재 github에 공개되어 있는 CDR 기법을 적용한 프로그램으로 'Dangerzone'이 있다. 해당 프로그램은 pixel 렌더링을 통해 안전한 flat PDF 파일로 바꾸는 것으로 무료로 사용이 가능하다. 하지만 사용하기 위해서는 docker와 'Dangerzone'을 local machine에 설치해야 되고 한국에서 많이 사용되는 HWP 확장자를 지원하지 않는다.

다 McAfee WebAdvisor



APT 멈춰!

Figure 6. McAfee WebAdvisor 기능

McAfee WebAdvisor는 피싱 사이트에 들어가거나 악성 파일 링크를 잘못 클릭했을 때 block 한다. 또한, 파일을 내려 받을 때 악성 코드 유무 검사를 진행해준다. 그리고 Chrome extension으로 사용해 편리함도 제공해준다. 그렇지만 메일 내 URL을 검사해주는 기능이 없어 Naver, Daum 메일 시스템을 통해 악성 URL 유포 하는 것이 비교적 수월해질 수 있다.

4.2. 차별성

<표 1> 기존 제품과의 차별성

제품	HWP	Open Document Format	안전한 파일 변환	악성 코드 유무	편리한 사용	Mail URL 검사
Dangerzone	X	O	O	X	X	
SaniTox	O	X	O	O	X	
Mc Afee 웹어드바이저				O	O	X
Our Project	O	O	O	O	O	O

CDR 기법을 사용하는 'Dangerzone'은 Docker와 'Dangerzone' 다운로드가 필요해 사용에 불편함이 있고, 한국에서 많이 사용되는 HWP 확장자를 지원하지 않으며 해당 파일이 악성코드를 가졌는지 알려주지 않는다.

SaniTox는 web, cloud 형태로 제공되어 편리하지만 유료라는 점에서 결제해야 하는 번거로움이 있고 linux 환경에서 사용되는 Open Document 확장자(odt, ods, odp, odg)를 지원하지 않는다.

McAfee WebAdvisor는 Chrome extension이고 무료로 편리하게 사용이 가능하나 웹 브라우저를 통해 연결된 URL의 악성 유무를 판단해 줄 뿐 mail을 통해 전달되는 URL을 검사하지는 않는다. Gmail은 자체적으로 피싱 사이트를 차단하지만 Naver, Daum에서는 차단 없을 하지 않는다.

이에 본 프로젝트에서는 앞의 단점들을 보완하여 HWP 기능을 지원하고 무료로 편리하게 CDR 기법을 사용할 수 있는 것과 메일 내 URL을 검사할 수 있는 것에 차별성을 두었다.

5. 예상 결과물 및 요구조건 분석

5.1. 시스템 구현 범위

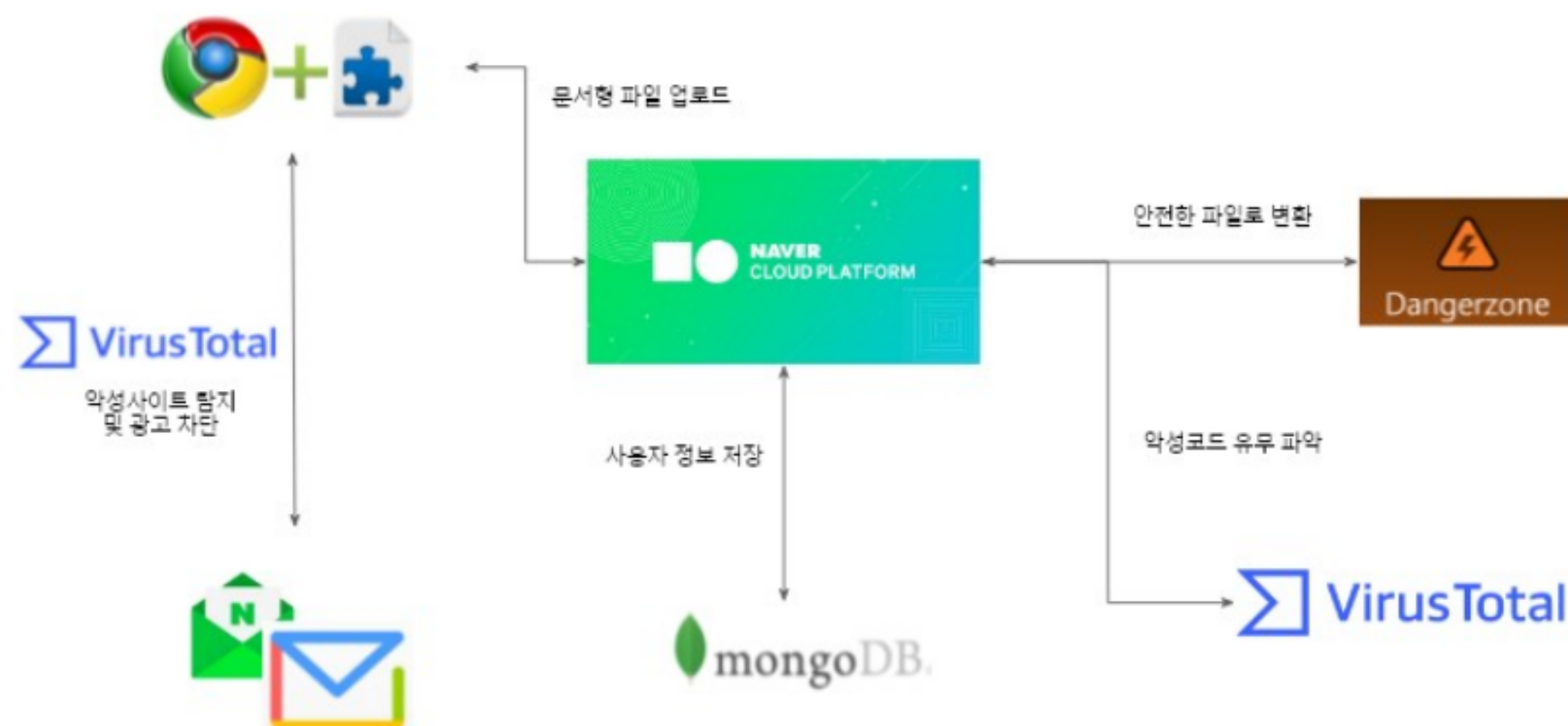


Figure 7. System Structure

본 프로젝트는 기본적으로 사용자가 사용할 Chrome에서 나타날 UI를 위해 HTML과 JavaScript를 함께 사용하고 있으며 Dangerzone, VirusTotal API, Naver Cloud Platform을 사용하고 있다.

본 프로젝트에서 제공하는 URL 위험도 분석은 크롬 extension을 바탕으로 구현되어 있으며 naver, daum 메일로 전달된 URL을 virustotal을 통해 검사하여 사이트에 포함된 위험요소 여부를 사용자에게 제공하며 Chrome Extension API와 EasyList에서 제공하는 URL을 바탕으로 배너형 광고를 차단한다. 또한 크롬 extension을 이용하여 사용자가 파일을 업로드 하면 미리 구축해놓은 Server로 파일을 받아 hwp 확장자가 추가된 dangerzone을 통해서 안전한 파일로 변환하고 Virustotal을 통해 검사하여 파일에 포함된 악성코드 유무를 사용자에게 제공한다. 서버로는 naver cloud를 통해 ubuntu server 18.04 버전을 사용한다. 서버의 사양으로는 vCPU 1개, RAM 1GB, DISK 50GB이다. 그리고 사용자를 관리하기 위해 mongoDB를 사용한다.

5.2. 사용자 서술

- 예상 사용자 : Chrome을 사용하는 모든 사용자
- 사용 시나리오 : 사용자는 인터넷을 사용하면서 배너형 광고 및 광고 사이트 자체 차단기능을 제공하는 AdBlock 기능을 기본적으로 사용 가능하고 메일이나 인터넷 서핑을 하며 url에 접속하기 전 사이트의 위험도를 사전에 파악할 수 있다. 또한 위험도를 지니고 있지만 내부 데이터가 필요해서 받은 파일이 존재한다면 이러한 파일들을 미리 구축한 서버로 보내 악성 파일인지 확인을 할 수 있고 악성 파일이라면 안전한 파일로 변환한 파일을 다운로드 하여 내부 데이터를 확인할 수 있다.

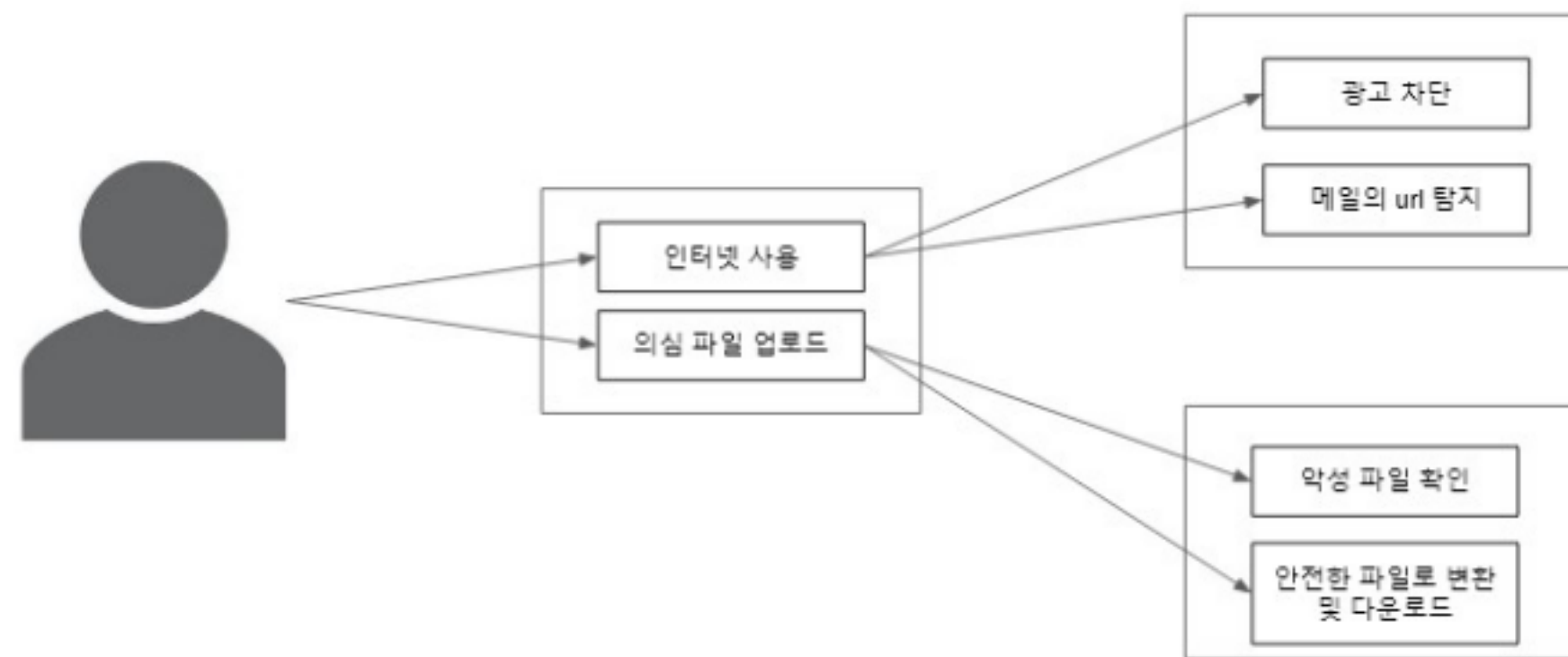


Figure 8. Use Case

5.3. 입출력

1. 사용자가 Chrome Extension 에 문서형 파일 업로드
 - 출력 : 사용자가 업로드한 파일의 내부데이터만을 뽑은 안전한 PDF 파일 생성
2. 사용자가 Naver, Daum 등의 이메일에서 특정 URL 에 onMouseover(MouseHover) 이벤트가 발생할 경우
 - 출력 : VirusTotal API 와 EasyList 기반의 URL 분석을 바탕으로 한 알고리즘으로 해당 URL 의 위험도 제공



Figure 9. URL 검사 예시

5.4. 기능적 요구사항

- HWP 파일 변환
 - HWP 파일 변환 시 HWP 파일의 악성 매크로 부분을 제외하고 그림 및 글만을 사용자가 확인할 수 있도록 해야 함
- 악성파일 탐지
 - 악성파일 탐지 시 안전한 파일인지, 안전하지 않은 파일이라면 어떤 악성 매크로가 포함되어 있는지 사용자가 확인할 수 있도록 해야 함
- 악성 URL 탐지
 - URL 분석기능 사용시 사용자가 브라우저 또는 이메일에서 URL 에 접속하기 이전에 해당 URL 에 대한 위험도를 확인할 수 있도록 해야 함
- 기록 저장
 - 기록 저장기능의 경우 사용자가 어떤 URL 을 완전히 차단시키고자 하는 경우 해당사용자가 해당 URL 에 대한 정보를 입력하여 완전히 차단될 수 있도록 해야 함
- 통합 기능
 - 통합 기능의 경우 파일업로드 기능과 URL 분석 및 차단 기능을 하나의 Chrome extension 에서 모두 사용할 수 있도록 해야 함

5.5. 비기능적 요구사항

- Usability(사용성)
 - 기존 Dangerzone 의 기능을 모두 사용할 수 있어야 한다.
- Reliability(신뢰성)
 - 파일 변환시 악성코드에서 완전히 벗어난 파일을 제공하여야 하며 URL 의 위험도를 정확하게 제공해야 한다.
- Performance(기능성)
 - 사용자의 접근성을 위해 Chrome extension 을 사용하며 성능 저하가 없어야 한다.

6. 개발 방법

6.1. 개발 환경

- Python
 - Python 을 사용해 OpenSource 인 Dangerzone 에 한글 확장자 추가
 - Python 을 사용해 VirusTotal API 를 사용하여 악성 파일인지 아닌지에 대한 여부와 URL 위험도 탐지에 사용함
- Ubuntu Server 18.04
 - 사용자가 파일을 업로드하면 해당 파일을 안전한 PDF 로 변환시키는 작업을 하는 서버로 Ubuntu Server 를 사용하였음
- Chrome Extension
 - Chrome Extension 개발을 위해 Javascript 및 HTML 을 사용
- MongoDB
 - 사용자 관리를 위한 데이터베이스로 MongoDB 사용

6.2. 개발에 활용되는 지식 및 기술

- Dangerzone
 - DOCX, PPTX, XLSX, ODT 등 다양한 문서 확장자를 가진 파일을 안전한 파일로 변환한다.
- Docker
 - 악성 파일을 열고 안전한 파일로 변환할 때 공격당하는 것을 방지하기 위해 네트워크가 분리된 독립적인 공간을 제공한다.
- VirusTotal API
 - 악성파일 탐지 : 사용자가 업로드한 파일이 악성파일인지 아닌지 판별하고 악성파일이라면 어떤 위험을 가지고 있는지 알려준다.
 - URL 탐지 : 사용자가 접속하고자 하는 URL 이 위험도를 가지고 있는지 판별하고 사용자에게 제공한다.
- Chrome Extension API
 - onBeforeRequest : Chrome Extension 사용중에 발생하는 웹 요청에 대해 요청이 발생하기 직전에 동작한다. 사용자가 URL 에 접속하기 이전에 Chrome Extension 이 이를 먼저 탐지해 배너형 광고 등을 차단시킨다.

7. 프로젝트 관리

7.1. 위험 요소 및 대처 방안

프로젝트를 진행하면서 발생할 수 있는 위험요소에는 악성 파일을 관리하면서 악성 코드 샘플에 감염될 위험이 있고, HWP 를 제외한 확장자 기능은 기존에 존재하는 Dangerzone 에서 사용하기 때문에 해당 기능을 유지해야 하며, 정상 사이트를 차단하거나 위험 사이트를 오탐지 할 수 있다. 이를 해결하기 위해 최대한 고립된 환경인 sandbox 환경에서 기능 구현을 테스트하고, Dangerzone 코드를 분석하고 해당 코드에서 HWP 변환을 추가하였으며, 최대한 많은 URL 테스트를 통해 여러 알고리즘을 테스트 해 보고 최대한 정확한 알고리즘을 설계할 것이다.

7.2. 개발 일정

개발 일정으로는 3 월엔 아이디어 제안 및 광고 차단, hwp 변환 기능 구현, 파일 업로드 구현 등 미니 프로젝트를 실시하며 기본적인 프로그램 틀을 만들고, 4 월에는 hwp 변환 기능을 Dangerzone 에 통합, 파일 다운로드 구현, URL 검사 구현을 진행하며, 5 월에는 Sandbox

환경으로 Dangerzone 구현, URL 위험도 UI 디자인, Virustotal 활용, MongoDB 구축을 한 뒤 코드를 통합함으로써 개발을 완료할 예정이다.

7.3. 역할 분담

역할 분담은 크게 Dangerzone 추가 기능 구현과 url 검사 및 광고 차단 두 가지로 나뉘어서 진행했다.

이름	역할
김두원	<ul style="list-style-type: none"> - Chrome extension BE/FE - 사용자 관리 - Mongo DB - 아이디어 제안 발표
한광석	<ul style="list-style-type: none"> - Dangerzone 분석 및 HWP 추가 - Virustotal 활용 - Sandbox 구현 - Docker - 최종 발표
성지훈	<ul style="list-style-type: none"> - 사용자 UI 설계 및 연동 - Chrome extension API 연동 - Virustotal API 활용한 알고리즘 설계 - 미니프로젝트, 제안서 발표
김희은	<ul style="list-style-type: none"> - 악성 URL 분석 기능 구현 - 광고 차단 기능 구현 - 설계서 발표

8. 참고 자료

- <https://www.virustotal.com/>
 - <https://developer.chrome.com/docs/extensions/reference/>
 - <https://github.com/firstlookmedia/dangerzone-converter>
 - <https://pythonhosted.org/pyhwp/ko/>
 - <https://wkhtmltopdf.org/>
- 위키백과, “APT 공격”
https://ko.wikipedia.org/wiki/%EC%A7%80%EB%8A%A5%ED%98%95_%EC%A7%80%EC%86%8D_%EA%B3%B5%EA%B2%A9
- 보안뉴스 “2 월 첫째 주 가장 많이 발견된 악성코드, 1 위 정보탈취형 ‘AgentTesla’”
<https://www.boannews.com/media/view.asp?idx=94881&page=1&kind=1>
- 지란지교시큐리티 SaniTOX, <https://www.jiransecurity.com/products/sanitox>
- McAfee Webadvisor
<https://www.mcafee.com/en-us/safe-browser/mcafee-webadvisor.html>