[양식 2] 아이디어 제안서

2021 융합 캡스톤 디자인 공모전

아이디어 제안서

작품명	APT 멈춰 !
참가팀명	yuk-jo

1. 아이디어 개요

APT(advanced persistent threat) 공격이란 잠행적이고 지속적인 컴퓨터 해킹 프로세스들의 집합으로 특정 실체를 목표로 행해지는 공격이다. 이러한 APT 공격은 대개 스팸 메일과 위장된 배너 광고 등 다양한 방식을 통해서 이루어 지며 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 20201년 2월 첫째 주 가장 많이 발견된 악성코드였다.

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.

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.

이번 아이디어에서는 APT 공격으로 사용될 수 있는 악성 URL과 악성 파일을 예방하는 Chrome extension을 개발한다. 해당 Chrome extension은 크게 2가지 기능을 가지고 있는데, 첫 번째 기능으로는 CDR 기법을 활용한 악성 파일 변환이고 두 번째 기능은 메일 내에 존재하는 링크의 URL을 검사하는 것이다 ‘Dangerzone’ open source를 활용해 HWP확장자를 지원하는 ‘Dangerzone’ 프로그램을 이용해 악성 파일을 안전한 PDF파일로 변환하고 VirusTotal API를 활용해 Naver, Daum 메일을 통해 유포되는 URL을 검사하고 알림을 제공한다.

2. 아이디어 설명

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.

국내에서 CDR 기법을 지원하는 대표적인 프로그램은 지란지교시큐리티의 SaniTOX이다. 지란지교 시큐리티의 SaniTOX는 파일 내 실행 가능한 액티브 콘텐츠를 원천 제거 후 안전한 파일로 재조합해 알려지지 않은 보안 위협에 대응할 수 있는 콘텐츠 악성코드 무해화 솔루션이다. Web형식으로 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.

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.

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 유포하는 것이 비교적 수월해질 수 있다.

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

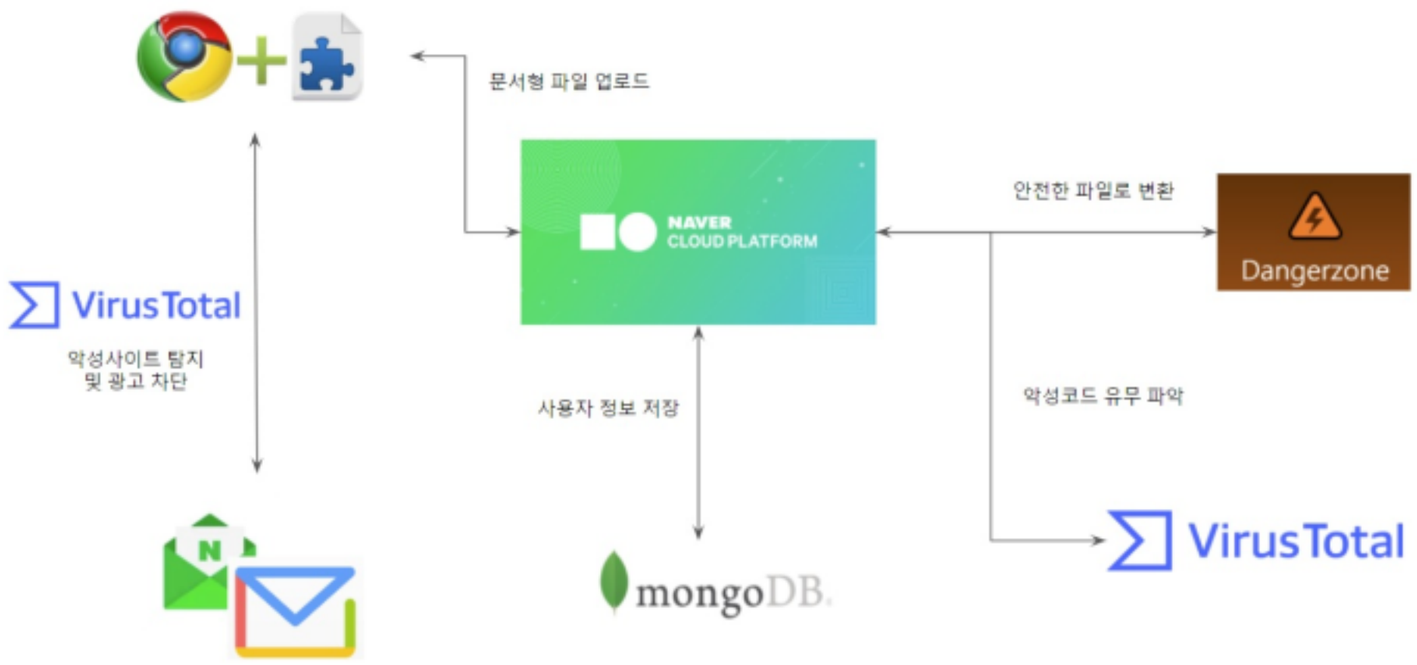
SaniTox는 web, cloud 형태로 제공되어 편리하지만 유료라는 점에서 결제해야 하는 번거로움이 있고 linux 환경에서 사용되는 Open Document 확장자(odt, ods, odp, odg) 를 지원하지 않는다.

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.

3. 주요 구성 및 설계

그림 1 설계도



아이디어를 구현하기 위한 설계도는 위와 같으며 총 3부분으로 나뉜다. 안전한 파일로 변환하고 악성 코드 리스트 보고서를 반환하는 부분, MongoDB를 통해 사용자를 관리하는 부분, mail 내에 존재하는 URL을 검사하고 공격 벡터로 사용될 수 있는 배너형 광고를 차단하는 부분이다.

악성 파일을 안전한 파일로 변환하는 부분에서 Dangerzone Open source에 HWP 확장자를 추가한 docker container를 Naver Cloud에서 생성한 Ubuntu server 18.04 LTS 운영체제 위에서 운영한다. CDR 기법으로 변환한 파일뿐만 아니라 VirusTotal API를 이용해 변환하려는 파일이 가진 악성코드 리스트의 보고서를 사용자에게 전달한다.

변환한 파일과 보고서가 다른 사용자에게 전달되는 것을 방지하기 위해 MongoDB를 사용해 사용자 정보를 관리한다.

마지막으로 EasyList에서 제공하는 URL을 Chrome Extension API를 사용해 배너형 광고를 차단하고 VirusTotal API과 Chrome Extension API를 사용해 메일로 전달되는 URL을 검사하고 위험도를 제공한다.

Python의 pyhwp 모듈과 wkhtmltopdf 모듈을 사용해 HWP 파일을 PDF 파일로 바꾸는 것이 가능하다. Chrome extension API와 VirusTotal API를 활용해 배너형 광고를 차단하고 악성 파일과 URL을 검사하고, Chrome extension으로 사용자에게 제공한다. 이를 바탕으로 본 프로젝트의 제작하고 시현한다.

4. 예산 계획

프로젝트의 예산 계획은 아래의 표와 같다. 본 프로젝트에서는 Dangerzone 서버를 유지하기 위한 서버 유지비 예산과, chrome extension 기반 프로그램 구축을 위한 웹 프로그래밍 관련 도서 구입 예산 및 회의비용이 필요하다.

세부 항목	사용 금액(원)
회의비	160,000
서버 유지비	400,000
문헌 구입비	30,000
총합	590,000

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.

§