오픈소스 기반 APT 공격 예방 Chrome extension

AJOU SOFTCON 2021-1

팀 명 Yuk-jo

팀 원 김두원, 김희은, 성지훈, 한광석

지도교수 손태식

멘 토 이규호

개발 동기 및 목적

2021년 2월 첫째 주 악성코드 통계[자료 = 보안뉴스]

APT 공격은 주로 메일에서 송장, 구매주문서 등으로 위장한 악성파일 및 악성 URL, 그리고 공격 벡터로 사용될 수 있는 수많은 배너형 광고들을 통해 이루어진다. Gartner에서는 첨부 파일 형태의 공격에 대한 솔루션으로 CDR(Content Disarm & Reconstruction) 기법을 권고하고 있다. CDR 기법을 사용하는 오픈소스 프로젝트인 'Dangerzone'이 존재하지만 HWP 확장자를 지원해주지 않는다. 또한, 손쉽게 메일 URL을 사전에 검사하는 제품이 존재하지 않는다. 이러한 문제점에서 착안하여 Chrome extension을 활용한 손쉬운 APT 예방 프로그램을 개발하였다.

주요 기술

1. 사이트 및 배너 차단

기본적으로 웹 Request를 기준으로 해당 URL이 EasyList의 목록에 존재하거나 광고와 관련된 특정 키워드를 포함할 시 해당 배너는 사용자에게 보이지 않도록 차단한다.

2. 사이트 위험도 검사

URL Scan 기능은 기본적으로 네이버, 다음 등의 메일에 포함된 악성 URL을 탐지하기 위해서 만들었지만 메일 이외에도 URL Scan이 가능하다. 사용자가 URL scan을 시도하면 Chrome Extension은 해당 URL을 받아 서버로 전달하고, 서버에서 해당 URL을 VirusTotal API를 사용하여 분석한다.

3. CDR(Content Disarm & Reconstruction)

파일 내 실행 가능한 Active Content를 제거하거나 비활성화 하기위해 오픈소스인 'Dangerzone'을 활용한다. 'Dangerzone'에서 지원하는 기능에 HWP 확장자를 추가해 CDR 기능을 구현했다. 먼저 파일이 서버로 전송되면 해당 파일은 PDF 파일로 변환된다. 변환된 PDF 파일은 페이지 별로 분할한 뒤 pdftocairo, gm, pdfunite 툴을 통해 안전한 PDF 파일로 변환된다. 만약 searchable PDF파일을 원한다면 OCR 기능을 수행하는 tesseract 툴을 사용한다.

4. 악성코드 탐지 보고서

의심 파일이 서버로 전달 됐을 때 VirusTotal API를 사용해 파일을 검사하고 부트 스트랩 프레임워크를 사용해 사용자에게 알기 쉽게 그 결과를 보여준다.

개발 내용

APT 공격으로 사용될 수 있는 배너형 광고, 악성 URL과 파일을 예방하는 Chrome extension을 개발했다. 해당 Chrome extension은 크게 3가지 기능을 가지고 있다. 먼저, 의심 파일을 서버로 전달하고, 변환된 안전한 파일과 파일 검사 결과를 받는다. 두 번째 기능은 의심 파일을 서버로 전달하고 서버에서 해당 URL을 검사하여 Chrome extension에 전달한다. Chrome extension은 전달된 결과에 따라 '안전 / 의심 / 위험 / 매우 위험 ' 페이지를 사용자에게 보여준다. 마지막으로 공격 벡터로 사용될 수 있는 배너형 광고를 EasyList와 Chrome extension API를 사용해 차단한다.

서버는 Ubuntu 18.04 LTS를 사용했으며, backend 프레임워크로 django를 사용하였다. Chrome extension으로부터 의심 URL을 받았을 때, 서버에서는 VirusTotal API를 활용해 해당 URL을 검사하고 그 결과를 전처리하여 돌려준다.

그리고 의심 파일을 받았을 때, Docker를 이용해 의심 파일을 안전한 파일로 변환하고 VirusTotal API를 활용해 해당 파일을 검사한다. 변환된 결과와 검사 결과는 의심 URL과 마찬가지로 Chrome extension으로 돌려준다.

결과 및 분석

'Dangerzone'에 HWP 기능을 추가하고 메일에 포함된 URL을 검사하는 기능과 배너형 광고를 차단하는 기능을 Chrome extension을 통해 구현함으로써 보다 편리하게 APT 공격을 예방할 수 있다. 해당 프로그램 이용 대상은 분야를 가리지 않고 일반인, 회사원, 공무원 등 많은 사람들이 사용할 수 있다.

또한 해당 프로젝트는 MIT license를 따르고 있어 어떠한 개발자도 오픈 소스 여부에 관계 없이 customizing 하여 재배포가 가능하며, 더불어 오픈 소스에 기여할 수 있다는 기대 효과를 얻을 수 있다.

끝으로 시간이 지남에 따라 서버 사양은 증가하고 악성 코드를 탐지하는 머신 러닝 모델이 등장하면서 속도 및 성능 향상을 기대하여 더욱 빠른 파일 검사와 파일 변환이 이뤄질 것이라 기대할 수 있다. 그리고 HWP와 마찬가지로 각국에서 자주 사용하는 파일 확장자를 추가함으로써 더 많은 파일 확장자를 지원하는 Dangerzone을 기대할 수 있다.