ICBM

Intelligent Compression for Binary Malware

임하늘, 박은혜, 황도현, 윤창조

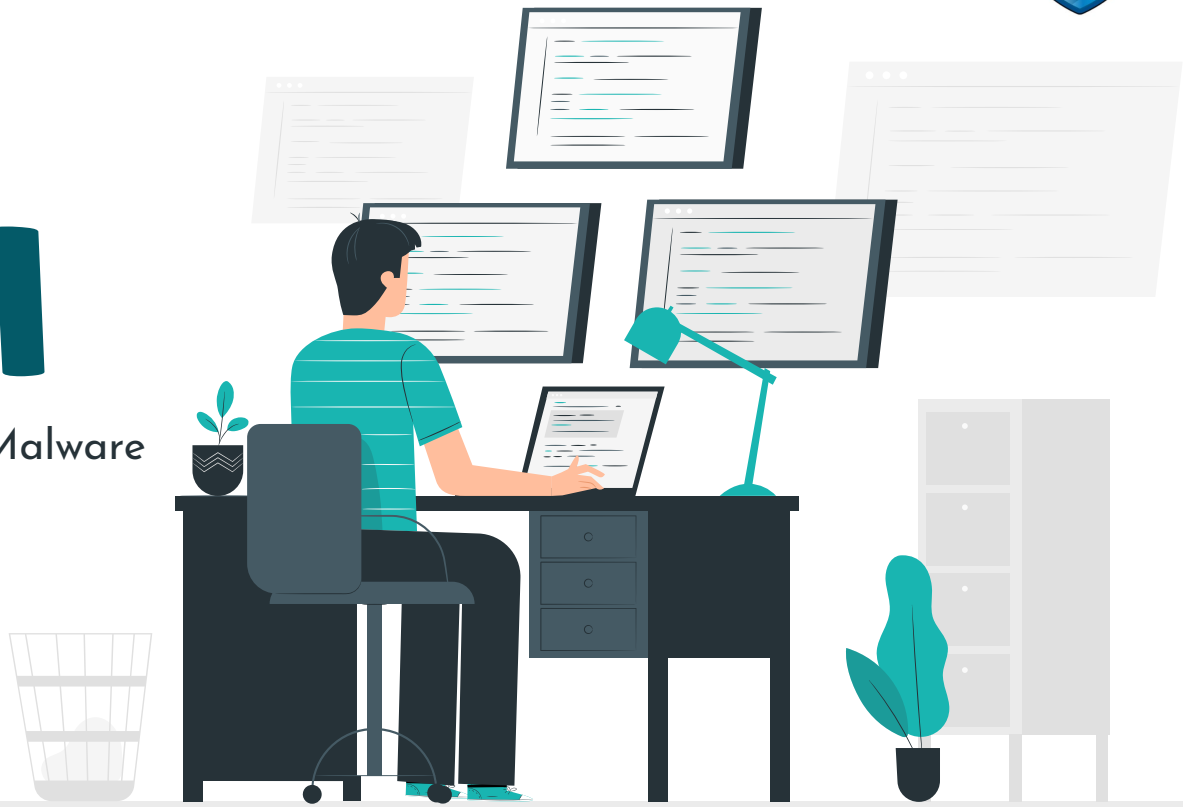


TABLE OF CONTENTS

제작 배경

01

악성코드 탐지 및 격리

악성 코드 탐지 및 탐지된 악성코드를 분석하고
효율적으로 격리함으로써 하나의 격리 집단군을 형성함

02

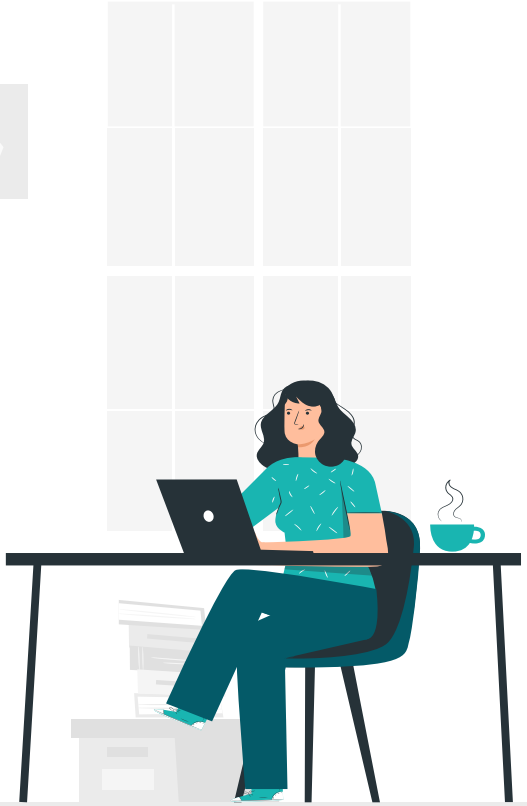
새로운 데이터셋 구축

데이터를 수집하고 격리된 악성코드의 feature을
만들어 새로운 데이터셋 환경을 구축 가능함

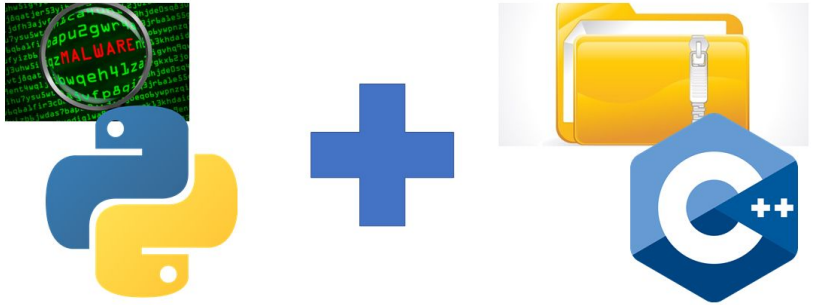
03

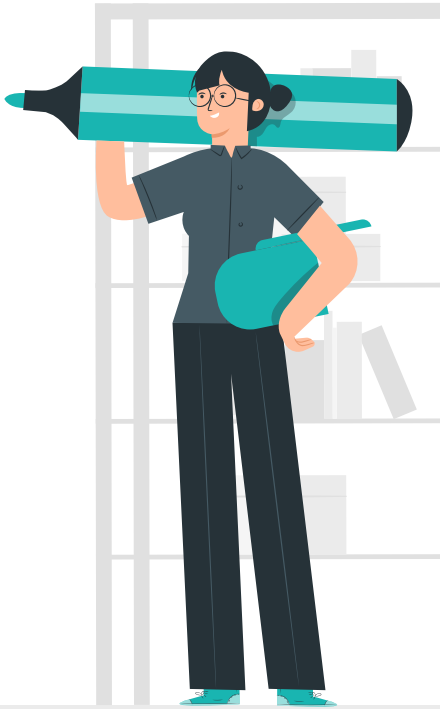
안정적 파일 환경 구성

악성파일이 실행되지 않도록 즉각 격리하여
파일 환경의 안전성과 편리성을 도모함



ICBM 소개

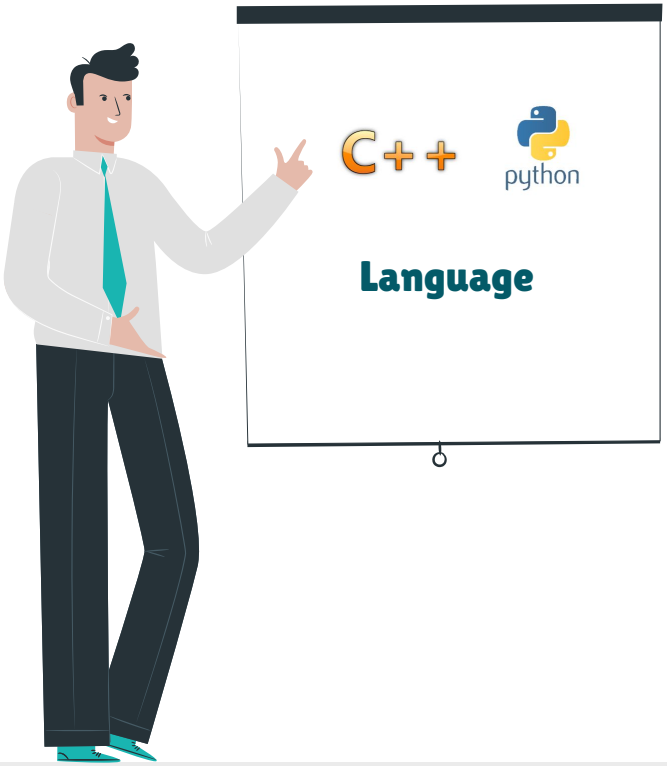




ICBM 이란 ??

-> Intelligent Compression for Binary Malware 으로
Python 을 통해 탐지된 **malware** 를 **file packaging** 하는 것을 목표로 함

Malware Detection -> Python
File Packaging or Making -> C/C++
을 이용 하여
Python + C = Multi-Language System 을 구축하여 만든 해커톤 프로젝트



개발 환경

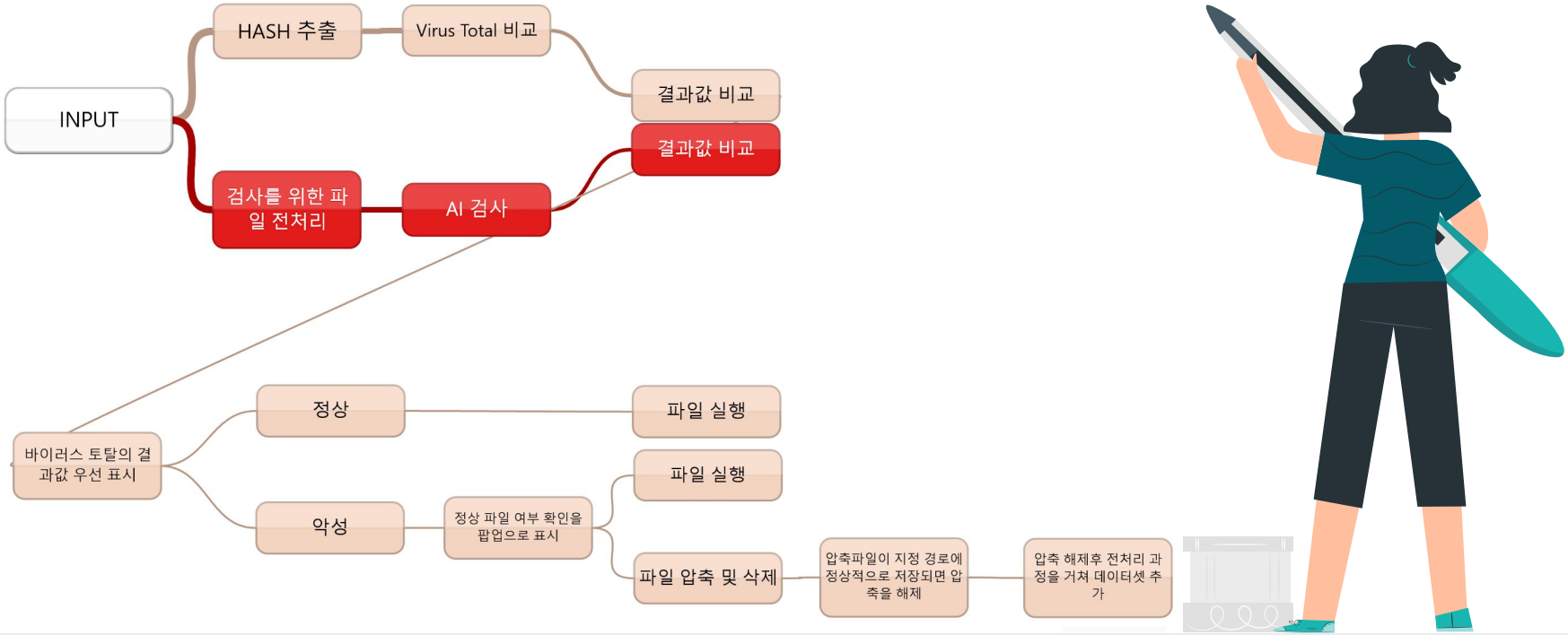
사용 언어 : C, C++, Python

사용 목적 : Malware classification and detection 후 detect된 malware를 packaging 하는 것을 목적으로 하여 안정성 있는 파일 검사 및 분석에 초점을 맞추도록 한다.

사용 환경 : Anaconda, Visual Studio, PyCharm, Visual Studio Code

주요 기능

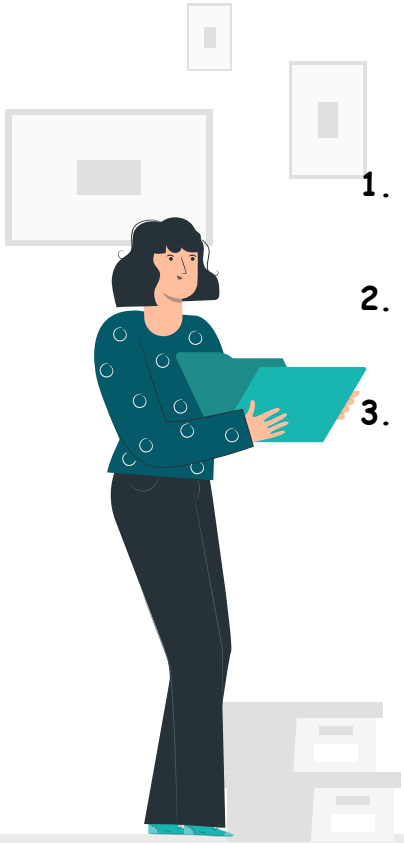
제품 프로세스


INPUT
HASH 추출
Virus Total 비교
결과값 비교
검사를 위한 파일 전처리
AI 검사
결과값 비교
바이러스 토탈의 결과값 우선 표시
정상
파일 실행
악성
정상 파일 여부 확인을 팝업으로 표시
파일 실행
파일 압축 및 삭제
압축파일이 지정 경로에 정상적으로 저장되면 압축을 해제
압축 해제후 전처리 과정을 거쳐 데이터셋 추가

사용 기술

코드 예제 및 시연

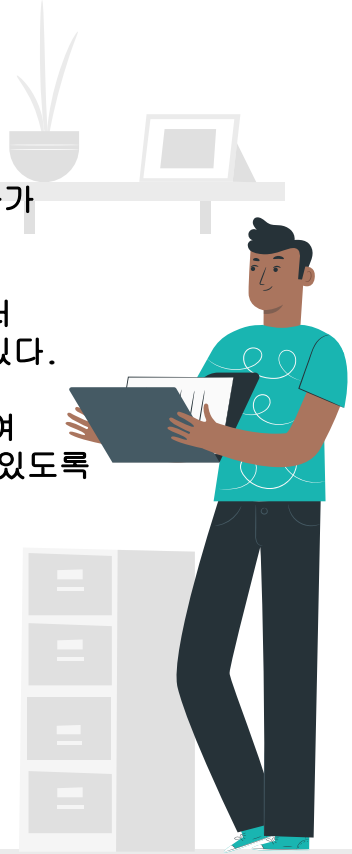
기대 효과



1. 악성코드 탐지 후 효율적으로 악성코드를 격리함으로써 사용자가 관리를 용이하게 할 수 있도록 한다.

2. 악성코드를 격리시켜 군집군이 형성될 수 있도록 하고 데이터 수집을 용이하게 하여 또 다른 악성코드 데이터셋을 만들 수 있다.

3. 새롭게 만들어진 악성코드 데이터셋을 모델에 학습 및 추가하여 악성코드 데이터 양을 늘리고, 더 많은 악성코드를 학습할 수 있도록 하여 탐지 기능을 구현할 수 있도록 한다.

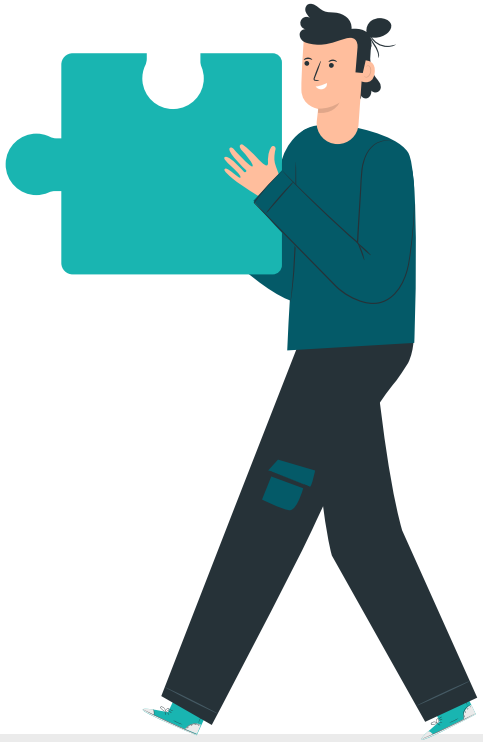


"저는 **zlib** 라이브러리와 함께,
악성코드를 **gz** 파일로 압축하여 별도로
격리하는 기능을 개발했습니다."

HDH

"저는 gz로 압축된 악성코드를 다른 디렉토리에 해제하여 새로운 데이터셋을 구성하는 프로그램을 작성했습니다."

Creation Yun



"저는 악성코드를 AI로 학습시켜
정확도 99.4%를 달성했습니다."

(Loss는 0.06 정도)

Lim Sky

"저는 VirusTotal에 악성코드 해시값을 매치하여 스캔 결과를 확인하고 분류할 수 있도록 하는 코드를 작성했습니다."

Eun Hye

THANKS

Do you have any questions?

https://github.com/sky81219/ICBM

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik