앙상블 모델 기반의 pdf 문서형 악성코드 탐지모델

캐치 잇(Catch it!)
임은선, 이수지, 방수경, 정수아

01 주차별 활동 소개

주차별 활동 정리

02 서비스 기획 배경

악성코드 현황

PDF 문서형 악성코드의 정의

PDF 문서형 악성코드의 심각성

유사 서비스

03 서비스 소개

주요기능

Feature 선택

모델의 탐지 방식

04 서비스 제공 방식

개발 환경

I.A.

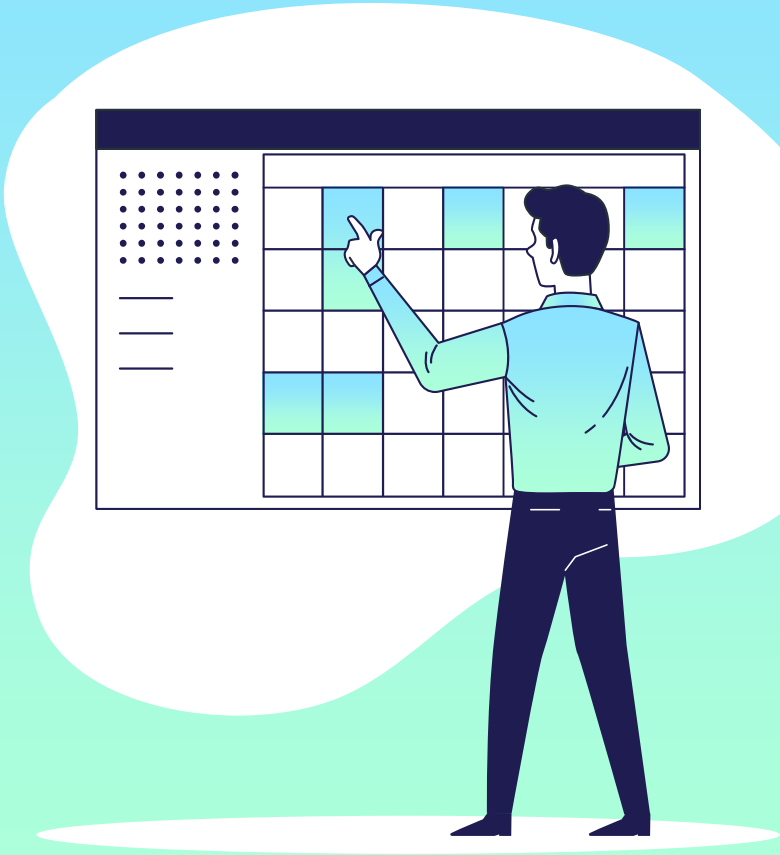
화면설계

향후 발전가능성

01

주차별 활동 소개

Weekly Activity Introduction



주차별 활동 정리

주차	활동 내용
1주차	주제 선정 및 팀 이름 결정
2주차	‘게임속의 악성코드’에 대한 자료조사
3주차	‘앙상블 모델 기반의 pdf 문서형 악성코드 탐지모델’로 주제 변경
4주차	주제에 대한 정의 및 기존 서비스 자료조사
5주차	데이터 수집 및 분석방법 결정
6주차	악성 샘플로 실습 & feature 선정(1)
7주차	악성 샘플로 실습 & feature 선정(2), 기획서 작성
8주차	서비스 주요기능에 대한 조사, 기획서 작성

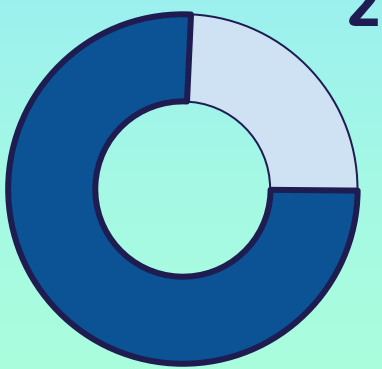
02

서비스 기획 배경

Background of Service Planning

악성코드 현황

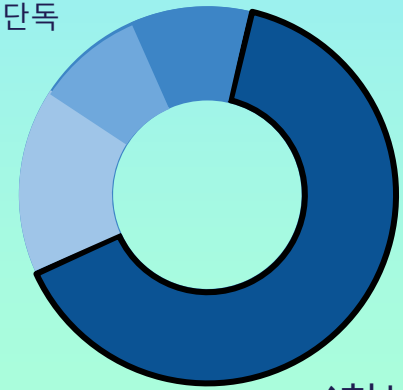
악성코드 공격의 침해유형



25%
기타

75%
이메일

이메일 내, 악성코드 위장기술 비율



5.9%
링크 방식

5.9%
.exe 단독

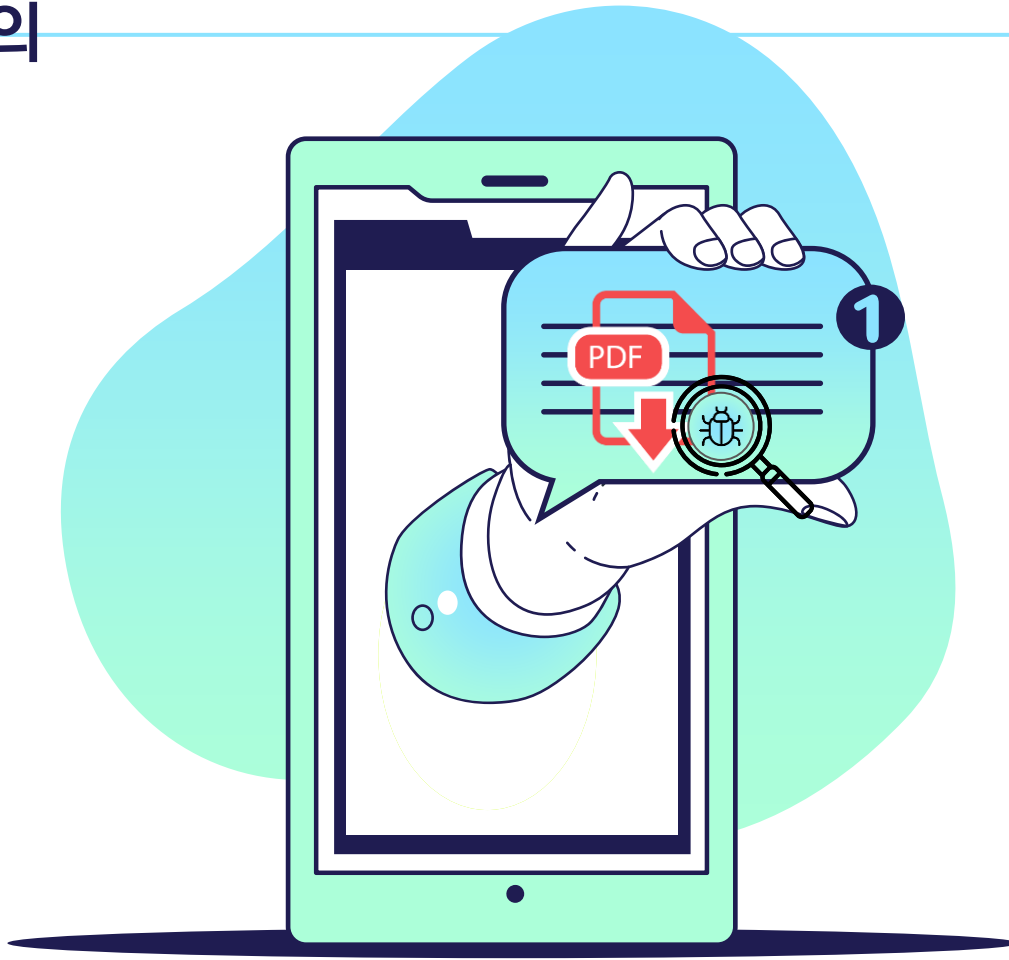
17.6%
Link & 확장자 조작

70.6%
(첨부) 문서형태

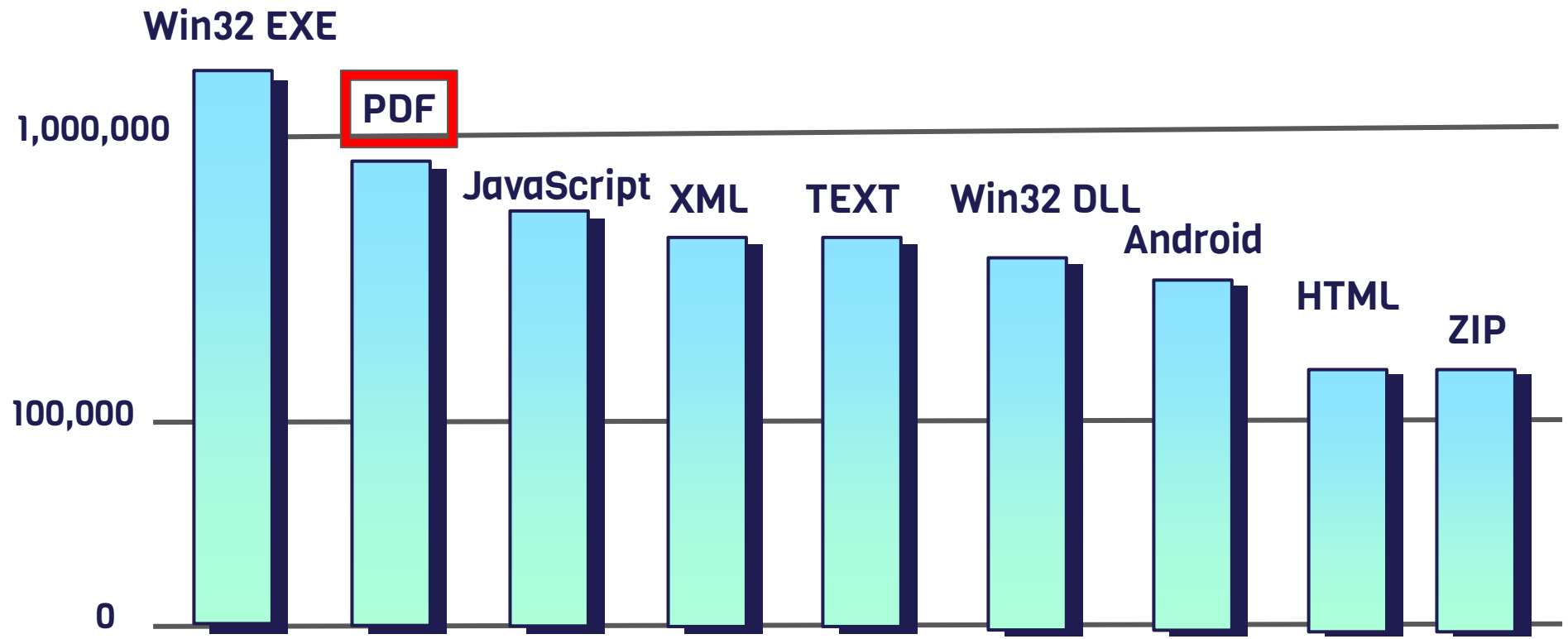
PDF 문서형 악성코드의 정의

- 실행파일(.exe)이 아닌 전자문서의 확장자 형태인 PDF로 위장하여 악의적인 행위를 하는 소프트웨어

- 사람들 간의 신뢰와 호기심을 기반으로 대상을 속이는 사회공학 기법을 이용하여 지능 형 지속 공격을 수행한다는 점에서 위협적



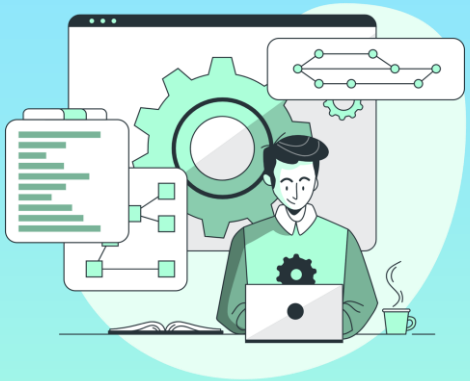
PDF 문서형 악성코드의 심각성



유사 서비스

SaniTox의 *CDR 솔루션

문서의 구조를 분석하고 악성 코드가 발생할 가능성이 있는 부분을 탐지 및 필터링하여 안전한 파일로 재조합



인섹시큐리티의 Joe Sandbox ML

인공지능 엔진 기반 악성코드 정밀 분석 솔루션으로 다양한 유형의 파일 형식들을 지원하며 정적분석을 통한 탐지도 가능함

* CDR(Content Disarm & Reconstruction) : 콘텐츠 무해화

03

서비스 소개

Service Introduction

서비스 주요 기능

- VirusTotal과 같은 악성행위 한눈에 보기
- CDR(콘텐츠 무해화) 기술을 통해 안전한 문서 파일로 재구성 후 제공

악성코드 탐지 모델

Hash	Target
D1C2CC0CA653DF88…..	1
22a9f60764801...	0
….	..
6d044ac0556bef3d1…	0

INPUT DATASET

Feature 추출

결측치/이상값 처리

데이터 인코딩

Training model
: Random Forest model

SAFE

MALICIOUS

OUTPUT DATASET

Feature 선택

/nLaunch

nLaunch의 값에 따라 첨부파일의 저장 경로 및 실행 방식 결정

/EmbeddedFile, /F, /RichMedia

내부에 포함된 파일을 열 때 사용

/URI, /GOTO

Fetch하거나 URL 접근

/ActionScript, /Acroform

JavaScript 코드와 결합 및 활용해 악성 행위를 수행

Feature 선택

/JS, / JavaScript

JavaScript 코드 실행

Obj의 수, /PAGE

악성 파일의 경우 압축되어 있기 때문에 수가 적음

/OpenAction, /AA

자동작업을 수행

/Object Stream

다른 타입은 길이 제약이 있어 보통 여기에 삽입됨

악성 PDF VS 일반 PDF

파일 이름	D1C2CC0CA653DF8DDB46C1337A5972EACEB81EA924E8EBDB7AF0699A7AB909FD.pdf
Type	PDF(Portable Document Format)
MD5	578684aff04e625a2d6801a2fbedc005
SHA-256	d1c2cc0ca653df8ddb46c1337a5972eaceb81ea924e8ebdb7af0699a7ab909fd

악성 **PDF**

파일 이름	딥러닝과 PDF 객체분석을 이용한 문서형 악성코드 탐지.pdf
Type	PDF(Portable Document Format)
MD5	22a9f6076448012fa8353c2f00d224f3
SHA-256	4906eb0f946d500458d09c5213b1a26215c7beaa93a77eb8754267ac715984a6

일반 **PDF**

악성 PDF VS 일반 PDF

```
remnux@remnux:~/Downloads/malware$ pdfid.py d1c2cc0ca653df8ddb46c1337a5972eaceb81ea9
7ab909fd.pdf
PDFiD 0.2.8 d1c2cc0ca653df8ddb46c1337a5972eaceb81ea924e8ebdb7af0699a7ab909fd.pdf
 PDF Header: %PDF-1.5
 obj                    28
 endobj                 28
 stream                 26
 endstream              26
 xref                    0
 trailer                 0
 startxref               1
 /Page                   0
 /Encrypt                0
 /ObjStm                 1
 /JS                     1
 /JavaScript             0
 /AA                     0
 /OpenAction             1
 /AcroForm               1
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           1
 /XFA                    0
 /URI                    0
 /Colors > 2^24          0
```

악성 **PDF**

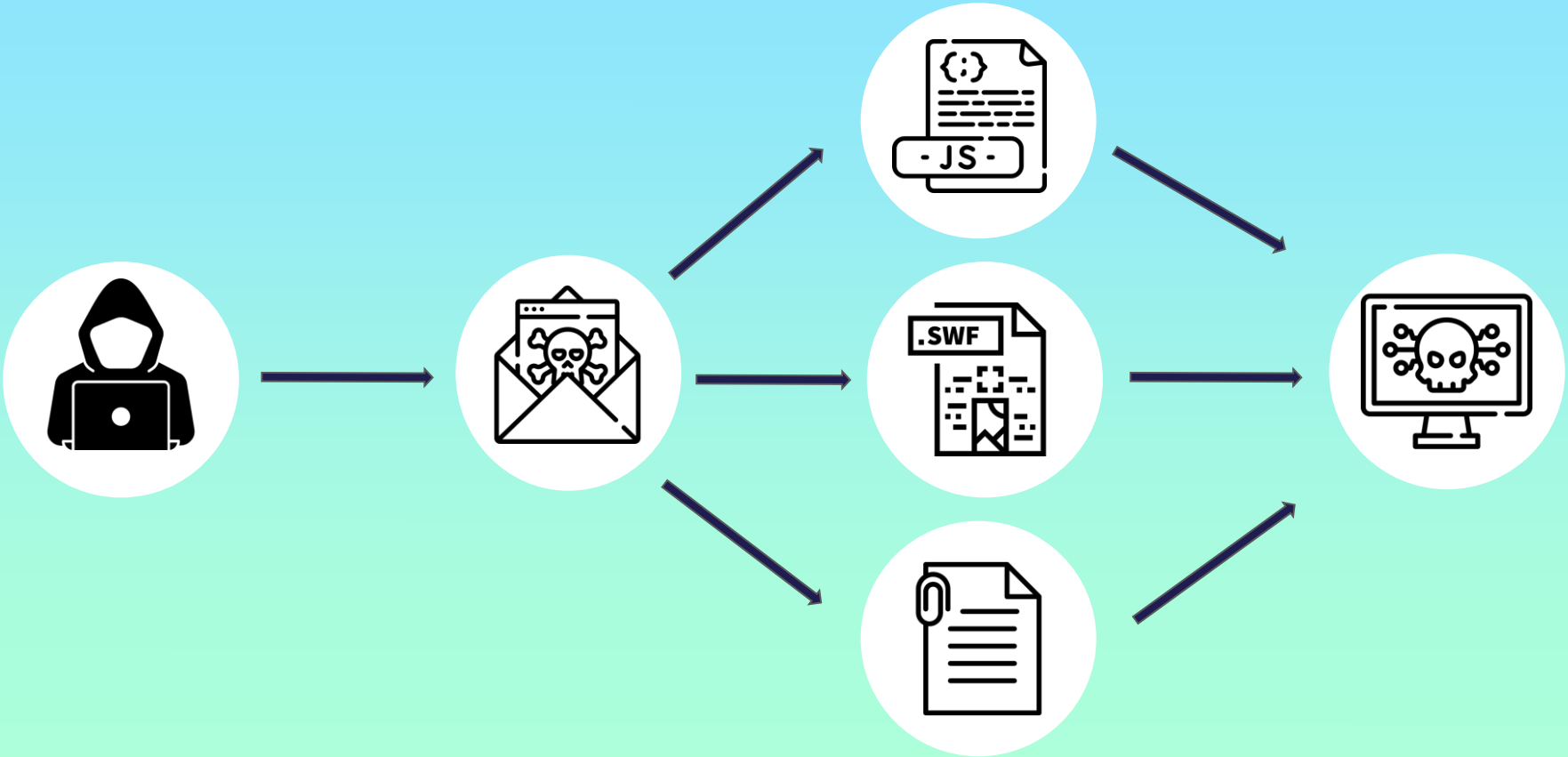
```
C:₩Users₩sue₩Desktop₩pdf_tool>python pdfid.py -f deep.pdf
PDFiD 0.2.8 deep.pdf
 PDF Header: %PDF-1.7
 obj                   113
 endobj                113
 stream                 54
 endstream              54
 xref                    1
 trailer                 1
 startxref               1
 /Page                   6
 /Encrypt                0
 /ObjStm                 0
 /JS                     0
 /JavaScript             0
 /AA                     0
 /OpenAction             1
 /AcroForm               0
 /JBIG2Decode            0
 /RichMedia              0
 /Launch                 0
 /EmbeddedFile           0
 /XFA                    0
 /Colors > 2^24          0
```

일반 **PDF**

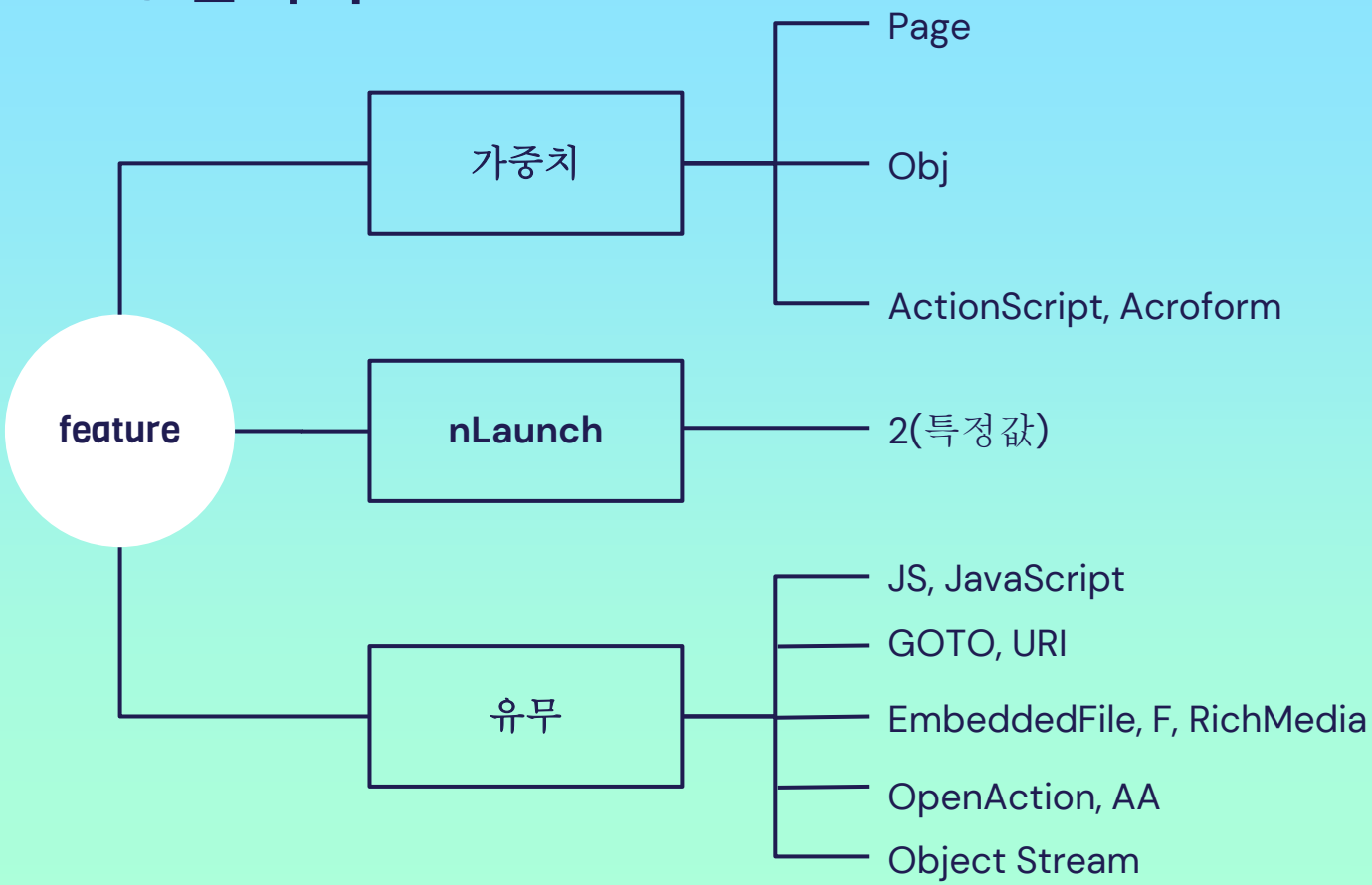
악성 PDF VS 일반 PDF

	Obj	Page	Objstm	JS/ Javascript	Acroform	Embedded File
악성 **PDF**	28	0	1	1	1	1
일반 **PDF**	113	6	0	0	0	0

악성코드 동작 방식



Feature 전처리

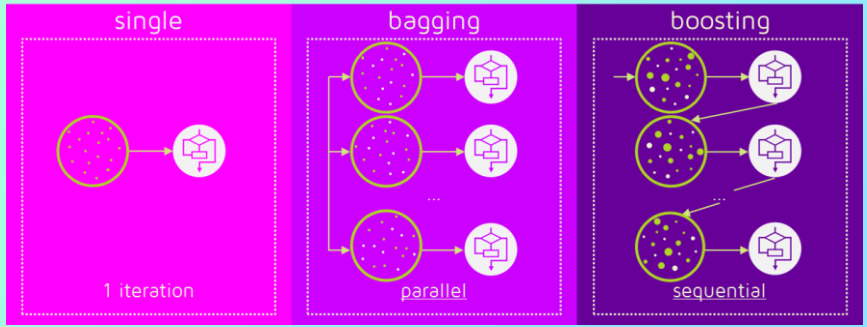

feature
가중치
Page
Obj
ActionScript, Acroform
nLaunch
2(특정값)
유무
JS, JavaScript
GOTO, URI
EmbeddedFile, F, RichMedia
OpenAction, AA
Object Stream

앙상블 모델

앙상블 모델

- 모델의 성능을 높이기 위해 여러가지의 모델을 학습시키는 것
- 즉, 약 분류기들을 결합하여 강 분류기를 만듦
- 오픈 플랫폼 캐글에서 앙상블 알고리즘이 머신러닝의 선도 알고리즘으로 인기를 모으고 있음

앙상블 모델



앙상블 모델 학습 방법

- **Bagging**

  샘플을 여러 번 뽑아(Bootstrap) 각 모델을 학습시켜 결과물을 집계하는 방법

- **Boosting**

  처음 모델이 예측하면 그 예측 결과에 따라 데이터에 가중치가 부여되고, 부여된 가중치가 다음 모델에 영향을 줌

Why 앙상블 모델?

‘Decision Tree’ 알고리즘을 이용해
문서형 악성코드 탐지

↓

앙상블 모델을 이용한
PDF 악성코드 탐지 모델 제작

우리가 선택한 모델은?

Random Forest

- 분류, 회귀 분석 등에 사용되는 앙상블 학습 방법의 일종

- 여러 개의 Decision tree를 형성하고 각 트리가 분류한 결과에서 투표를 실시하여 가장 많이 득표한 결과를 최종 분류 결과로 선택

선택한 이유

- 랜덤 포레스트는 배깅 방식 기반으로 이루어진 모델이며, 배깅은 부스팅보다 성능이 뛰어나서 불안정한 모형일 수록 좋은 성능을 발휘

- PDF 문서형 악성코드는 데이터양이 적기 때문에 데이터의 양이 적고 데이터 속성이 단순할 수록 좋은 배깅 알고리즘이 적합

- Data Scaling을 할 필요가 없고, 과적합이 잘 되지 않음

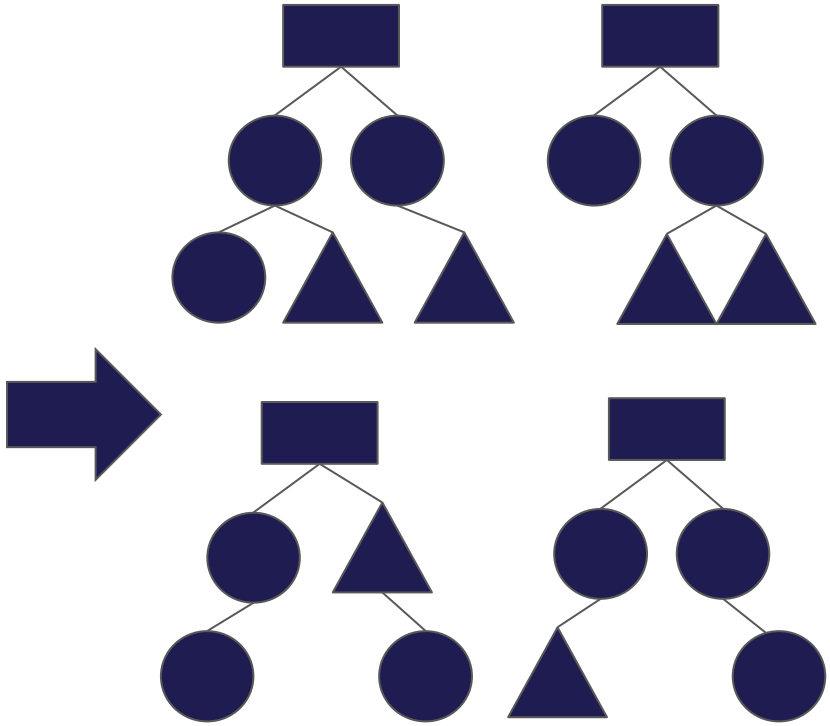
동작방식 - 데이터셋

	nLaunch	JS	. . .	obj	Embedded File	Page
D1C2CC0CA653DF8DDB46C1337A597…	2	1		28	1	1
22a9f6076448012fa8353c2…	0	0		130	0	12
. . .						. . .
6d044ac0556bef3d1e569…	1	0		22	1	8

동작방식 - 모델 학습

Train set

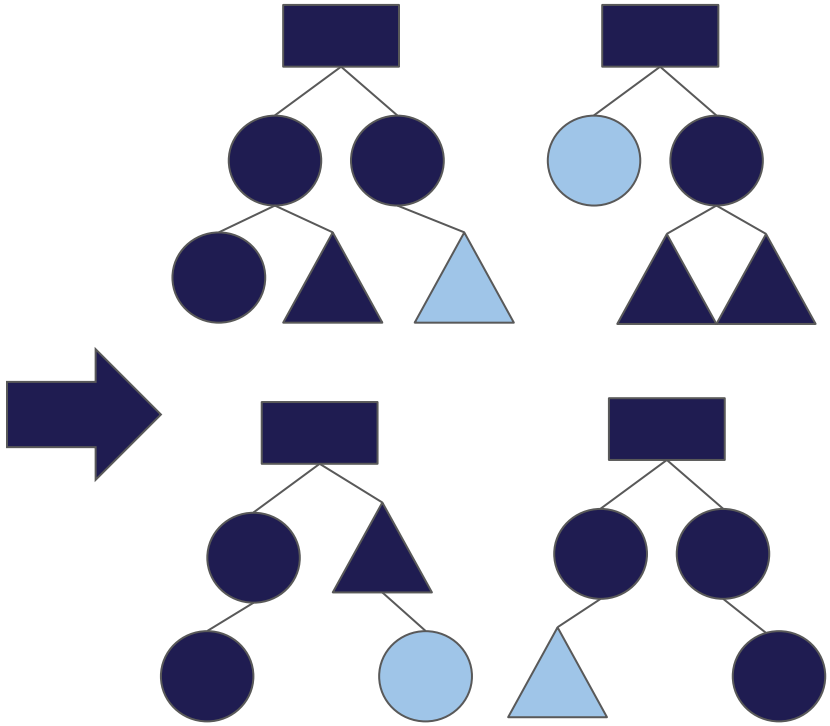
Boosting 1	Boosting 2	Boosting n
악성 파일 1	정상 파일 5	정상 파일 34
정상 파일 13	정상 파일 26	정상 파일 52
악성 파일 5	악성 파일 32	악성 파일 12
악성 파일 12	악성 파일 8	악성 파일 32
정상 파일 10	악성 파일 9	정상 파일 15
. . .	. . .	. . .



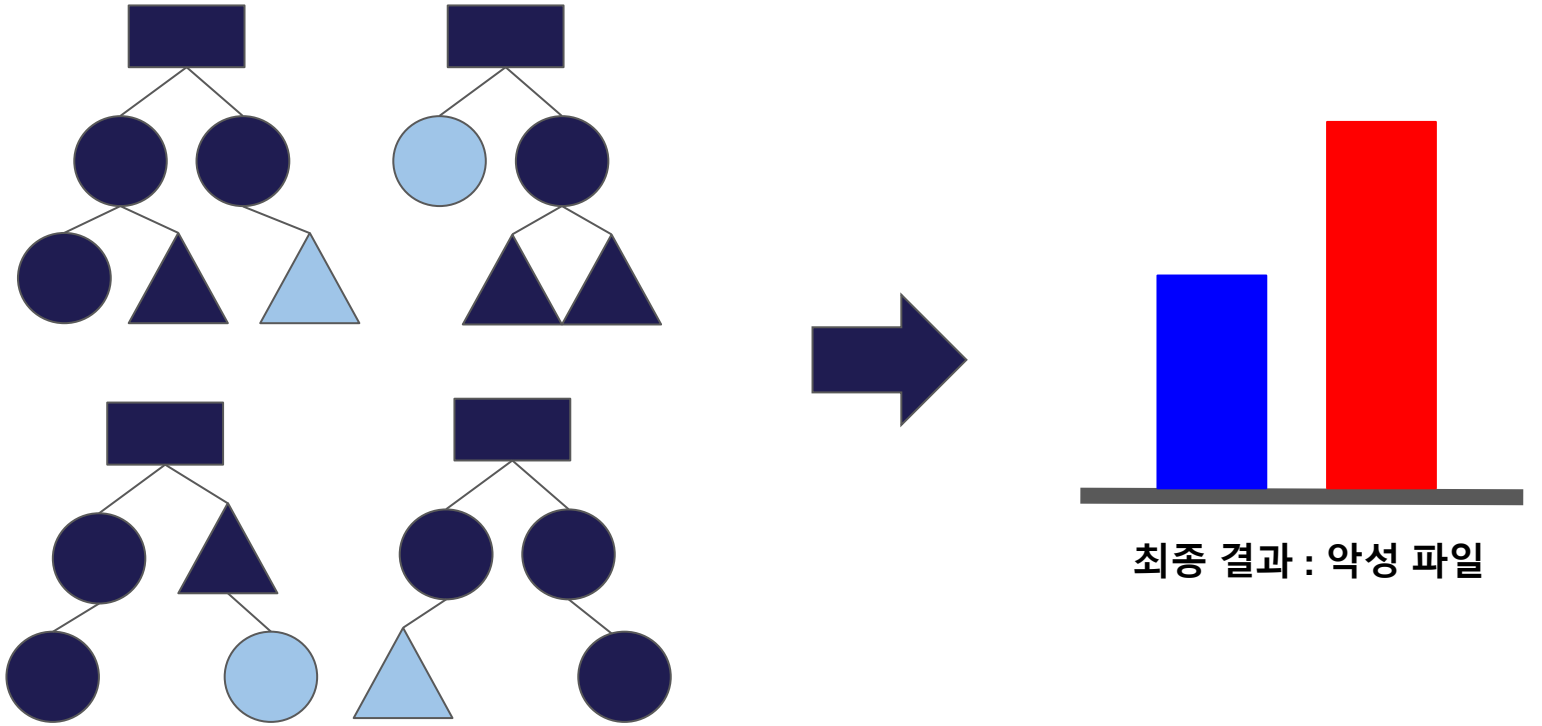
동작방식 - 각 모델 결과 도출

Test set

Boosting 1	Boosting 2	Boosting n
악성 파일 5	정상 파일 2	정상 파일 13
악성 파일 12	정상 파일 13	악성 파일 55
악성 파일 23	악성 파일 25	악성 파일 25
정상 파일 31	악성 파일 6	정상 파일 7
정상 파일 53	정상 파일 12	정상 파일 6
. . .	. . .	. . .



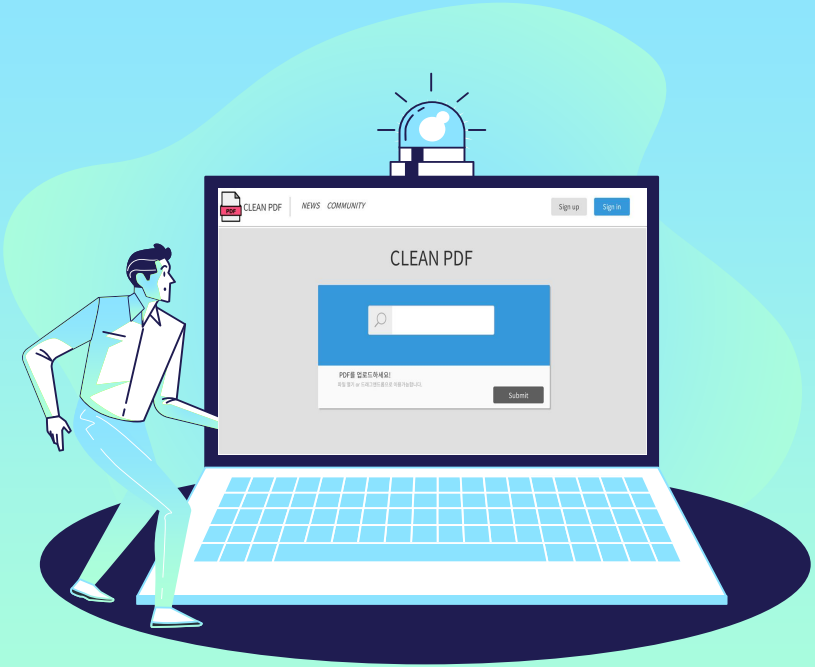
동작방식 - 최종 결과 도출



최종 결과 : 악성 파일

04
서비스 제공 방식

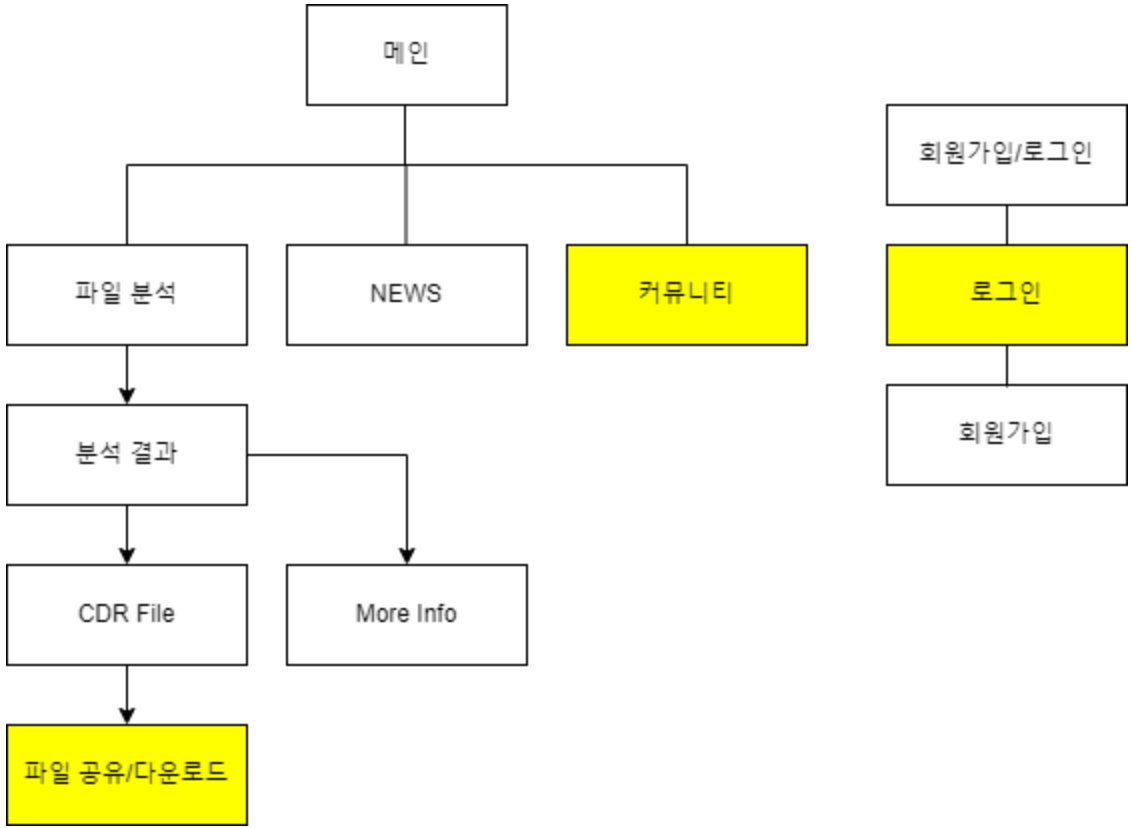
Service Providing System



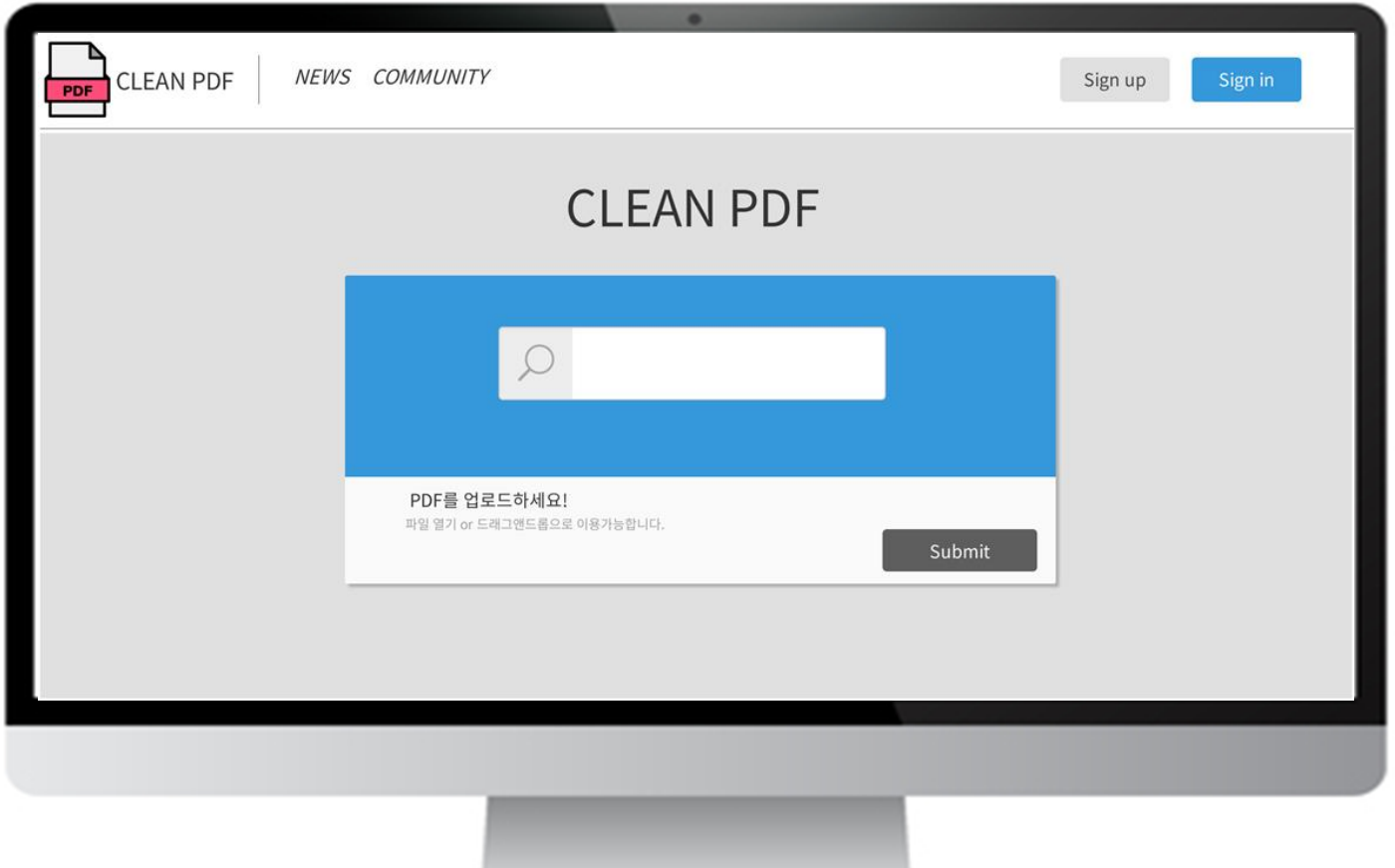
개발 환경

Tool	
언어	Python , Javascript, html, css
프레임워크	Django , bootstrap
서버, DB	mysql

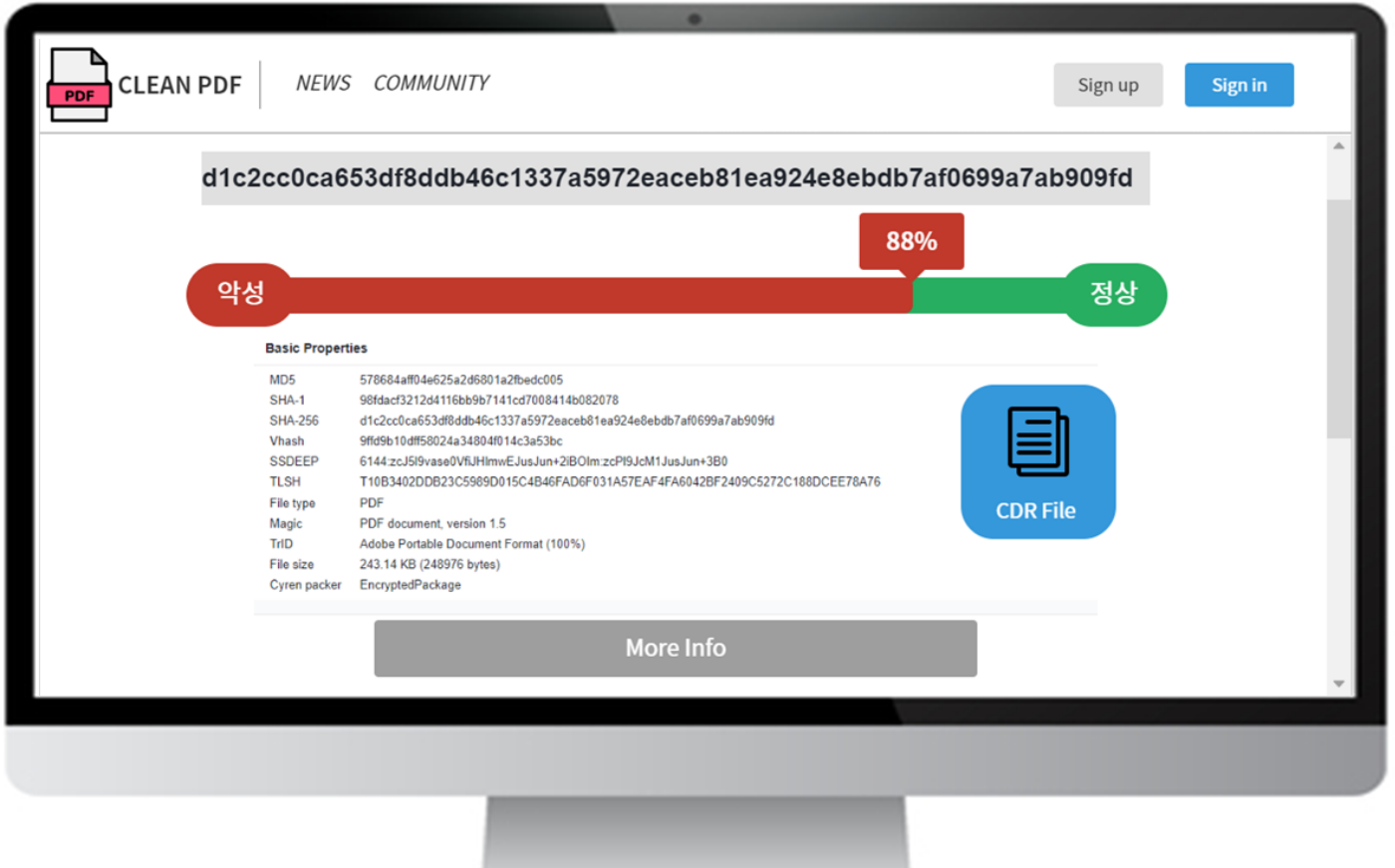
I.A (Information Architecture)



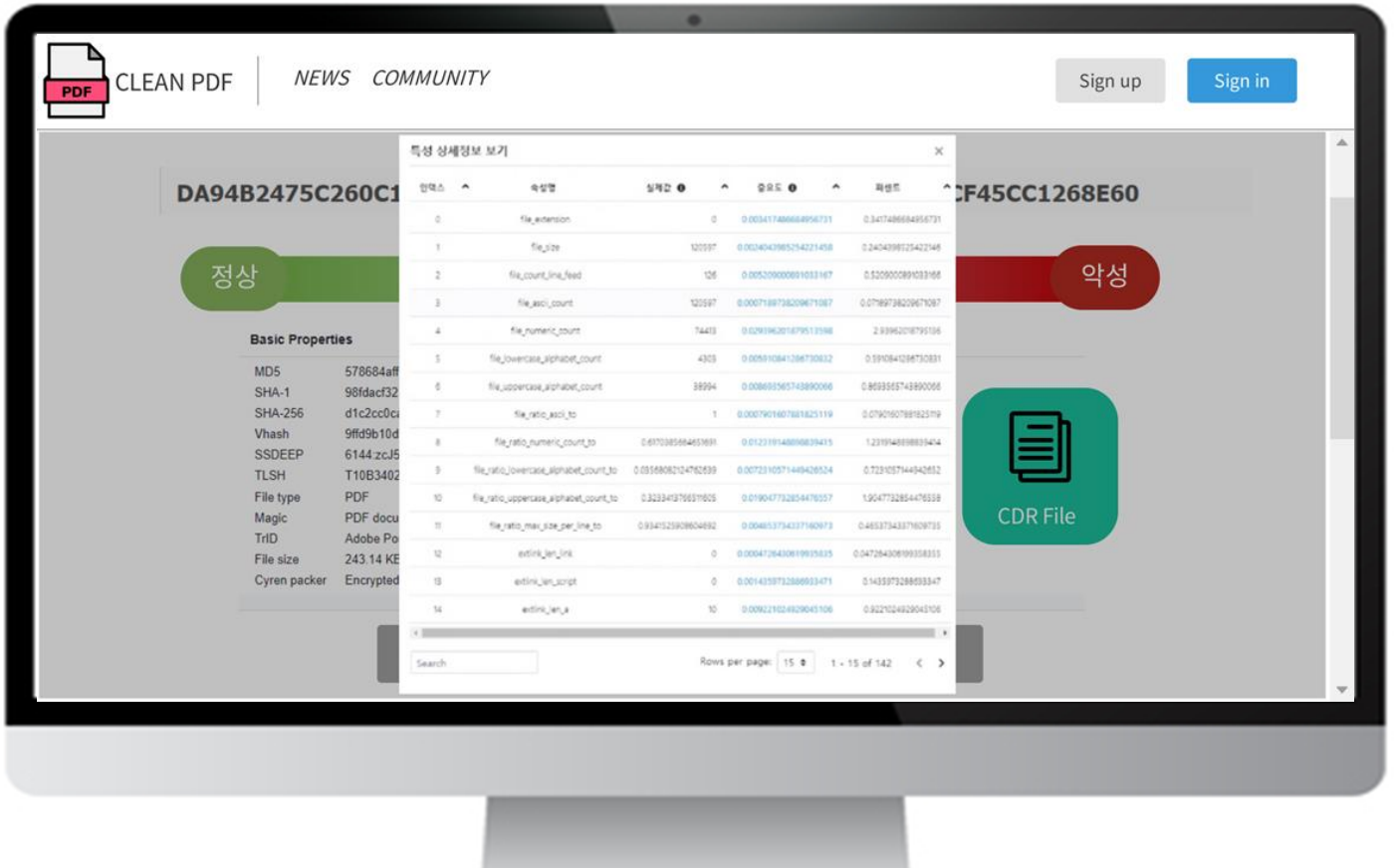
화면 설계 (UI)


PDF
CLEAN PDF
NEWS
COMMUNITY
Sign up
Sign in
CLEAN PDF
PDF를 업로드하세요!
파일 열기 or 드래그앤드롭으로 이용가능합니다.
Submit

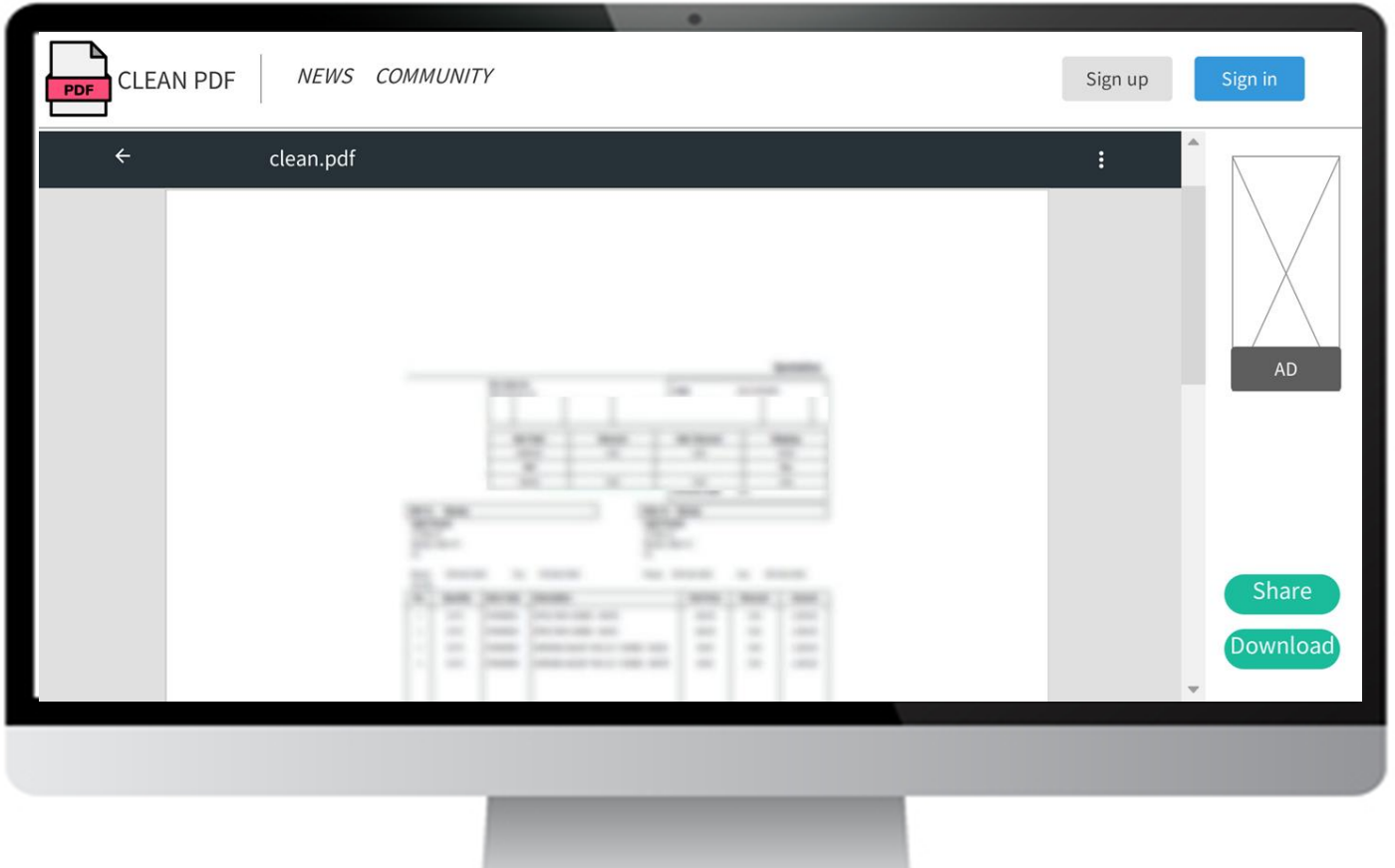
화면 설계 (UI)


PDF
CLEAN PDF
NEWS
COMMUNITY
Sign up
Sign in
d1c2cc0ca653df8ddb46c1337a5972eaceb81ea924e8ebdb7af0699a7ab909fd
88%
악성
정상
Basic Properties
MD5 578684aff04e625a2d6801a2fbedc005
SHA-1 98fdacf3212d4116bb9b7141cd7008414b082078
SHA-256 d1c2cc0ca653df8ddb46c1337a5972eaceb81ea924e8ebdb7af0699a7ab909fd
Vhash 9ffd9b10dff58024a34804f014c3a53bc
SSDEEP 6144:zcJ5l9vase0VfiJHlmwEJusJun+2iBOlm:zcPl9JcM1JusJun+3B0
TLSH T10B3402DDB23C5989D015C4B46FAD6F031A57EAF4FA6042BF2409C5272C188DCEE78A76
File type PDF
Magic PDF document, version 1.5
TrID Adobe Portable Document Format (100%)
File size 243.14 KB (248976 bytes)
Cyren packer EncryptedPackage
CDR File
More Info

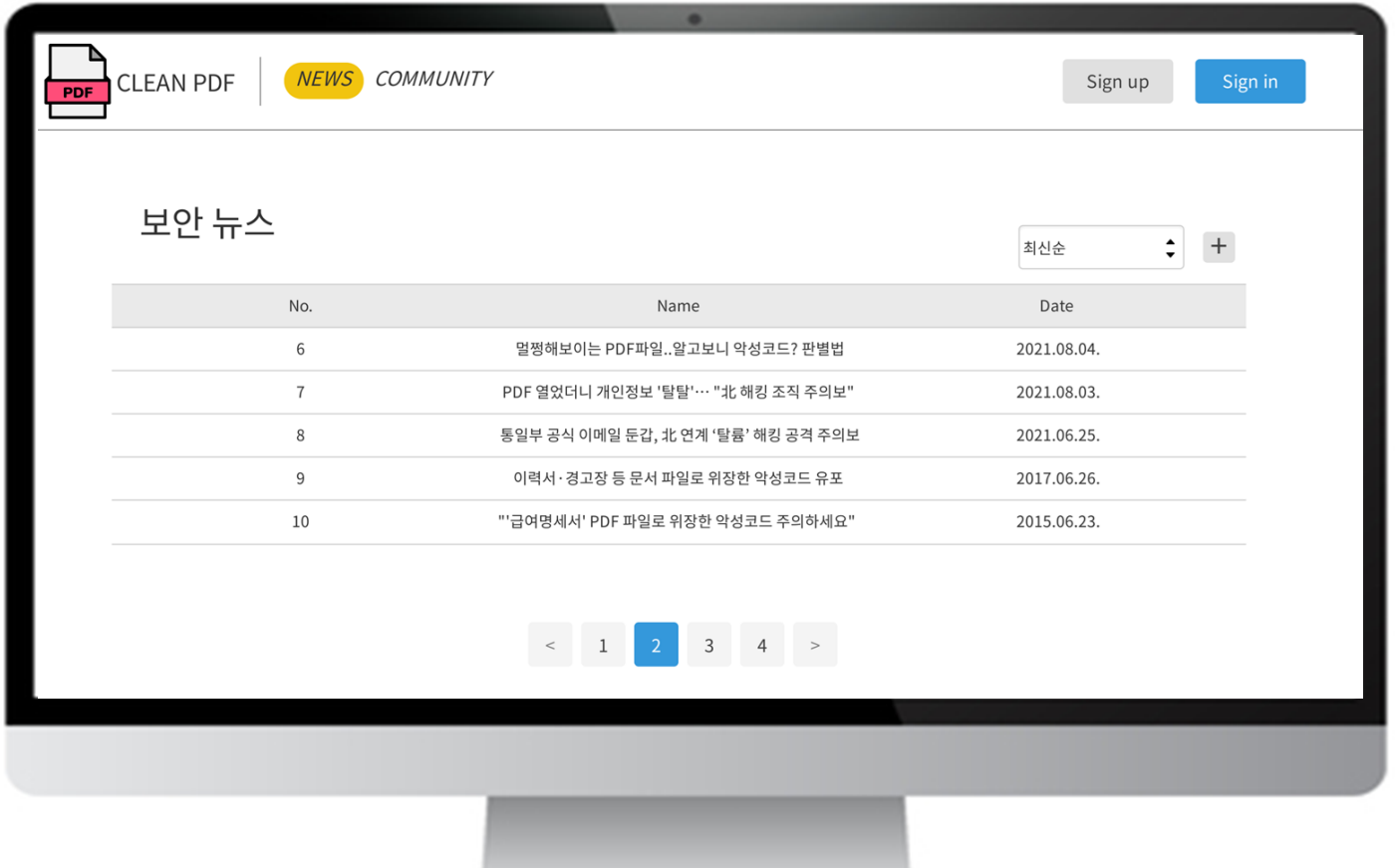
화면 설계 (UI)


PDF
CLEAN PDF
NEWS
COMMUNITY
Sign up
Sign in
특성 상세정보 보기
DA94B2475C260C1
CF45CC1268E60
정상
악성
Basic Properties
MD5
SHA-1
SHA-256
Vhash
SSDEEP
TLSH
File type
Magic
TrID
File size
Cyren packer
CDR File

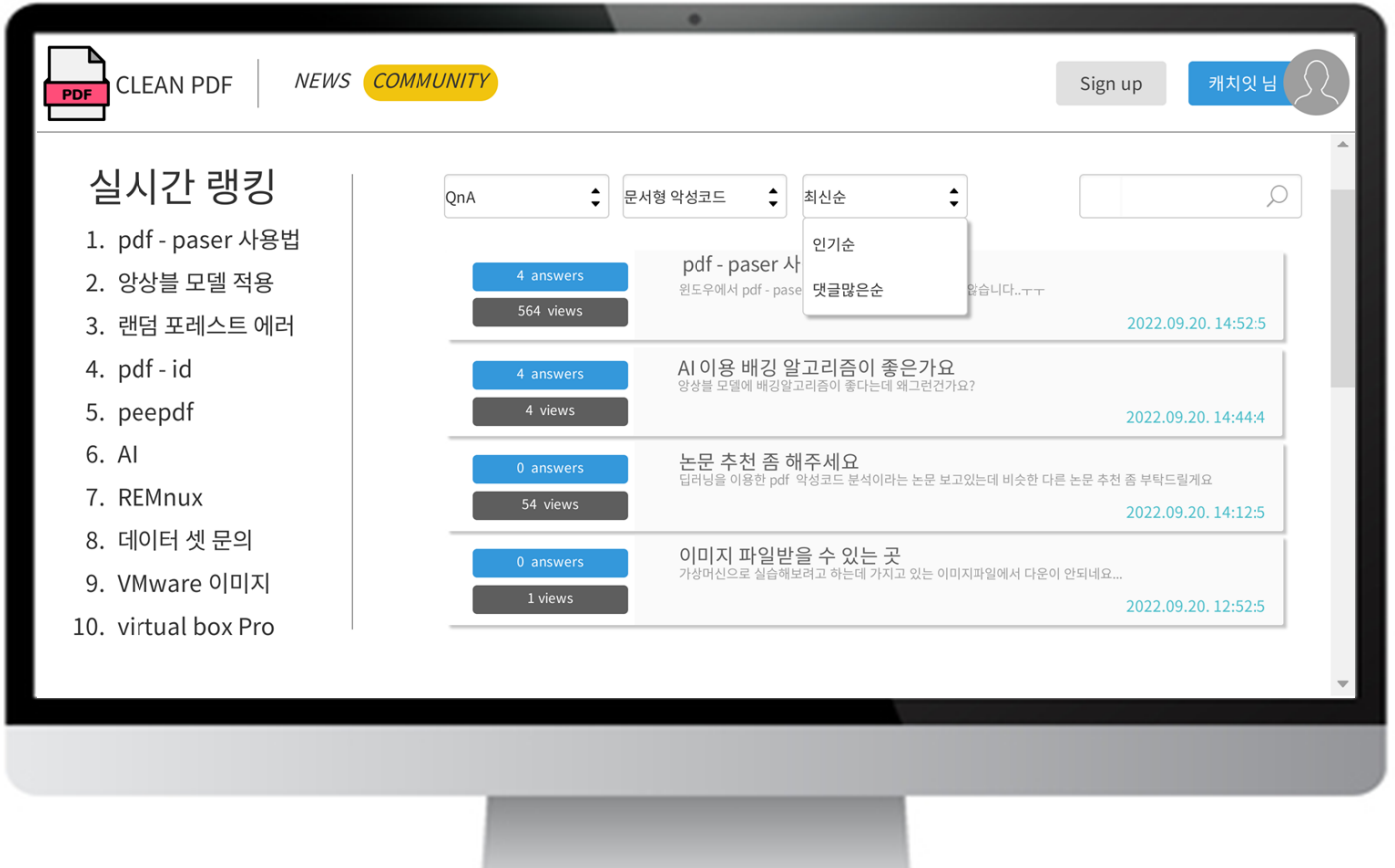
화면 설계 (UI)


PDF
CLEAN PDF
NEWS
COMMUNITY
Sign up
Sign in
clean.pdf
AD
Share
Download

화면 설계 (UI)


PDF
CLEAN PDF
NEWS
COMMUNITY
Sign up
Sign in
보안 뉴스
최신순
No.
Name
Date
6
멀쩡해보이는 PDF파일..알고보니 악성코드? 판별법
2021.08.04.
7
PDF 열었더니 개인정보 '탈탈'… "北 해킹 조직 주의보"
2021.08.03.
8
통일부 공식 이메일 둔갑, 北 연계 '탈륨' 해킹 공격 주의보
2021.06.25.
9
이력서·경고장 등 문서 파일로 위장한 악성코드 유포
2017.06.26.
10
"'급여명세서' PDF 파일로 위장한 악성코드 주의하세요"
2015.06.23.
< 1 2 3 4 >

화면 설계 (UI)


PDF
CLEAN PDF
NEWS
COMMUNITY
Sign up
캐치잇 님
실시간 랭킹
1. pdf - paser 사용법
2. 앙상블 모델 적용
3. 랜덤 포레스트 에러
4. pdf - id
5. peepdf
6. AI
7. REMnux
8. 데이터 셋 문의
9. VMware 이미지
10. virtual box Pro
QnA
문서형 악성코드
최신순
인기순
댓글많은순
4 answers
564 views
pdf - paser 사
윈도우에서 pdf - pase
2022.09.20. 14:52:5
4 answers
4 views
AI 이용 배깅 알고리즘이 좋은가요
앙상블 모델에 배깅알고리즘이 좋다는데 왜그런건가요?
2022.09.20. 14:44:4
0 answers
54 views
논문 추천 좀 해주세요
딥러닝을 이용한 pdf 악성코드 분석이라는 논문 보고있는데 비슷한 다른 논문 추천 좀 부탁드릴게요
2022.09.20. 14:12:5
0 answers
1 views
이미지 파일받을 수 있는 곳
가상머신으로 실습해보려고 하는데 가지고 있는 이미지파일에서 다운이 안되네요...
2022.09.20. 12:52:5

향후 발전 가능성

- 더 다양한 **feature**들을 추출 **&** 모델 기법을 다르게 하여 정확도를 높이는 것을 계획
- **Pdf** 뿐만 아니라 워드나 엑셀, 한글 등 여러 문서 형태의 악성파일 여부를 판단하고 정상파일로 다운받을 수 있도록 하는 것을 계획
- 메신저 서비스를 이용한 분석/탐지 기능 서비스 확장에 대한 가능성도 고려

참고문헌

강아름, 정영섭, 김세령, 김종현, 우지영, 최선오.(2018).문서 구조 및 스트림 오브젝트 분석을 통한 문서형 악성코드 탐지.한국컴퓨터정보학회논문지 ,23(11),85-93.

윤채은, 정혜현, 서창진.(2021).딥러닝과 PDF 객체분석을 이용한 문서형 악성코드 탐지.전기학회논문지 P,70P(1),44-49.

“(pdf 문서)”정상 pdf 파일”도 안심하지 마세요.”CSRC Weblob.n.d.수정, 2022년 9월 25일 접속, https://csrc.kaist.ac.kr/blog/2022/01/25/pdf-문서-정상-pdf-파일도-안심하지-마세요

"[2021 CDR 리포트] 디지털 시대를 위한 사이버 방역, 콘텐츠 무해화(CDR)." 보안뉴스 . n.d. 수정, 2022년9월25일 접속, https://m.boannews.com/html/detail.html?idx=99426.

“악성코드 정밀 분석 조샌트박스.”Joe Sandbox ML.n.d.수정, 2022년 9월 25일 접속,http://www.malwareanalysis.co.kr/ml.

"시큐레터 “자동화된 역분석 기술로 APT 방어”." DataNet. n.d. 수정, 2022년9월25일 http://www.datanet.co.kr/news/articleView.html?idxno=176173.

Thank you