오픈소스 이메일 보안 솔루션

[정보보호학전공_GOAT]

송지현, 김근수, 김원태, 김평안, 전유병

목차

1 프로젝트 소개

1. 팀 소개

2. 프로젝트 주제 및 목표

3. 프로젝트 구상도

1. 팀 소개

김근수

- 메일 서버 구축, 설정
- 메일 콘텐츠 확인
- 메일 프로세싱
- API 연동

김원태

- Cuckoo 구축, 설정
- Cuckoo 모듈 설치
- Cuckoo 확장자 설치
- API 연동

김평안

- WEB 개발

송지현

- 총괄
- Cuckoo 구축
- DB 구축
- 머신러닝

전유병

- Cuckoo REST API
- 메일 ClamAV
- 메일 SpamAssassin
- 메일, Cuckoo 구축

2. 프로젝트 주제 및 목표

보안뉴스

한국인터넷진흥원 스팸대응센터 사칭 피싱 메일 유포... 악성 링크 클릭 유도

최근 우리나라 유일의 정보보호 전문기관인 한국인터넷진흥원(KISA)을 사칭한 피싱 이메일이 유포되고 있어 모니터링 강화 및 첨부파일 열람 자제 등...

1일 전

머니투데이

"은행에서 보낸 줄" 이 메일 눌렀다가 정보 '탈탈'...악성코드 파고든다

'카드 이용한도 조정 안내' '보험료 자동이체' 등 메일을 가장해 악성코드를 심는 수법의 공격이 확인돼 이용자들의 주의가 필요하다는 제언이...

2023. 7. 21.

보안뉴스

공격자들에게 '이메일'은 여전히 가성비 높은 최고의 공격수단

BEC 공격, 적은 투자로 큰 수익 얻을 수 있는 성공률 높은 수법 악성 QR코드 및 생성 AI 사용해 우회 공격 시도...사이버 공격 점점 고도화·정교해져

2024. 3. 5.

최근까지 악성메일에 대한
피해가 꾸준히 지속되고 있는 사실 확인

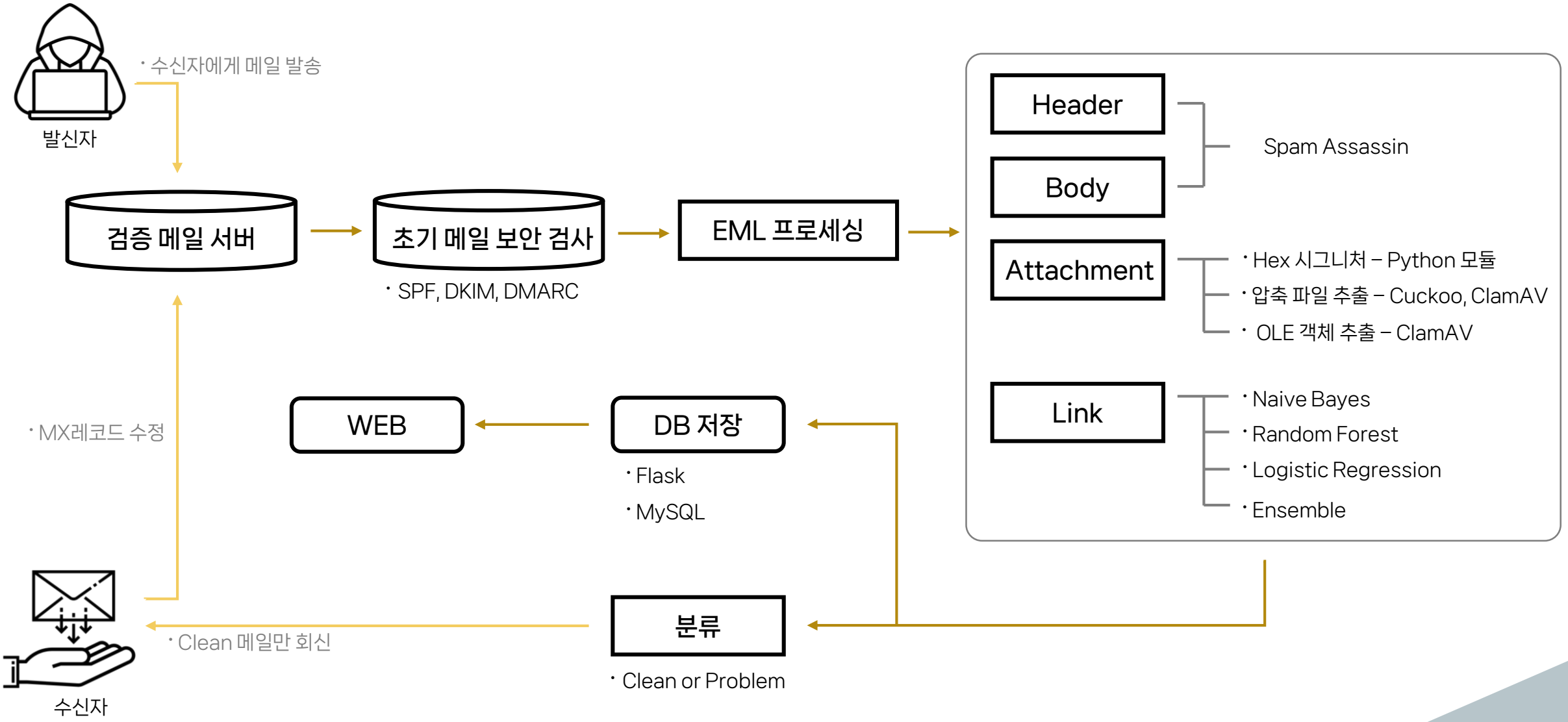
↓

이메일 검사, 의심스러운 링크 등
다양한 보안 기능을 머신러닝을 통해 자동화

↓

사용자의 보안 취약성을 해결, 사이버 보안을 강화

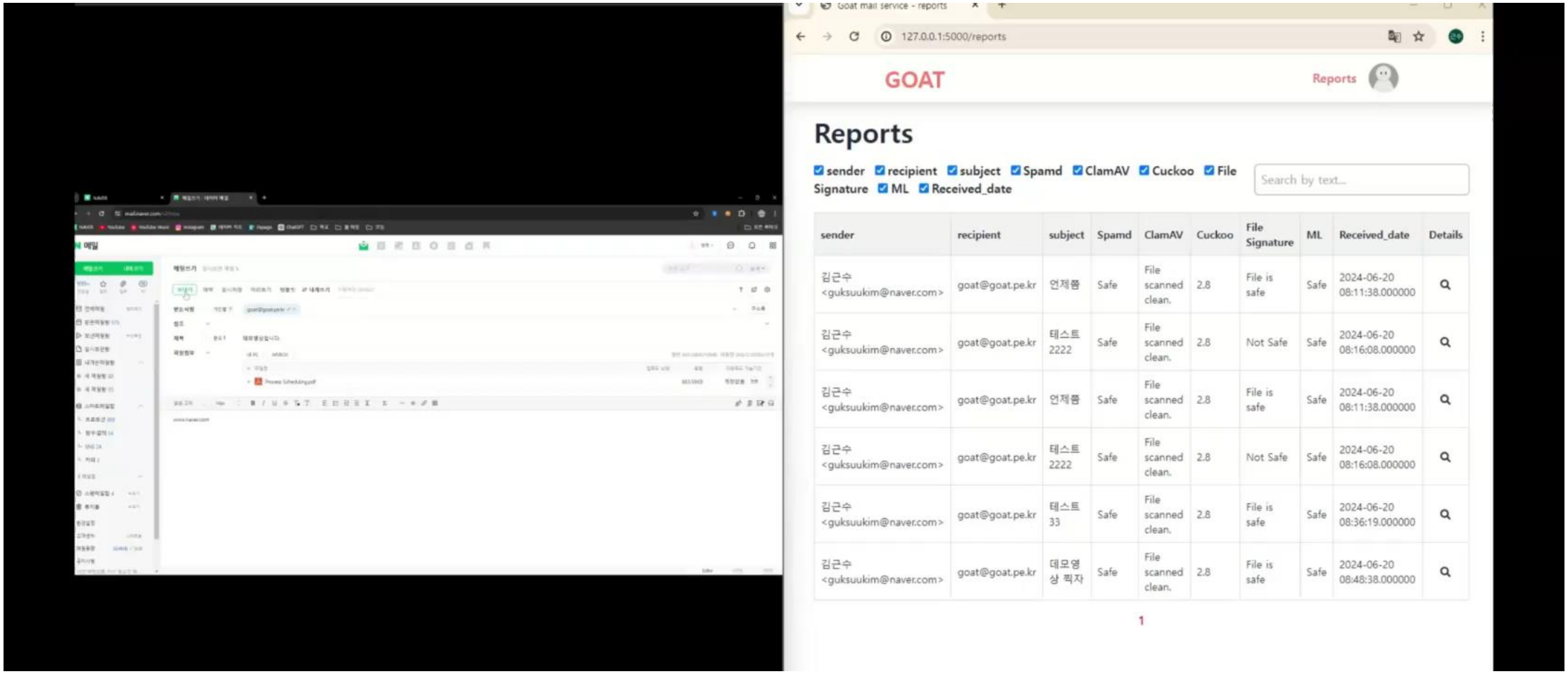
3. 프로젝트 구상도


발신자
• 수신자에게 메일 발송
검증 메일 서버
초기 메일 보안 검사
• SPF, DKIM, DMARC
EML 프로세싱
Header
Body
Spam Assassin
Attachment
• Hex 시그니처 – Python 모듈
• 압축 파일 추출 – Cuckoo, ClamAV
• OLE 객체 추출 – ClamAV
Link
• Naive Bayes
• Random Forest
• Logistic Regression
• Ensemble
WEB
DB 저장
• Flask
• MySQL
• MX레코드 수정
분류
• Clean or Problem
• Clean 메일만 회신
수신자

2 프로젝트 진행

1. 시연 영상
2. Mail Server 보안 설정
3. Cuckoo Sandbox 설정
4. 머신러닝 학습
5. DB 구축

1. 시연 영상


Goat mail service - reports
127.0.0.1:5000/reports
GOAT
Reports
Reports
sender recipient subject Spamd ClamAV Cuckoo File Signature ML Received_date
Search by text...
sender | recipient | subject | Spamd | ClamAV | Cuckoo | File Signature | ML | Received_date | Details
김근수 <guksuukim@naver.com> | goat@goat.pe.kr | 언제쯤 | Safe | File scanned clean. | 2.8 | File is safe | Safe | 2024-06-20 08:11:38.000000
김근수 <guksuukim@naver.com> | goat@goat.pe.kr | 테스트 2222 | Safe | File scanned clean. | 2.8 | Not Safe | Safe | 2024-06-20 08:16:08.000000
김근수 <guksuukim@naver.com> | goat@goat.pe.kr | 언제쯤 | Safe | File scanned clean. | 2.8 | File is safe | Safe | 2024-06-20 08:11:38.000000
김근수 <guksuukim@naver.com> | goat@goat.pe.kr | 테스트 2222 | Safe | File scanned clean. | 2.8 | Not Safe | Safe | 2024-06-20 08:16:08.000000
김근수 <guksuukim@naver.com> | goat@goat.pe.kr | 테스트 33 | Safe | File scanned clean. | 2.8 | File is safe | Safe | 2024-06-20 08:36:19.000000
김근수 <guksuukim@naver.com> | goat@goat.pe.kr | 데모영상 찍자 | Safe | File scanned clean. | 2.8 | File is safe | Safe | 2024-06-20 08:48:38.000000
1

2. Mail Server 보안 설정

MX레코드 수정 후 메일 수신

과정 : guksuukim@naver.com -> goat@goat.pe.kr (최종 목적지)

(redhat12.xyz (검증서버) 먼저 받기)

※ goat.pe.kr MX레코드 : mail.redhat12.xyz 수정

```
> set q=mx
> goat.pe.kr
서버:
[redacted]

권한 없는 응답:
goat.pe.kr      MX preference = 10, mail exchanger = mail.redhat12.xyz
>
```

→ MX 레코드 수정

```
MariaDB [postfix_accounts]> select * from alias_table;
+---------+----------+---------------------+---------------------+
| AliasId | DomainId | Source              | Destination         |
+---------+----------+---------------------+---------------------+
|       1 |        1 | testfc@kks.com      | testsc@kks.com      |
|       2 |        1 | redhats@redhat12.xyz | redhat12@redhat12.xyz |
|       8 |        1 | @redhat12.xyz       | @mail.redhat12.xyz  |
+---------+----------+---------------------+---------------------+
```

→

goat@goat.pe.kr로 메일이 들어왔을 때

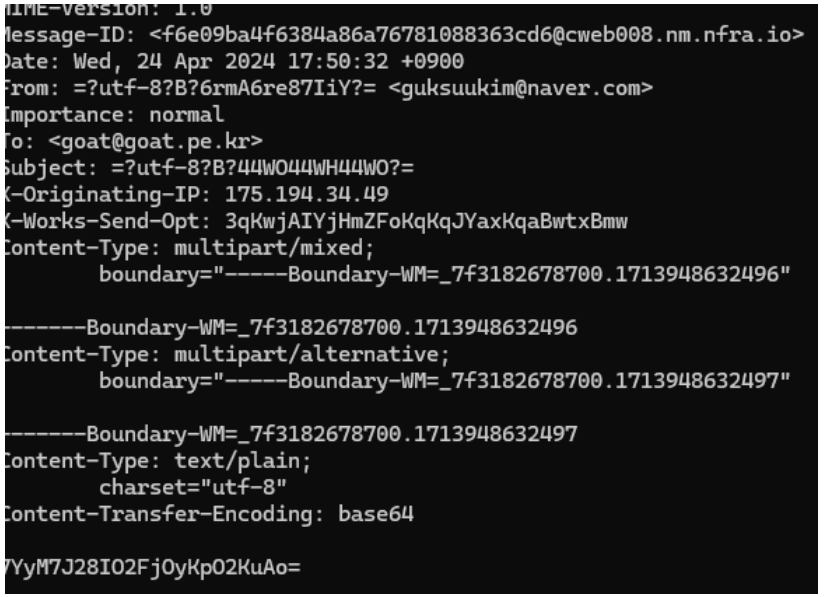
MX 레코드 설정된 mail.redhat12.xyz 로 메일 들어옴

검증 끝난 후 최종 목적지 goat@goat.pe.kr로 포워딩

2. Mail Server 보안 설정

MX레코드 수정 후 메일 수신

1. pe.kr로 메일 발신



```
MIME-Version: 1.0
Message-ID: <f6e09ba4f6384a86a76781088363cd6@cweb008.nm.nfra.io>
Date: Wed, 24 Apr 2024 17:50:32 +0900
From: =?utf-8?B?6rmA6re87IiY?= <guksuukim@naver.com>
Importance: normal
To: <goat@goat.pe.kr>
Subject: =?utf-8?B?44WO44WH44WO?=
X-Originating-IP: 175.194.34.49
X-Works-Send-Opt: 3qKwjAIYjHmZFoKqKqJYaxKqaBwtxBmw
Content-Type: multipart/mixed;
        boundary="-----Boundary-WM=_7f3182678700.1713948632496"

-------Boundary-WM=_7f3182678700.1713948632496
Content-Type: multipart/alternative;
        boundary="-----Boundary-WM=_7f3182678700.1713948632497"

-------Boundary-WM=_7f3182678700.1713948632497
Content-Type: text/plain;
        charset="utf-8"
Content-Transfer-Encoding: base64

7YyM7J28IO2FjOyKpO2KuAo=
```

3. 들어온 메일 오픈했을 때 EML 파일 형식 확인

```
Apr 24 17:50:32 mail postfix/cleanup[1898]: BDF8023B90: message-id=<f6e09ba4f6384a86a76781088363cd6@cweb008.nm.nfra.io>
Apr 24 17:50:32 mail postfix/qmgr[1409]: BDF8023B90: from=<guksuukim@naver.com>, size=98151, nrcpt=1 (queue active)
Apr 24 17:50:32 mail postfix/local[1899]: BDF8023B90: to=<goat@mail.redhat12.xyz>, orig_to=<goat@goat.pe.kr>, relay=local, delay=0.11, delays=0.09/0.02/0/0, dsn=2.0.0, status=sent (delivered to maildir)
Apr 24 17:50:32 mail postfix/qmgr[1409]: BDF8023B90: removed
Apr 24 17:50:32 mail postfix/smtpd[1891]: disconnect from cvsmtppost20.nm.naver.com[114.111.35.235]
```

2. MX레코드 수정 후 검증 서버에 수신 성공 로드

2. Mail Server 보안 설정

EML추출_본문

```
[root@mail goat]# python body.py
본문 추출 완료
```

```
[root@mail goat]# cd Maildir/body/
[root@mail body]# ls
1714577664_body.txt
[root@mail body]#
[root@mail body]#
[root@mail body]# cat 1714577664_body.txt

[root@mail body]#
```

↓

```
[root@mail body]# cat 1714654000_body.txt
https://www.naver.com/
```

2. Mail Server 보안 설정

EML추출_첨부파일

```
[root@mail ~]# cd /home/goat/Maildir/attachments
[root@mail attachments]# ls
4월 근무사유서 - 김근수.hwp  MT결석 협조전 수요조사(응답).xlsx  학습, 뇌, 마음 성찰일지 (13, 14, 15주차).hwpx
```

```
PS C:₩WINDOWS₩system32> scp root@175.194.34.231:/home/goat/Maildir/attachments/*.hwp C:₩
root@175.194.34.231's password:
4월 근무사유서 - 김근수.hwp                                    100%   40KB   1.5MB/s   00:00
PS C:₩WINDOWS₩system32> scp root@175.194.34.231:/home/goat/Maildir/attachments/*.xlsx C:₩
root@175.194.34.231's password:
MT결석 협조전 수요조사(응답).xlsx                             100%   17KB 662.1KB/s   00:00
```

↓

2. Mail Server 보안 설정

SpamAssassin

스팸 메일을 골라서 차단 또는 분류해주는 프로그램

실제로 여러 테스트 결과 90% 이상의 높은 차단율을 보임

---

rule 기반 하에 메일 헤더와 내용(body)을 분석

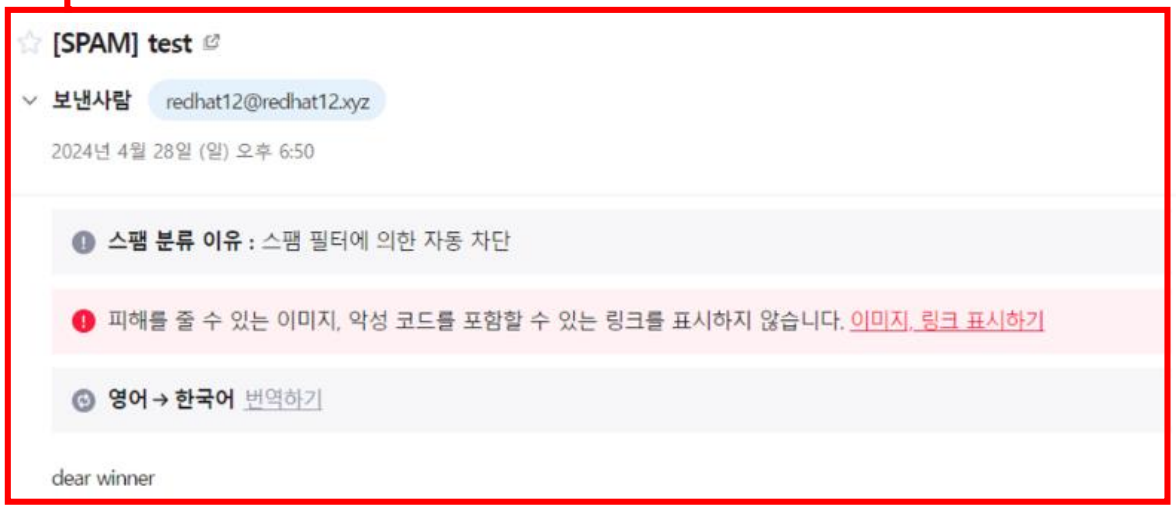
실시간 차단리스트(internet-based realtime blacklists)를 참고

각각의 룰에 매칭될 경우 +나 - 점수를 매겨 총 점수가 기준점수를 초과하는지에 따라 스팸 여부 결정

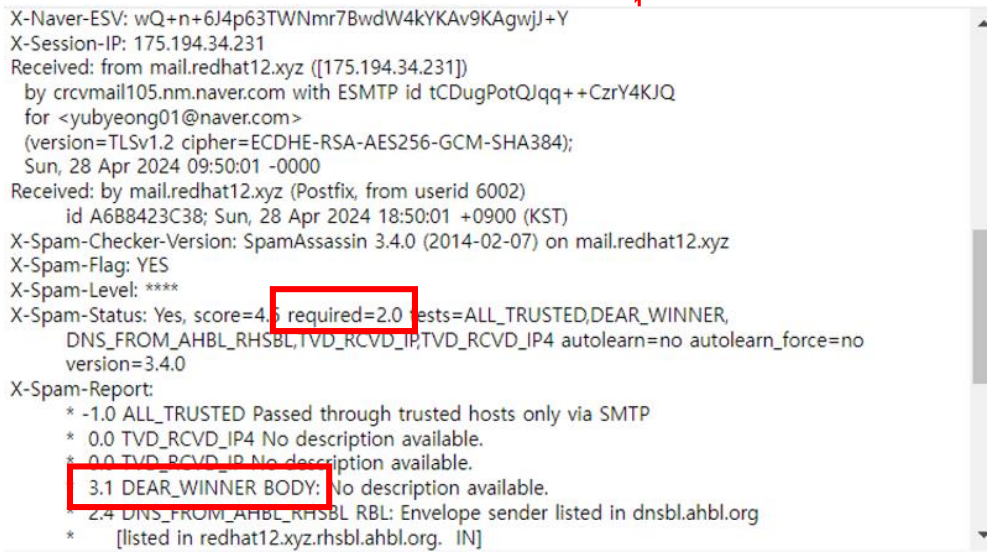
2. Mail Server 보안 설정

SpamAssassin

제목에 스팸으로 분류됨에 따라 설정했던 [SPAM] 문구가 자동 삽입



헤더 분석




```
4월  28 19:06:50 mail.redhat12.xyz spamd[2960]: spamd: connection from localhost [::1]:38916
o port 783, fd 6
4월  28 19:06:50 mail.redhat12.xyz spamd[2960]: spamd: setuid to spamd succeeded
4월  28 19:06:50 mail.redhat12.xyz spamd[2960]: spamd: processing message <88b884f25b8a533320
717c545fdea@cweb016.nm.nfra.io> for spamd:6002
4월  28 19:06:54 mail.redhat12.xyz spamd[2960]: spamd: identified spam (6.0/2.0) for spamd:60
2 in 3.7 seconds, 2475 bytes.
4월  28 19:06:54 mail.redhat12.xyz spamd[2960]: spamd: result: Y 5 - DEAR_WINNER,DKIM_SIGNED,
KIM_VALID,DKIM_VALID_AU,DNS_FROM_AHBL_RHSBL,HTML_IMAGE_ONLY_08,HTML_MESSAGE,RCVD_IN_DNSWL_LO
,RP_MATCHES_RCVD,SPF_PASS,T_REMOTE_IMAGE scantime=3.7,size=2475,user=spamd,uid=6002,required
score=2.0,rhost=localhost,raddr=::1,rport=38916,mid=<88b884f25b8a533320a717c545fdea@cweb016.
m.nfra.io>,autolearn=no autolearn_force=no
4월  28 19:06:54 mail.redhat12.xyz spamd[2959]: prefork: child states: II
4월  28 19:06:54 mail.redhat12.xyz postfix/pipe[3784]: B34B823C36: to=<goat@mail.redhat12.xyz
, orig_to=<goat@goat.pe.kr>, relay=spamassassin, delay=3.8, delays=0.04/0.01/0/3.8, dsn=2.0.
```

→ grep, spam 단어 검색으로도 확인가능

2. Mail Server 보안 설정

ClamAV

- 컴퓨터 시스템에서 악성 코드와 바이러스를 탐지하고 제거하는 오픈소스 안티바이러스 소프트웨어
- 시스템 보안을 강화하고, 악성코드에 대한 보호를 제공하는데 도움 제공
- 메일 서버, 파일 서버 ,웹 서버 등 여러 환경에서 사용

```
[root@mail Maildir]# wget https://secure.eicar.org/eicar.com
--2024-05-02 18:41:42--  https://secure.eicar.org/eicar.com
Resolving secure.eicar.org (secure.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to secure.eicar.org (secure.eicar.org)|89.238.73.97|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68
Saving to: 'eicar.com'

100%[==========================================================>] 68

2024-05-02 18:41:44 (2.13 MB/s) - 'eicar.com' saved [68/68]

[root@mail Maildir]# ls
attachments  body  clean  cur  eicar.com  header  isolation  new
```

악성코드 삽입

감염파일 탐지

```
[root@mail Maildir]# clamscan -r /home/vmail/mail.redhat12.xyz/goat/Maildir
/home/vmail/mail.redhat12.xyz/goat/Maildir/eicar.com: OK
/home/vmail/mail.redhat12.xyz/goat/Maildir/dovecot-uidlist: OK
/home/vmail/mail.redhat12.xyz/goat/Maildir/dovecot-uidvalidity.66277a1d: Empty file
/home/vmail/mail.redhat12.xyz/goat/Maildir/dovecot.index.log: OK
/home/vmail/mail.redhat12.xyz/goat/Maildir/eicar.com.1: Win.Test.EICAR_HDB-1 FOUND
/home/vmail/mail.redhat12.xyz/goat/Maildir/dovecot-uidvalidity: OK

----------- SCAN SUMMARY -----------
Known viruses: 8691892
Engine version: 0.103.11
Scanned directories: 4
Scanned files: 5
Infected files: 1
Data scanned: 0.09 MB
Data read: 0.07 MB (ratio 1.29:1)
Time: 53.757 sec (0 m 53 s)
Start Date: 2024:04:30 18:21:15
End Date:   2024:04:30 18:22:09
```

2. Mail Server 보안 설정

OLE 객체 추출

- 파이썬의 olefile, oletools 라이브러리를 사용하여 객체를 추출하고 파일형태로 저장

```
[root@mail extracted_files]# ls -l
합계 8
drwxr-xr-x 2 root root 4096  5월  31 18:28 수정.hwp
drwxr-xr-x 2 root root 4096  5월  31 18:03 패킷 분석 보고서 양식.hwp
[root@mail extracted_files]# cd 수정.hwp/
[root@mail 수정.hwp]# | ㄴ
bash: | ㄴ: 명령을 찾을 수 없습니다...
[root@mail 수정.hwp]# ls -l
합계 388
-rw-r--r-- 1 root root    473  5월  31 18:14 수정 _?HwpSummaryInformation
-rw-r--r-- 1 root root 165823  5월  31 18:15 수정 _BinData_BIN0001.PNG
-rw-r--r-- 1 root root  48193  5월  31 18:16 수정 _BinData_BIN0002.bmp
-rw-r--r-- 1 root root  75356  5월  31 18:18 수정 _BinData_BIN0003.bmp
-rw-r--r-- 1 root root   7569  5월  31 18:19 수정 _BodyText_Section0
-rw-r--r-- 1 root root    987  5월  31 18:20 수정 _DocInfo
-rw-r--r-- 1 root root    524  5월  31 18:21 수정 _DocOptions__LinkDoc
-rw-r--r-- 1 root root    256  5월  31 18:23 수정 _FileHeader
-rw-r--r-- 1 root root  63279  5월  31 18:24 수정 _PrvImage
-rw-r--r-- 1 root root   2046  5월  31 18:25 수정 _PrvText
-rw-r--r-- 1 root root    136  5월  31 18:26 수정 _Scripts_DefaultJScript
-rw-r--r-- 1 root root     13  5월  31 18:28 수정 _Scripts_JScriptVersion
```

- **추출 요소**

  매크로 (VBA 코드)

  임베디드 객체

  (문서 내의 다른 문서, 실행파일, 이미지 등)

✓ OLE 파일 구조 첨부파일 들어올 경우

객체 단위 추출하여 ClamAV에
파일단위로 넘겨 악성파일 탐지율 높임

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

2. Mail Server 보안 설정

압축 파일(zip) 포맷 추출

1718592782.Mt2.zip

```
[root@mail attachments]# cd ..
[root@mail Maildir]# cd zipfile/
[root@mail zipfile]# ls
1718592782.Mt2_zip
[root@mail zipfile]# cd 1718592782.Mt2_zip/
[root@mail 1718592782.Mt2_zip]# ls
MT▒ß╜« ╟•┤╢└ⁿ ╜÷┐Σ┤╢╗τ(└┤Σ).xlsx  ┴ñ║╕║╕╚ú╟╨└ⁿ▒º ╟╨╜.┴ª ▓│╛τ▒·┐± ╟•┤╢└ⁿ ╜÷┐Σ┤╢╗τ(└┤Σ).xlsx
[root@mail 1718592782.Mt2_zip]# |
```

첨부파일이 zip파일로 들어올 경우

↓

압축파일 안의 파일 포맷 추출하여 압축파일 내부의 파일들을 검증

2. Mail Server 보안 설정

파일 signature 검증

- Naver, Gmail의 첨부 불가능한 확장자 우회

  ↪ 악성 공격 탐지 위한 파일 Hex signature 검사하여 확장자 탐지

id	file_type	header_signature_hex	footer_signature_hex
1	PDF	25 50 44 46 2D 31 2E	25 25 45 4F 46
2	PNG	89 50 4E 47 0D 0A 1A 0A	49 45 4E 44 AE 42 60 82
3	ZIP	50 4B 03 04	50 4B 05 06
4	ALZ	41 4C 5A 01	43 4C 5A 02
5	RAR	52 61 72 21 1A 07	3D 7B 00 40 07 00
6	JPEG	FF D8 FF E0	FF D9
7	JPEG	FF D8 FF E8	FF D9
8	COM	4D 5A	
9	DLL	4D 5A	
10	DRV	4D 5A	
11	EXE	4D 5A	
12	PIF	4D 5A	
13	QTS	4D 5A	
14	QTX	4D 5A	
15	SYS	4D 5A	
16	DOCX	50 4B 03 04 14 00 06 00	50 4B 05 06
17	MP3	49 44 33 03	
18	HWP	D0 CF 11 E0 A1 B1 1A E1	NULL
19	JAR	4A 41 52 43 53 00	NULL

✓ 올바른 파일

Header signature, Footer signature
둘 다 존재하는 파일

↓

무조건 signature 둘 다 있어야 올바른 파일

2. Mail Server 보안 설정

파일 signature 검증

- 수신된 메일의 첨부파일을 open 라이브러리로 사용
  ↪ 바이너리 모드로 연 후 바이트 단위로 읽도록 진행

- 해당 첨부파일의 Header signature, Footer signature 부분
  ↪ DB에 저장시킨 각 확장자 파일의 signature와 대조 후 검증 실행

✓ DB에 저장 시킨 Header · Footer signature와
수신된 메일의 첨부파일 확장자 시그니처 부분이 같으면 변조가 되지 않은 파일로 판단

단, 둘 중 하나라도 비교하였을 때 다른 부분이 있다면 악성 파일로 판단

```
"File Signature Details": [
    "File '/home/goat/Maildir/attachments/1718785802.리버스엔지니어링 기말평가 범위(2024).p\tdf' Safe.",
    "File header signature: 25 50 44 46 2D 31 2E 36",
    "File footer signature: 65 6E 64 6F 62 6A 0D 73 74 61 72 74 78 72 65 66 0D 0A 33 32 36 32 33 0D 0A 25 25 45 4F 4

    "Checking against PDF signature:",
    "Expected header: 25 50 44 46 2D 31 2E",
    "Expected footer: 25 25 45 4F 46"
],
```

2. Mail Server 보안 설정

.json 형식 보고서


```
[root@mail FinalReport]# more 1718785802.Vfd01I200faM725070.mail.redhat12_FinalReport.json
{
    "SpamAssassin": [
        "Safe"
    ],
    "SpamAssassinDetails": [
        "X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on mail.redhat12.xyz",
        "X-Spam-Level:",
        "X-Spam-Status: No, score=1.0 required=8.0"
    ],
    "ClamAV": [
        "Safe"
    ],
    "ClamAVDetails": [
        "File '/home/goat/Maildir/attachments/1718785802.리버스엔지니어링 기말평가 범위(2024).p\tdf' scanned clean."
    ],
    "File Signature": [
        "File is safe"
    ],
    "File Signature Details": [
        "File '/home/goat/Maildir/attachments/1718785802.리버스엔지니어링 기말평가 범위(2024).p\tdf' Safe.",
        "File header signature: 25 50 44 46 2D 31 2E 36",
        "File footer signature: 65 6E 64 6F 62 6A 0D 73 74 61 72 74 78 72 65 66 0D 0A 33 32 36 32 33 0D 0A 25 25 45 4F 4
6",
        "Checking against PDF signature:",
        "Expected header: 25 50 44 46 2D 31 2E",
        "Expected footer: 25 25 45 4F 46"
    ],
    "Cuckoo": [
        "The score of this file is 2.8 out of 10."
    ],
    "CuckooDetails": [
        "{",
        "\"info\": {",
        "\"added\": 1718817090.224665,",
        "\"started\": 1718817090.677409,",
        "\"duration\": 14,",
        "\"ended\": 1718817105.00106,",
        "\"owner\": \"\",",
        "\"score\": 2.8,",
        "\"id\": 1,",
```


- json형식으로 작성 후 저장

SpamAssassin
ClamAV
파일 시그니처 검증
Cuckoo Sandbox
ML

↳ 모듈들의 검증 결과에 필요한 세부 내용들을 추출

웹 서비스에서 검증의 세부정보를 열람할 수 있도록 설정

3. Cuckoo Sandbox 설정

Cuckoo Sandbox 란?

- 오픈 소스로 이루어진 자동화된 악성 파일 분석 시스템
- 격리된 운영체제 내에서 실행 파일을 자동으로 실행, 분석하는 데에 사용

주요 기능

1. 악성코드에 의해 수행되는 Window API 함수 호출 추적
2. 악성코드에 의해 파일 생성 및 복사, 삭제 확인
3. 선택 프로세스 메모리 덤프, 분석 시스템 전체 메모리 덤프
4. 악성코드 실행하는 동안 스크린샷 (process explorer)
5. 네트워크 덤프 (PCAP format)
6. Virustotal 검색 결과 (기본으로 연결, 사용 유무 설정 가능)
7. 패턴 이용하여 악성코드 식별 및 분류 (yara 설치)
8. 네트워크 트래픽 분석 (TCP dump 설치)
9. 분석을 위한 가상환경 구성 (Virtualbox 설치)

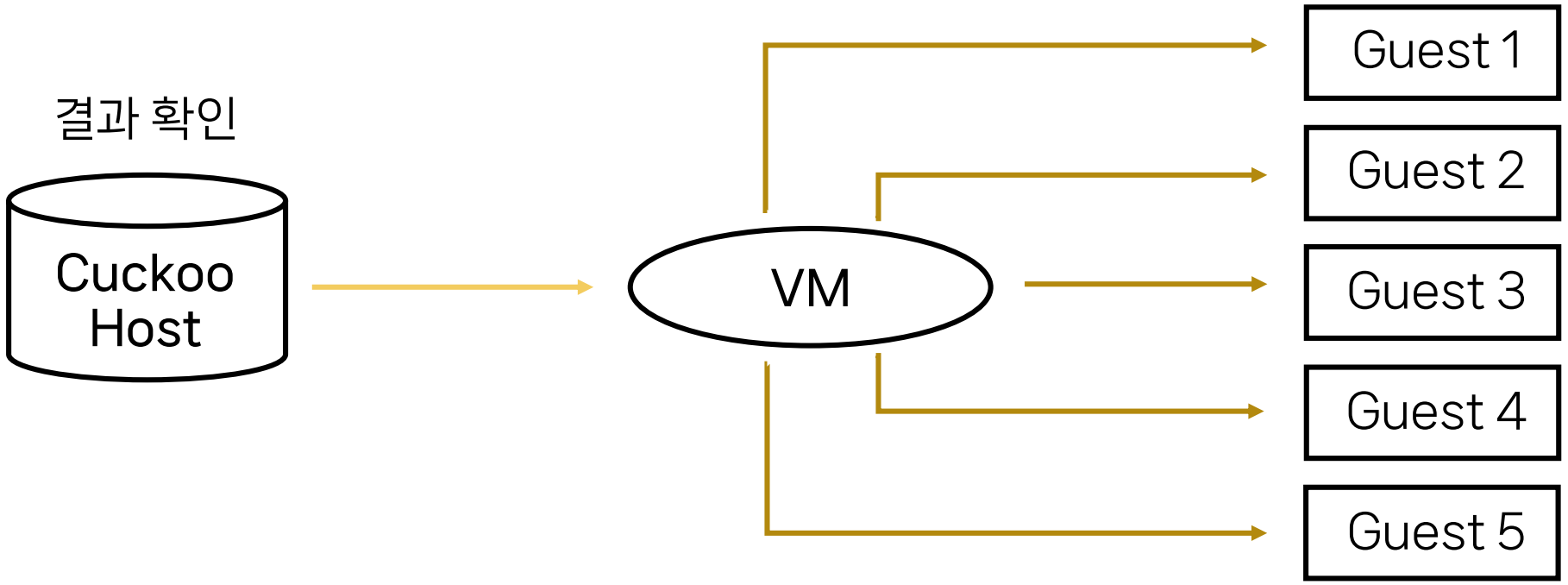
분석 가능 파일

- 실행파일
- DLL파일
- PDF 문서
- MS office 문서
- URLs 및 HTML 파일
- ZIP 파일
- JAVA 파일
- Python 파일
- PHP 스크립트
- 한컴 오피스

3. Cuckoo Sandbox 설정

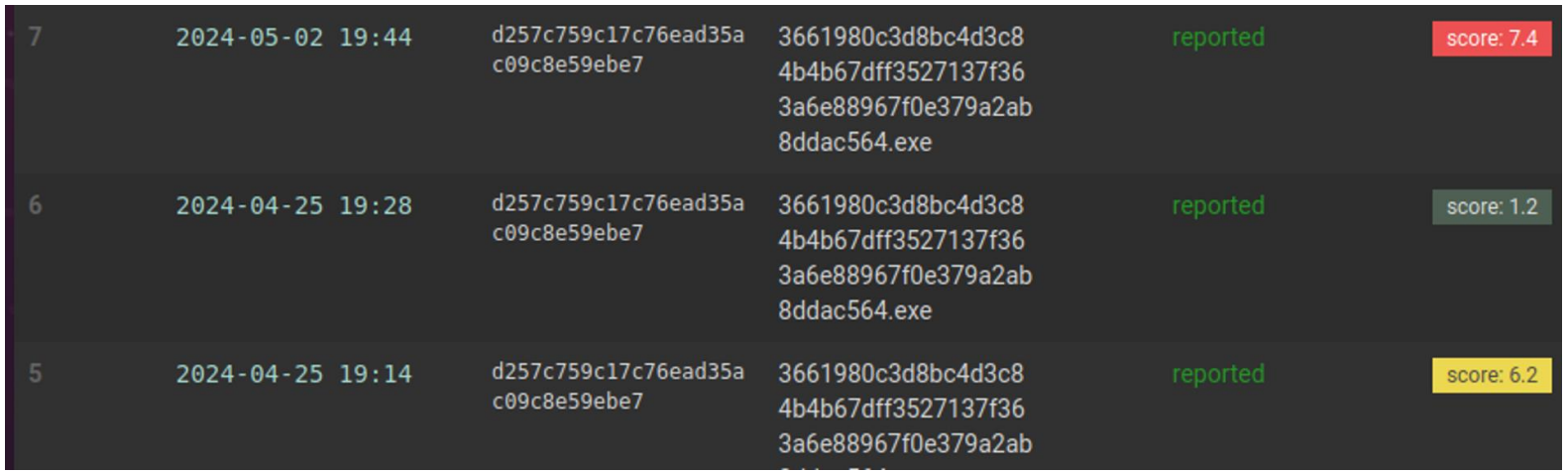
Cuckoo Sandbox 로직

- 5대의 분석 머신으로 host 결과 확인



3. Cuckoo Sandbox 설정

Cuckoo Sandbox 모듈



7	2024-05-02 19:44	d257c759c17c76ead35ac09c8e59ebe7	3661980c3d8bc4d3c84b4b67dff3527137f363a6e88967f0e379a2ab8ddac564.exe	reported	score: 7.4
6	2024-04-25 19:28	d257c759c17c76ead35ac09c8e59ebe7	3661980c3d8bc4d3c84b4b67dff3527137f363a6e88967f0e379a2ab8ddac564.exe	reported	score: 1.2
5	2024-04-25 19:14	d257c759c17c76ead35ac09c8e59ebe7	3661980c3d8bc4d3c84b4b67dff3527137f363a6e88967f0e379a2ab	reported	score: 6.2

Volatility, Suricata, Yara Rule 추가

⟶ 초기 대비 탐지 스코어 상승

- Volatility

  시간대비 탐지율 결과
  API Hooks 기능 제외

- Suricata

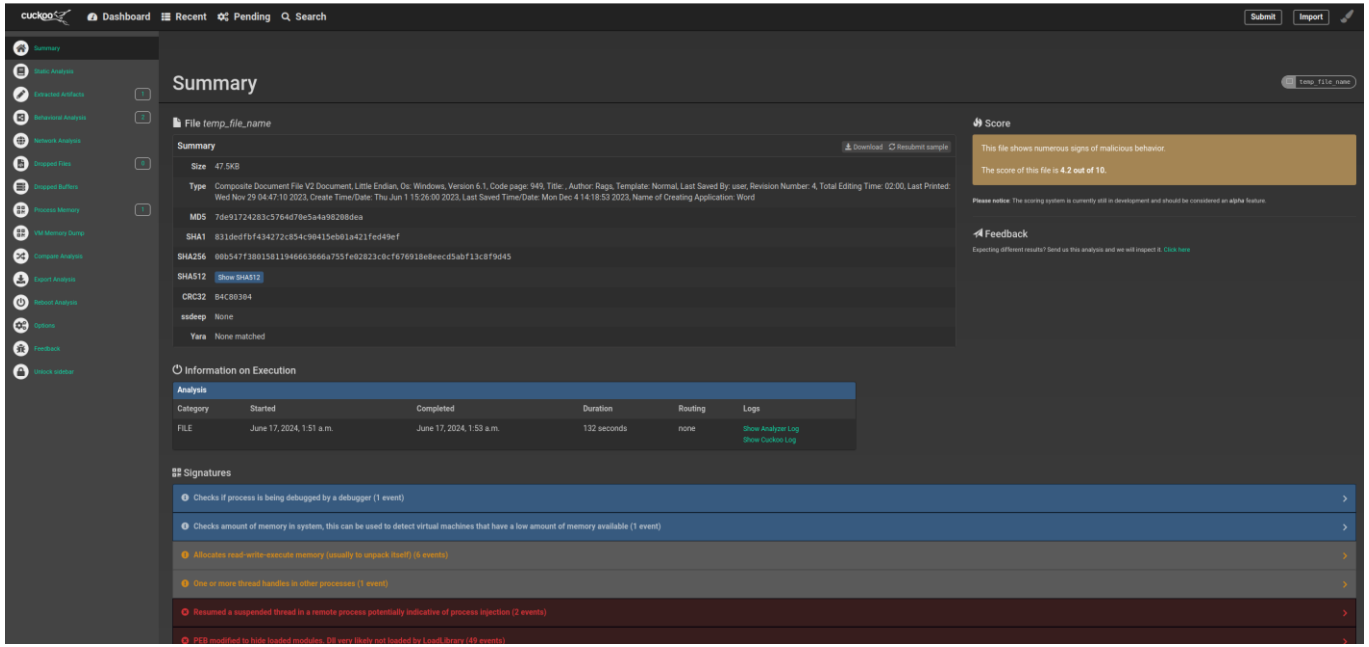
  지속적인 업데이트
  가장 최신의 룰 사용 가능

- Yara Rule

  최신 버전의 룰 업데이트
  시그니처 베이스의 딥한 검사

3. Cuckoo Sandbox 설정

Cuckoo Sandbox 검사



사용자가 보낸 메일의 첨부파일을 검사

실행형 첨부파일, 문서형 첨부파일 모두 동적 검사

파일이 확인되면 검사 진행

↓

설치된 가상환경에서 파일 실행하여 동적 검사 진행

위 사진과 같이 검사 결과를 받을 수 있고,

사용자는 이 중 스코어, 요약본을 받을 수 있도록 설정했다.

4. 머신러닝 학습

NB + RF + LR + EN

4개 모델 결합하여 최적의 결과

- VotingClassifier
  앙상블 모델 생성
- GridSearchCV
  각 모델의 최적 하이퍼파리미터 탐색

피처

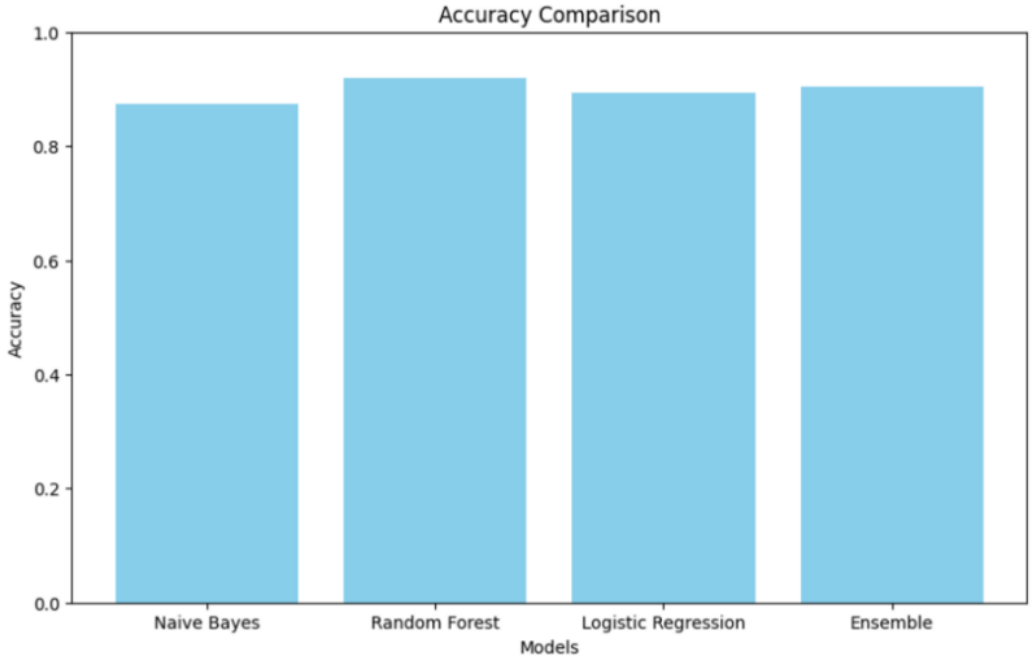
총 42개의 피처 생성

코드 수행

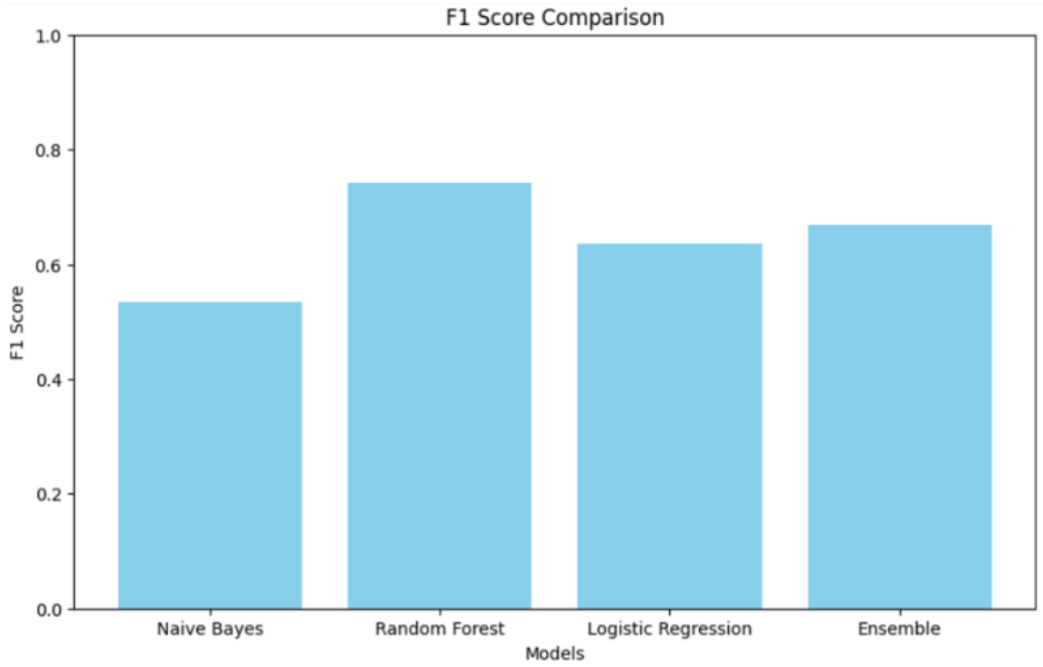
1. **피처 스케일링**
   피처 스케일링 수행
2. **피처 선택**
   상위 피처 선택
3. **모델 학습 및 튜닝**
   최적의 하이퍼파리미터 탐색, 모델 학습
4. **앙상블 모델**
   최적의 모델 결합, 앙상블 모델 학습
5. **성능 평가**
   정확도와 F1 스코어 그래프로 시각화
6. **오탐 방지**
   혼동 행렬 시각화, 오탐 관련 문제 확인

4. 머신러닝 학습

NB + RF + LR + EN



랜덤 포레스트, 앙상블 모델의 높은 정확도

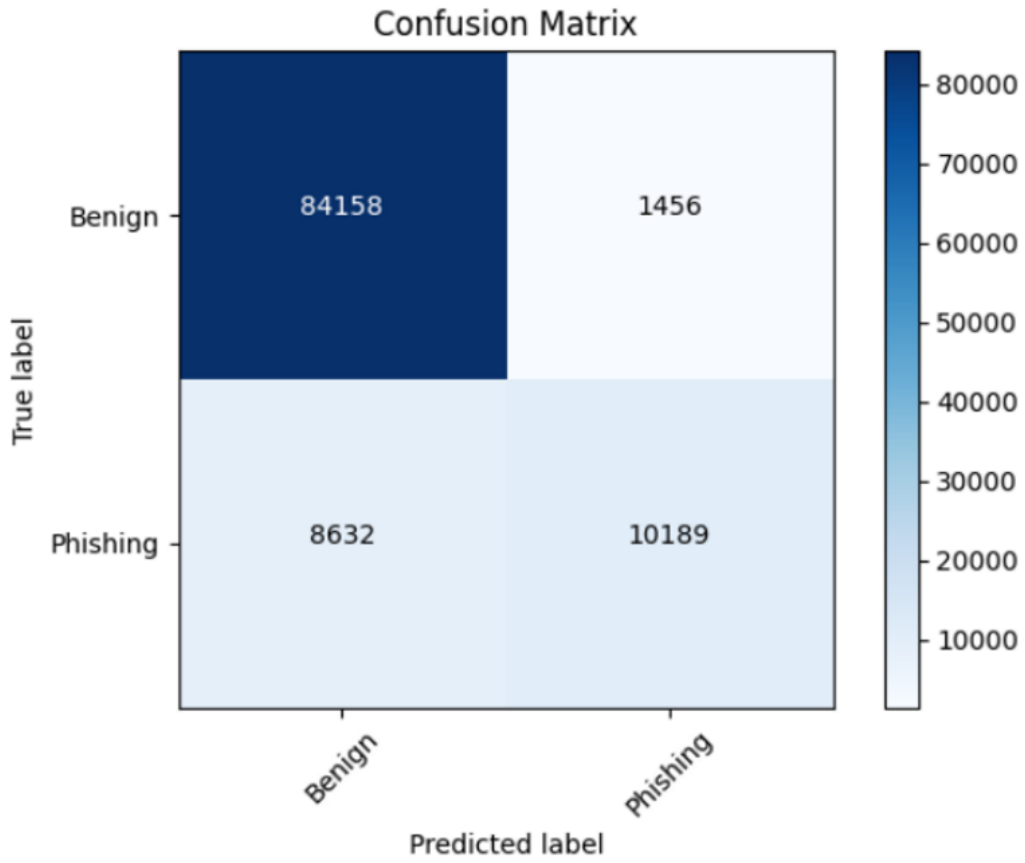


랜덤 포레스트가 가장 높은 F1 점수를

가지고 있어 정밀도와 재현율 사이의 균형이 가장 좋음

4. 머신러닝 학습

NB + RF + LR + EN



- True Positive (TP)
  정확하게 피싱으로 예측된 수 - 10189
- True Negative (TN)
  정확하게 양성으로 예측된 수 - 84158
- False Positive (FP) - 미탐
  피싱으로 잘못 예측된 수 - 1456
- False Negative (FN) - 오탐
  양성으로 잘못 예측된 수 - 8632

! 전반적으로, Benign 샘플을 잘 예측
Phishing 샘플 재현율 낮아 개선 필요

4. 머신러닝 학습

NB + RF + LR + EN + 재현율 개선

Phishing 샘플 재현율 개선

- SMOTE (Synthetic Minority Over-sampling Technique)
  데이터 불균형 처리
- class_weight
  더 많은 Phishing 샘플 예측 유도

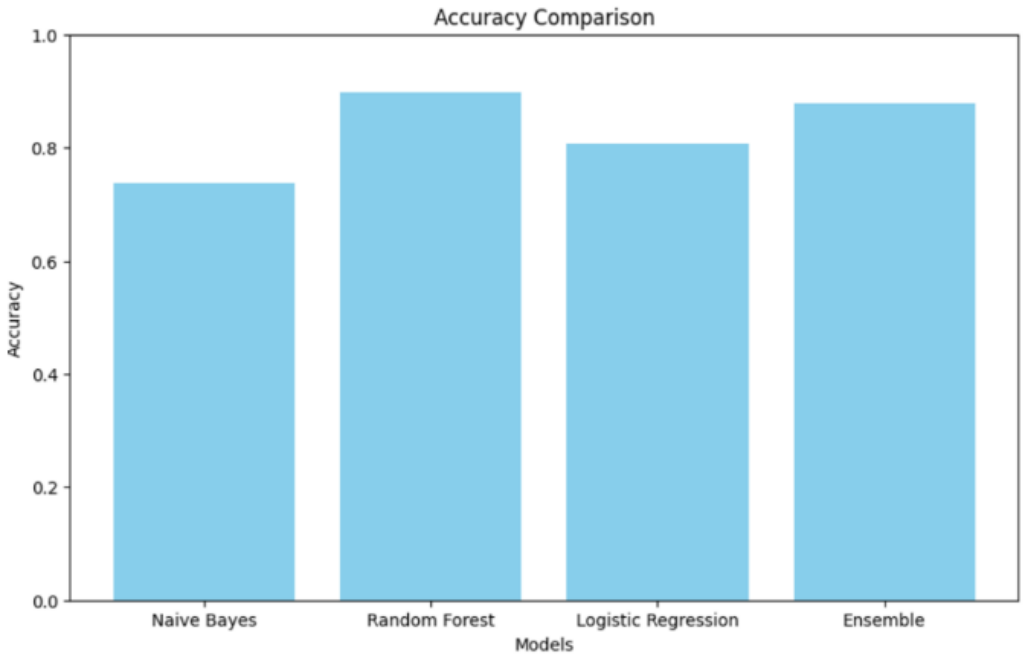
피처

총 42개의 피처 생성

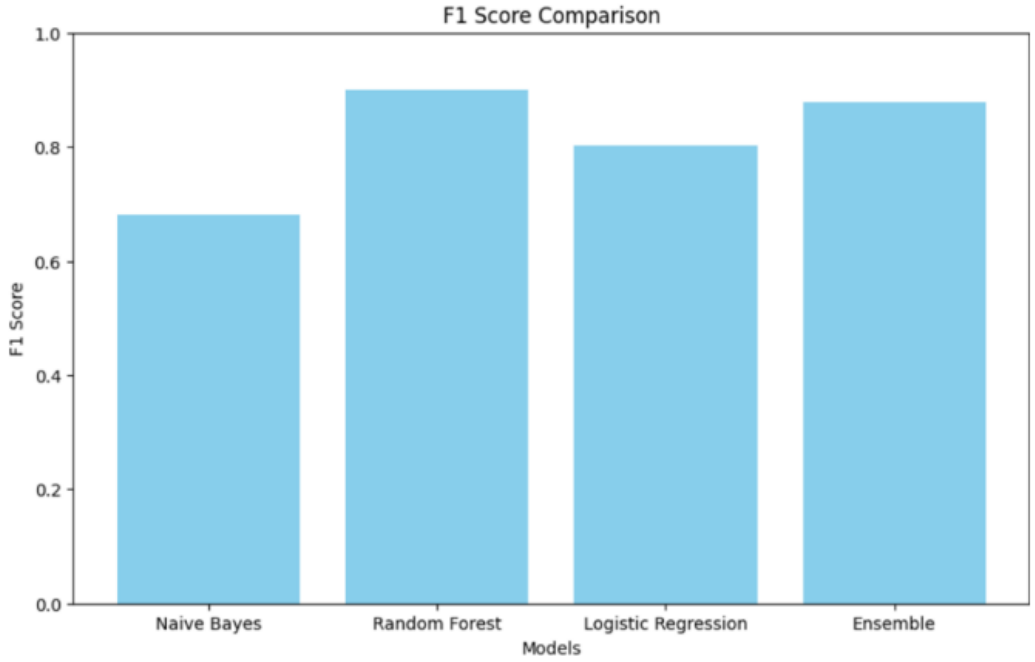
✓ URL 데이터를 효과적으로 전처리 가능
Phishing 샘플에 대한 재현율을 높이면서 다양한 모델을 학습 및 평가 가능

4. 머신러닝 학습

NB + RF + LR + EN + 재현율 개선



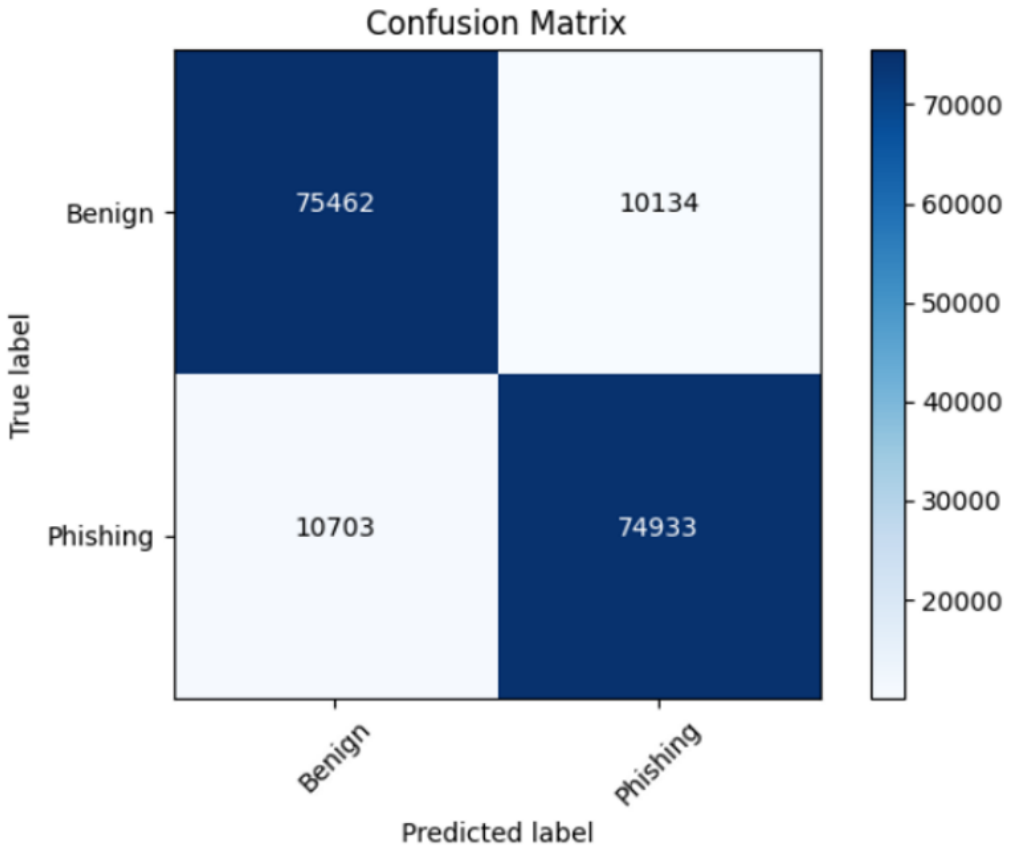
랜덤 포레스트 모델의 높은 정확도



랜덤 포레스트 모델의 가장 높은 F1 수치

4. 머신러닝 학습

NB + RF + LR + EN + 재현율 개선

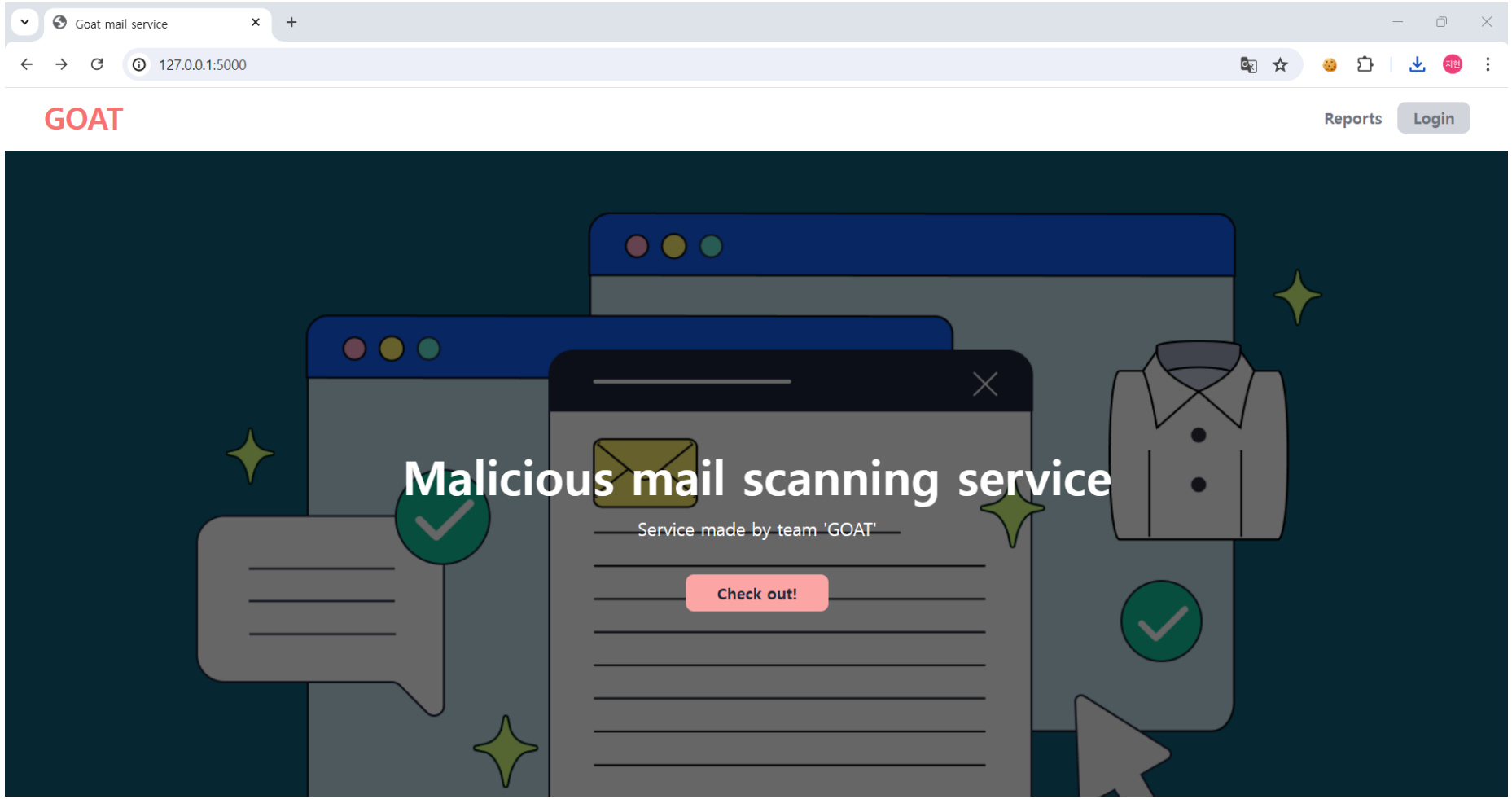


- True Positive (TP) : 75462
- True Negative (TN) : 74933
- False Positive (FP) – 미탐 : 10134
- False Negative (FN) – 오탐 : 10703

! Benign과 Phishing 샘플을 예측하는 데 전반적으로 높은 정확도와 정밀도, 재현율 보유

5. DB 구축

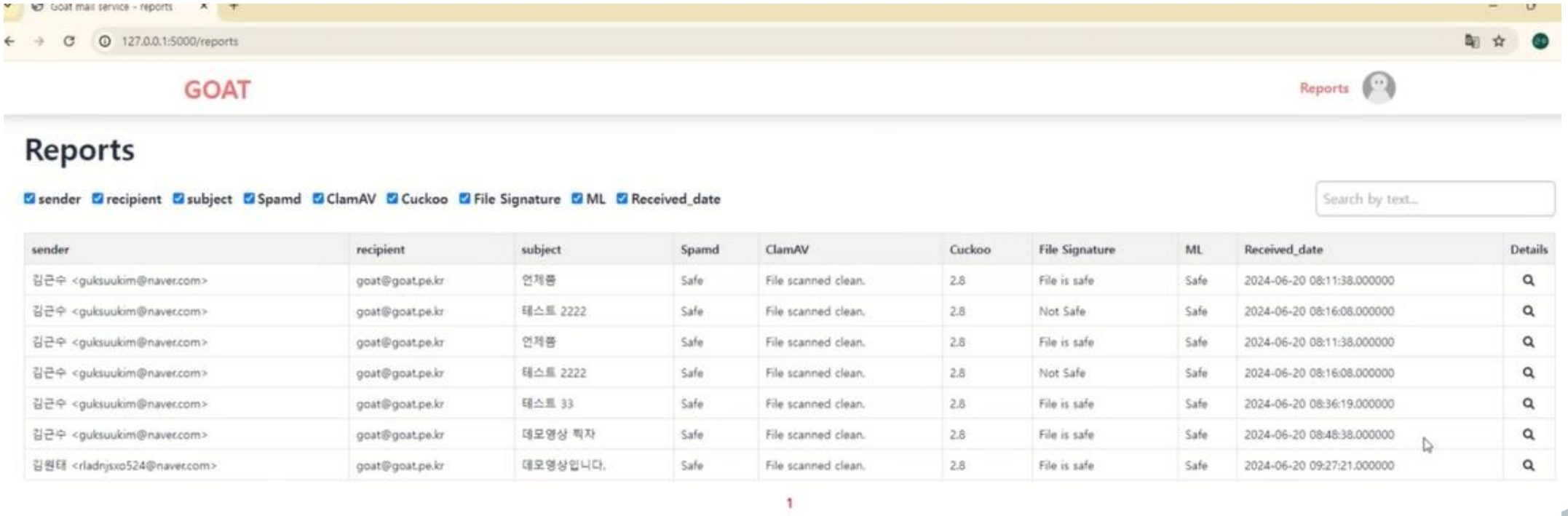
Flask + MySQL_Main 화면



5. DB 구축

Flask + MySQL_DB 화면

id	Sender	recipient	subject	Spamd	ClamAV	Cuckoo	File Signature	ML	Received_date
1	김근수 <guksuukim@naver.com>	goat@goat.pe.kr	테스트	Safe	File scanned clean.	2.8	File is safe	Safe	2024-06-19 20:08:55.000000
2	김근수 <guksuukim@naver.com>	goat@goat.pe.kr	테스트2	Safe	File scanned clean.	2.8	File is safe	Safe	2024-06-19 21:15:03.000000
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

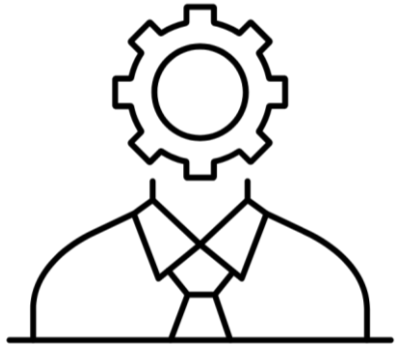


3 프로젝트 결과

1. 향후 계획

2. 최종 목표

1. 향후 계획



각 사용자의 관리자 페이지 구현

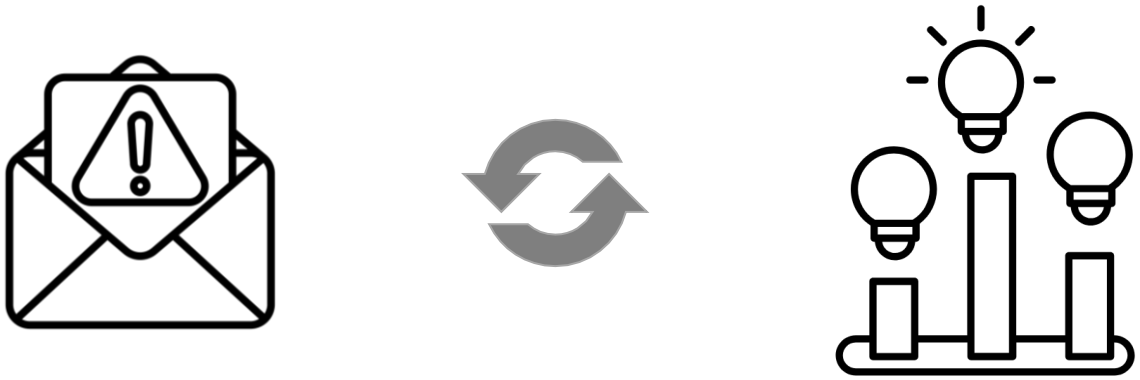
보다 쉽게 확인할 수 있도록 보완

1. 향후 계획

hwp 등 국내에서 자주 사용하는

파일 및 확장자에 대한 모듈 고도화

1. 향후 계획

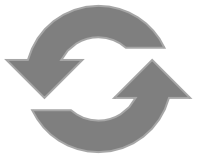


여러 모듈 중 하나라도 악성 탐지 시 악성메일로 분류

↓

스코어링 전략을 체계적으로 수립

2. 최종 목표



오픈 소스 제공

↓

영세사업자 & 기업을 위한 ETP 솔루션 제공,

많은 사람들이 무료로 가져다 사용할 수 있는 장점

CCIT
CULTURE CONTENTS & INFORMATION TECHNOLOGY

감사합니다.