2025 졸업프로젝트 결과 발표회

악성 문서 중심의 이메일 솔루션 개발

2025. 11. 04.

팀 명 ROAT

중부대학교 정보보호학전공

1

CONTENT

01 프로젝트 소개
- 1 팀원 소개
- 2 주제 선정

02 프로젝트 계획
- 1 프로젝트 구상도
- 2 검증 로직

03 프로젝트 진행
- 1 Mail Server 보안 설정
- 2 Cukoo Sandbox 설정
- 3 정적 분석기 개발
- 4 DB 구축

04 프로젝트 결과
- 1 프로젝트 결과물
- 2 향후 계획

2

1. 팀원 소개

· 총괄

· 메일 서버 구축, 설정

· Cuckoo 구축, 설정

· HWP/HWPX 파일 분석

· DB 구축, WEB 개발

2. 주제 선정

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

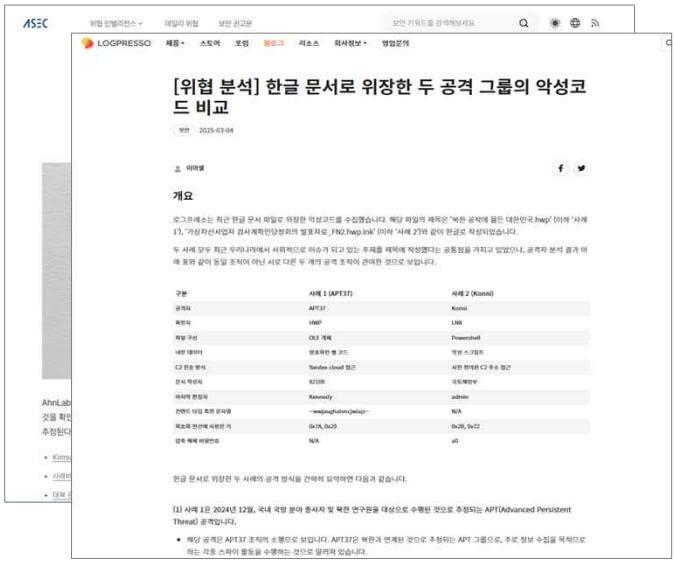
↓

이메일 검사, 의심스러운 링크 뿐 아니라 악성 문서 분석을 통해 탐지 기술 연구

↓

사용자의 보안 취약성을 해결, 사이버 보안을 강화

2. 주제 선정



최근까지 악성메일에 대한
피해가 꾸준히 지속되고 있는 사실 확인

↓

이메일 검사, 의심스러운 링크 뿐 아니라 악성
문서 분석을 통해 탐지 기술 연구

↓

사용자의 보안 취약성을 해결, 사이버 보안을 강화

1. 프로젝트 구상도

· 수신자에게 메일 발송

검증 메일 서버 → 초기 메일 보안 검사 → EML 프로세싱

· SPF, DKIM, DMARC

· MX레코드 수정

Header
Body
Spam Assassin

Attachment
· Hex 시그니처 – Python 모듈
· 첨부 파일 추출 – Cuckoo, ClamAV
· OLE 객체 추출 – ClamAV

DB 저장 → WEB

· MySQL
· Flask

분류 → · Clean 메일만 회신 → 수신자

· Clean or Problem

2. 검증 로직

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. 검증 로직

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

2. 검증 로직

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

2. 검증 로직

한글 파일(hwp, hwpx)

hwp

파일 특성
· OLE(Object Linking and Embedding)

파일 형식
· Compound File Binary Format

파일 구조
· Compound 파일 구조

가독성
· 이진 형식, 가독성 낮음

hwpx

파일 특성
· OOXML(Office Open XML)

파일 형식
· ZIP 아카이브로 압축된 XML 파일들의 집합

파일 구조
· 개별 파일로 구성된 ZIP 아카이브 구조

가독성
· XML 기반, 가독성 높음

2. 검증 로직

한글 파일(hwp, hwpx)

hwp

📁 **파일 특성**
· OLE(Object Linking and Embedding)

📌 **파일 형식**
· Compound File Binary Format

🛡️ **파일 구조**
· Compound 파일 구조

⚠️ **가독성**
· 이진 형식, 가독성 낮음

1. HWP 내부 분석 (OLE 개체 탐지)
2. ClamAV를 활용해 단위 별로 추출 하여 검증
3. 검증 로직 구현

2. 검증 로직

한글 파일(hwp, hwpx)

1. HWPX 내부 분석 (xml 파일 파싱)
2. 검증 로직 구현

hwpx

📁 **파일 특성**
· OOXML(Office Open XML)

📌 **파일 형식**
· ZIP 아카이브로 압축된 XML 파일들의 집합

🛡️ **파일 구조**
· 개별 파일로 구성된 ZIP 아카이브 구조

⚠️ **가독성**
· XML 기반, 가독성 높음

1. Mail Server 보안 설정

SpamAssassin

제목에 스팸으로 분류됨에 따라 설정했던 [SPAM] 문구가 자동 삽입

헤더 분석

```
X-Spam-Checker-Version: SpamAssassin 3.4.0 (2014-02-07) on mail.redhat12.xyz
X-Spam-Level: **
X-Spam-Status: No, score=3.0 required=8.0 tests=DEAR_WINNER,DKIM_SIGNED,
        DKIM_VALID,DKIM_VALID_AU,FREEMAIL_FROM,HTML_MESSAGE,RCVD_IN_DNSWL_NONE,
        RCVD_IN_MSPIKE_H2,RCVD_IN_VALIDITY_RPBL_BLOCKED,RCVD_IN_VALIDITY_SAFE_BLOCKED,
        SPF_HELO_NONE,SPF_PASS,TVD_SPACE_RATIO,T_SCC_BODY_TEXT_LINE autolearn=no
        autolearn_force=no version=3.4.0
```

```
4월  28 19:06:50 mail.redhat12.xyz spamd[2960]: spamd: connection from localhost [::1]:38916
 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

1. 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%[=============================================

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

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

악성코드 삽입

감염파일 탐지

```
File '/home/goat/Maildir/attachments/1760434138.7050af905f1696b2b8cdb4c6e6805a618addf5acfbd4edc3fc807a663016ab26.hwp' co
ntains virus/malware:
/home/goat/Maildir/attachments/1760434138.7050af905f1696b2b8cdb4c6e6805a618addf5acfbd4edc3fc807a663016ab26.hwp: Win.Troj
an.Dropper-9787492-1 FOUND

----------- SCAN SUMMARY -----------
Known viruses: 8708306
Engine version: 0.103.11
Scanned directories: 0
Scanned files: 1
Infected files: 1
Data scanned: 0.19 MB
Data read: 0.14 MB (ratio 1.36:1)
Time: 136.632 sec (2 m 16 s)
Start Date: 2025:10:14 18:29:05
End Date:   2025:10:14 18:31:21
```

1. 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▒° ╟╨╜.┴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

1. 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 파일이란?**

-> Header signature, Footer signature 둘 다 존재하는 파일

↓

무조건 signature 둘 다 있어야 올바른 파일

1. Mail Server 보안 설정

파일 signature 검증

· 수신된 메일의 첨부파일을 open 라이브러리로 사용
  ㄴ 바이너리 모드로 연 후 바이트 단위로 읽도록 진행

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

ㄴ 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"
],
```


1. Mail Server 보안 설정

.json 형식 보고서

· **json형식으로 작성 후 저장**
SpamAssassin
ClamAV
파일 시그니처 검증
Cuckoo Sandbox
정적 분석 결과(한글)
ㄴ 모듈들의 검증 결과에 필요한 세부 내용들을 추출

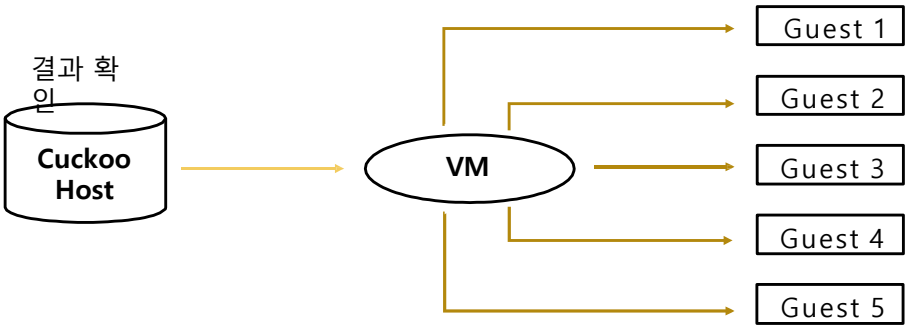
웹 서비스에서 검증의 세부정보를
열람할 수 있도록 설정


```
{
    "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=3.0 required=8.0"
    ],
    "ClamAV": [
        "File contains virus/malware."
    ],
    "ClamAVDetails": [
        "File '/home/goat/Maildir/attachments/1760434138.7050af905f1696b2b8cdb4c6e6805a618addf5acfbd4edc3fc807a663016ab26.hwp' contains virus/malware:
",
        "/home/goat/Maildir/attachments/1760434138.7050af905f1696b2b8cdb4c6e6805a618addf5acfbd4edc3fc807a663016ab26.hwp: Win.Trojan.Dropper-9787492-1
FOUND",
        "",
        "----------- SCAN SUMMARY -----------",
        "Known viruses: 8708306",
        "Engine version: 0.103.11",
        "Scanned directories: 0",
        "Scanned files: 1",
        "Infected files: 1",
        "Data scanned: 0.19 MB",
        "Data read: 0.14 MB (ratio 1.36:1)",
        "Time: 136.632 sec (2 m 16 s)",
        "Start Date: 2025:10:14 18:29:05",
        "End Date:   2025:10:14 18:31:21",
        ""
    ],
```

2. Cuckoo Sandbox 설정

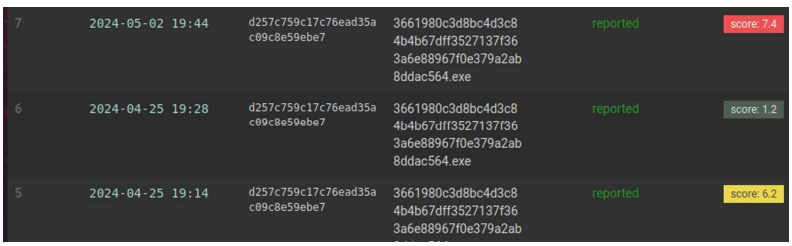
Cuckoo Sandbox 로직

· 여러대의 분석 머신으로 host 결과 확인



2. Cuckoo Sandbox 설정

Cuckoo Sandbox 모듈



Volatility, Suricata, Yara Rule 추가

⟶ 초기 대비 탐지 스코어 상승

· **Volatility**

시간대비 탐지율 결과
API Hooks 기능 제외

· **Suricata**

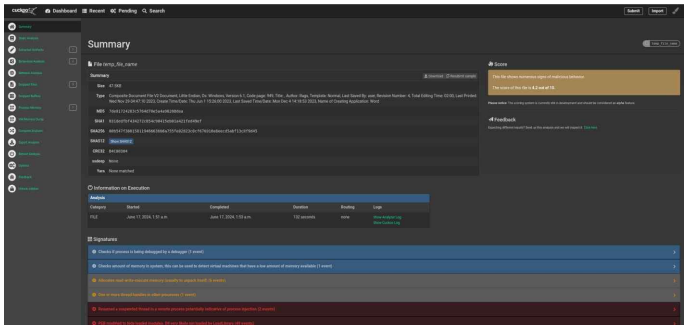
지속적인 업데이트로 가장 최신의 룰 사용 가능

· **Yara Rule**

최신 버전의 룰 업데이트로 시그니처 베이스의 딥한 검사

2. 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 설정

3. 정적 분석기 개발

HWP 주요 섹션

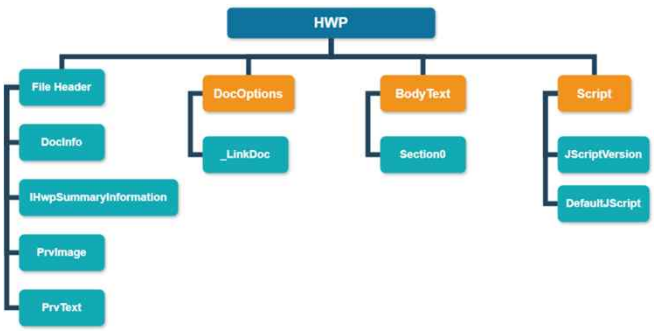
FileHeader: 매직, 버전, 암호화 플래그

DocInfo: 문서 메타데이터, 스트림 포인터

BodyText/Sections: 본문 내용 저장 영역

BinData: 이미지·임베디드 오브젝트(PE, WMF, EPS 등)

OLE Storage: 스트림/스토리지 계층
-> OLE 컨테이너 기반 임베디드 실행 객체 가능



3. 정적 분석기 개발

HWPX 주요 섹션

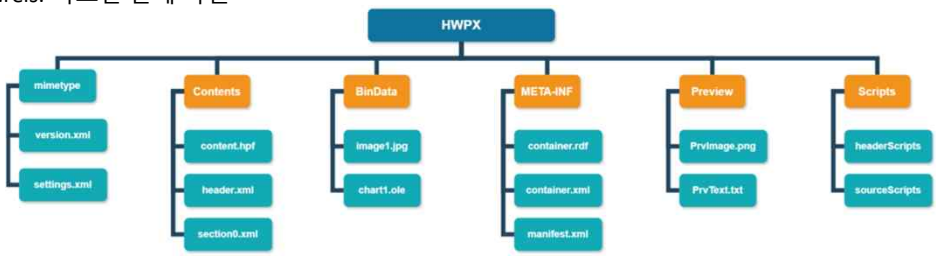
Contents: 문서 본문 및 스타일 정의

BinData: 이미지·OLE·WMF 등 임베디드 바이너리 파일 데이터

META-INF: 패키지 메타데이터 및 파일 관계 정의

Preview: 미리보기 이미지 및 텍스트

_rels/.rels: 파트간 관계 파일



3. 정적 분석기 개발

HWP / HWPX 관련 공격

1. 임베디드 실행파일(OLE Packager)
-> Ole10Native 등에 EXE/스크립트 삽입 → 사용자 상호작용으로 실행 유도

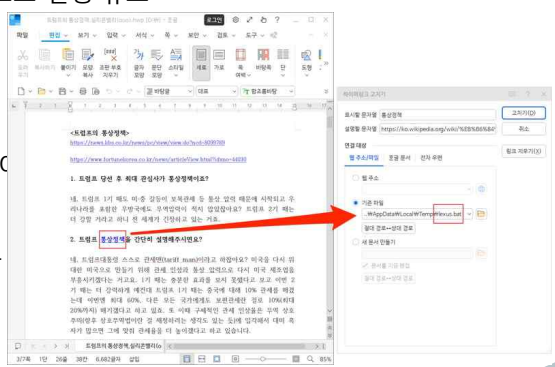
2. 이미지 렌더러 취약점 (WMF/EMF)
-> 특수 레코드로 렌더러 트리거 → 메모리 손상 → 코드 실행

3. EPS / PostScript 악용
-> exec/run/system 등 위험 연산자 또는 Ghostscript 취약점 C

4. HWPX 구조 조작 (타입 혼동 / 정수 오버플로우)
-> XML/파트 조작 → 길이/카운터 오버플로우로 힘 손상 유도

5. 외부 리소스 로드 (.rels TargetMode="External")
-> 원격 페이로드 또는 리소스 로드로 2차 공격 연결

6. 은닉·다중 레이어(압축·인코딩)
-> zlib/Base64 등으로 은닉 후 재검출 회피 시도



악성 OLE 데이터가 포함된 HWP 문서

3. 정적 분석기 개발

HWP/HWPX 가중치 설정

1. 포맷/컨테이너 불일치
-> .hwp인데 OLE 아님: +3
-> FileHeader 암호화 비트 설정: +3

2. 임베디드 매직 / 실행성 징후
-> PE/ZIP/7z/RAR/EPS/WMF 등 매직 감지: +2
-> WMF 발견 → 추가 +2
-> 실행성 확장자(.exe/.dll/.js 등) 포함: +2

3. EPS (PostScript)연산자
-> Mild (file/filter/putinterval 등): +2
-> Danger (exec/system/run): +3
-> 압축 해제 후 EPS 재검출: +3 (은닉 정황)

4. URL·링크 위험성
-> IP 기반 URL: +2 / 단축 URL: +1 / 비표준 포트: +1

5. 보조 신호(난독·대용량 등)
-> 고엔트로피(≥7.5): +1 / 대용량 블롭(≥200KB): +1

6. 파싱 에러 / BadZip: +1

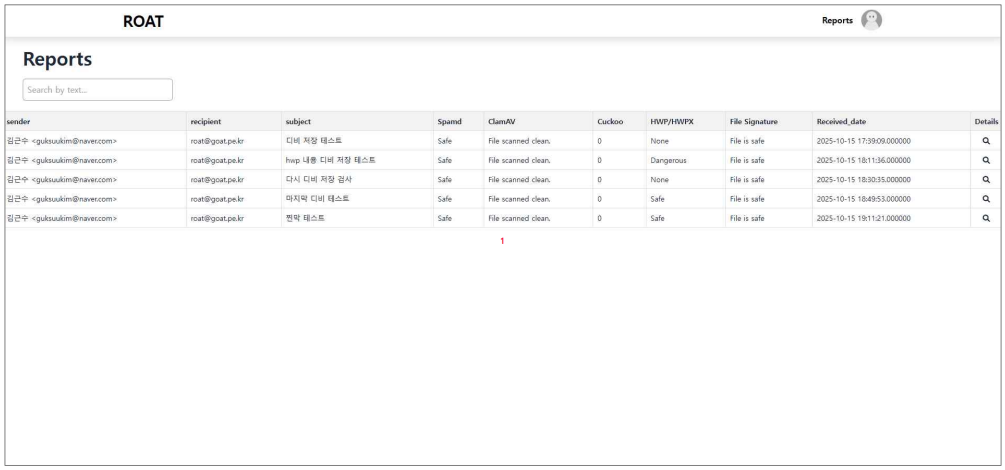
3. 정적 분석기 개발

HWP/HWPX 정적 분석 결과


```
"HWP/HWPX Analysis": [
    {
        "file": "1760432216.7050af905f1696b2b8cdb4c6e6805a618addf5acfbd4edc3fc807a663016ab26.hwp",
        "type": "HWP",
        "indicators": [
            "Info: FileHeader present (size=256)",
            "Warn: EPS ops in stream BinData/BIN0001.png: file",
            "Info: High entropy blob in BinData/BIN0001.png (>=7.5)",
            "Warn: EPS ops after decompress in BinData/BIN0001.png: file",
            "Warn: EPS ops in stream BinData/BIN0001.png (decompressed): file",
            "Info: High entropy blob in BinData/BIN0002.png (>=7.5)",
            "Info: High entropy blob in BinData/BIN0003.jpg (>=7.5)",
            "Info: High entropy blob in BinData/BIN0004.jpg (>=7.5)",
            "Info: High entropy blob in BinData/BIN0005.ps (>=7.5)",
            "Warn: EPS ops after decompress in BinData/BIN0005.ps: exec",
            "Warn: EPS ops in stream BinData/BIN0005.ps (decompressed): exec",
            "Info: Streams=14, Storages=4, BodyText sections=1, BinData=6, OleLike=0"
        ],
        "bin_hits": [],
        "links": [],
        "structure": {
            "streams": 14,
            "storages": 4,
            "body_sections": 1,
            "has_docinfo": true,
            "has_summaryinfo": true,
            "bindata_count": 6,
            "ole_like_count": 0
        },
        "score": 10,
        "classification": "malicious"
    },
```

4. DB 구축

Flask + MySQL_Main 화면



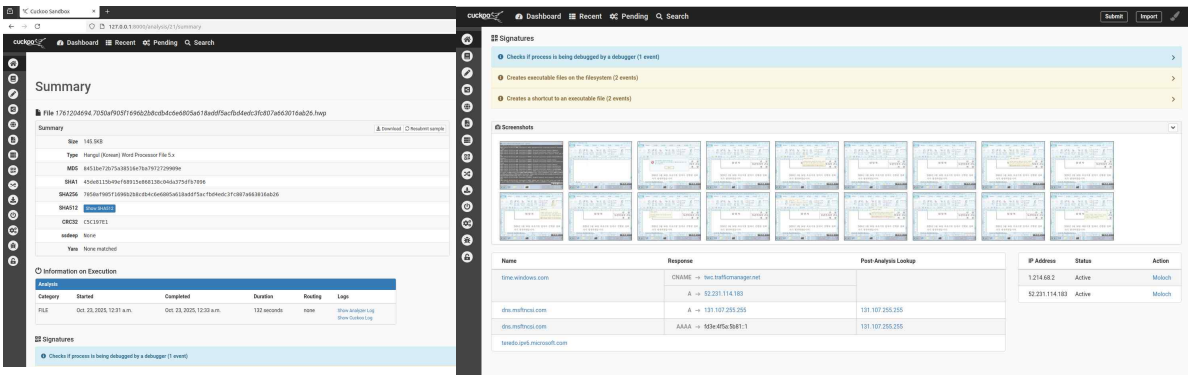
4. DB 구축

Flask + MySQL_DB 화면

id	Sender	recipient	subject	Spamd	ClamAV	Cuckoo	HWP/HWPX	File Signature	Received_date	json
12	김근수 <guksuukim@naver.com>	roat@goat.pe.kr	hwp 내용 디비 저장 테스트	Safe	File scanned clean.	0	Dangerous	File is safe	2025-10-15 18:11:36.000000	{"SpamAssassin": ["Safe"], "SpamAssass
14	김근수 <guksuukim@naver.com>	roat@goat.pe.kr	마지막 디비 테스트	Safe	File scanned clean.	0	Safe	File is safe	2025-10-15 18:49:53.000000	{"SpamAssassin": ["Safe"], "SpamAssass
15	김근수 <guksuukim@naver.com>	roat@goat.pe.kr	찐막 테스트	Safe	File scanned clean.	0	Safe	File is safe	2025-10-15 19:11:21.000000	{"SpamAssassin": ["Safe"], "SpamAssass
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

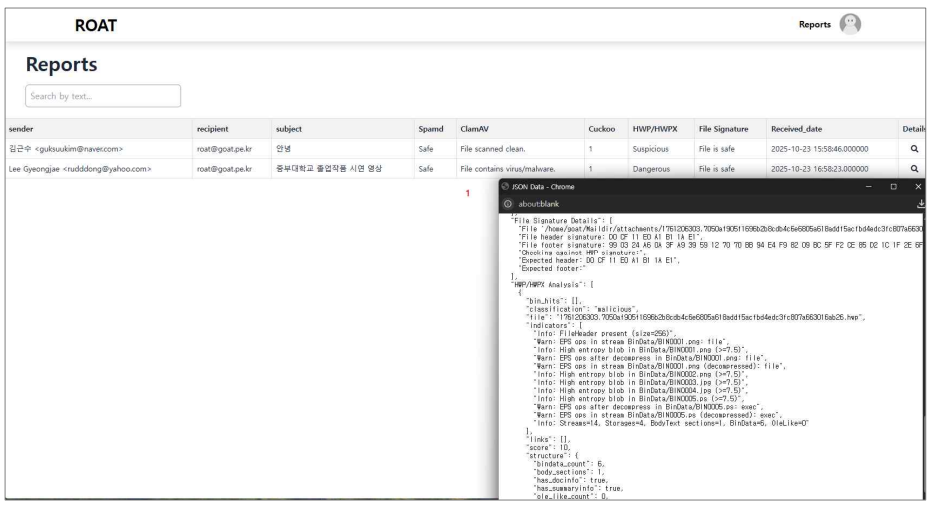
1. 프로젝트 결과물

Cuckoo SandBox 결과



1. 프로젝트 결과물

정적 분석기 결과



2. 향후 계획

오픈 소스 제공

↓

영세사업자 & 기업을 위한 ETP 솔루션 제공,

많은 사람들이 무료로 가져다 사용할 수 있는 장점

2025. 11. 04.
졸업 프로젝트 결과 발표회

Thank You

감사합니다. ☺