|  |  |  |  |
| --- | --- | --- | --- |
| **과제제안서** | | | |
| 교과목명 | ALML응용프로젝트1 | 교과목번호 | 101717-001 |
| 학점(설계)/시수 | 3학점/3시수 | | |
| 개설학과(학년) | 4학년 | 담당교수 | 김은삼 |
| 과제명 | 랜섬웨어 탐지 프로그램 | | |
| 팀명 | WatchService | | |
| 팀원 | 학번 | 이름 | 연락처/e-mail |
| C135086 | 김유민 | 010-3742-9043 / rladbals0329@gmail.com |
| B898061 | 이상혁 | 010-8389-9759 / patas1018@gmail.com |
|  |  |  |
|  |  |  |

**1. 과제 개요**

현대의 랜섬웨어 공격은 사용자의 문서, 사진, 업무 파일 등을 암호화한 뒤 금전을 요구하는 방식으로 심각한 피해를 유발하고 있습니다. 본 프로젝트에서는 폴더 및 파일 감시 기능(WatchService)을 기반으로 한 에이전트 프로그램을 제작하여, 사용자의 PC에서 발생하는 파일 이벤트를 실시간으로 수집하고, 이를 AI 모델을 통해 분석하여 랜섬웨어 여부 및 종류(페밀리)를 탐지하는 시스템을 개발하려고 합니다. 사용자는 프로그램 설치만으로 자동 탐지가 가능하며, 의심 행위 발생 시 즉각적인 알림을 받아 보안 위협에 신속히 대응할 수 있을 것입니다.

**2. 필요성 및 동기**

최근 랜섬웨어의 피해 규모는 매년 증가하고 있으며, 그 대상도 기업과 기관에서 개인 사용자까지 광범위하게 확산되고 있습니다. 이에 따라 개인 사용자가 직관적으로 랜섬웨어 감염 여부를 확인할 수 있는 도구의 필요성이 커지고 있습니다. 그러나 기존의 백신 프로그램은 보안 지식이 부족한 일반 사용자에게는 사용이 어렵고 복잡하게 느껴질 수 있습니다. 저희는 이러한 한계를 보완하기 위해, 간단한 설치만으로 동작하며 폴더 감시를 통해 가볍게 랜섬웨어 여부와 종류를 파악 및 확인할 수 있는 프로그램을 개발하고자 합니다.

**3. 요소 기술**

 **Java WatchService**: 파일/폴더 이벤트 감시 (생성, 수정, 삭제, 확장자 변경)

 **Spring Boot**: 이벤트 수집 서버 + 정책 엔진 + API 제공

 **DB (-)**: 이벤트 로그 저장 및 분석

 머신러닝 기반 랜섬웨어 탐지 모델 서빙

**4. 상세 내용**

**4.1 요구 사항**

 특정 폴더 감시 (생성/수정/삭제/확장자 변조 이벤트 탐지)

 이벤트 → 서버 전송 → AI 분석 → 탐지 결과 반환

 사용자 알림 제공 (정상/의심/공격 구분)

 로그 저장 및 조회 기능 제공

**4.2 구현**

 **OS**

* Windows 11

 **개발 언어/프레임워크**

* Java 24 + Spring Boot
* Python 3.9 + FastAPI (AI 서비스)

 **데이터베이스**

* H2 (테스트)
* - (운영)

 **개발 툴**

* IntelliJ, VS Code
* GitHub
* Postman

**5. 팀원의 기능 및 역할**

 **김유민**

* 랜섬웨어 데이터 셋 조사 후 필요한 피처를 추출해 db생성
* Ai 모델 구축
* Agent 프로그램 개발 (폴더 감시, 이벤트 전송)

 **이상혁**

* Agent 프로그램 개발 (폴더 감시, 이벤트 전송)
* Spring Boot 서버 개발 (이벤트 수집 API, 정책 엔진, 로그 저장)
* 웹 대시보드 구축 (이벤트 로그 조회)

**6. 주간별/팀원별 과제 수행 계획**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 설계요소 / 주 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 데이터 셋 조사 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 오픈 소스 조사 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 설계 목표 설정 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 파일 구조 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 사용할 피쳐(feature) 추출 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 로직 설계 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| db구축 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| ai모델 생성 후 성능 검사 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 김유민 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 이상혁 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |