Yeungnam University

Sys Miner

Conceptualization Document

[Revision history]

Revision date	Version #	Description	Author
03/24/2025	1.0.0	초안 작성	서주형

[Contents]

1. Business purpose

1) Project background

[그림 1] 글로벌 랜섬웨어 피해 금액 및 예측

정보화 시대가 진점됨에 따라 사이버 공간에서의 위협과 공격은 점점 더 교묘해지고 있다. 경험담으로, 랜섬웨어에 감염되었을 때 어떤 조취를 취해야 하는지, 어떻게 해야 해결할 수 있는지 등 해결 방안이 도저히 떠오르지 않았던 기억이 있다. 인터넷 검색을 해보니 초동 조치가 굉장히 중요하다고 하는데, 너무 복잡하고 어려운 단어들이 많아 컴퓨터를 포맷했던 기억이 있다.

이러한 변화는 많은 사람들이 사이버 위협의 대상이 될 수 있음을 의미하며, 효과적인 대응을 위해서는 빠르고 정밀한 조사와 대응이 필수적이다. 이에따라, 사고 발생 시 효율적이고 신속하게 데이터가 손상되기 전에 정보들을 추출해야 할 필요가 있다.

본 프로그램은 이러한 어려움에 조금이나마 도움을 주기 위해 개발하게되었다.

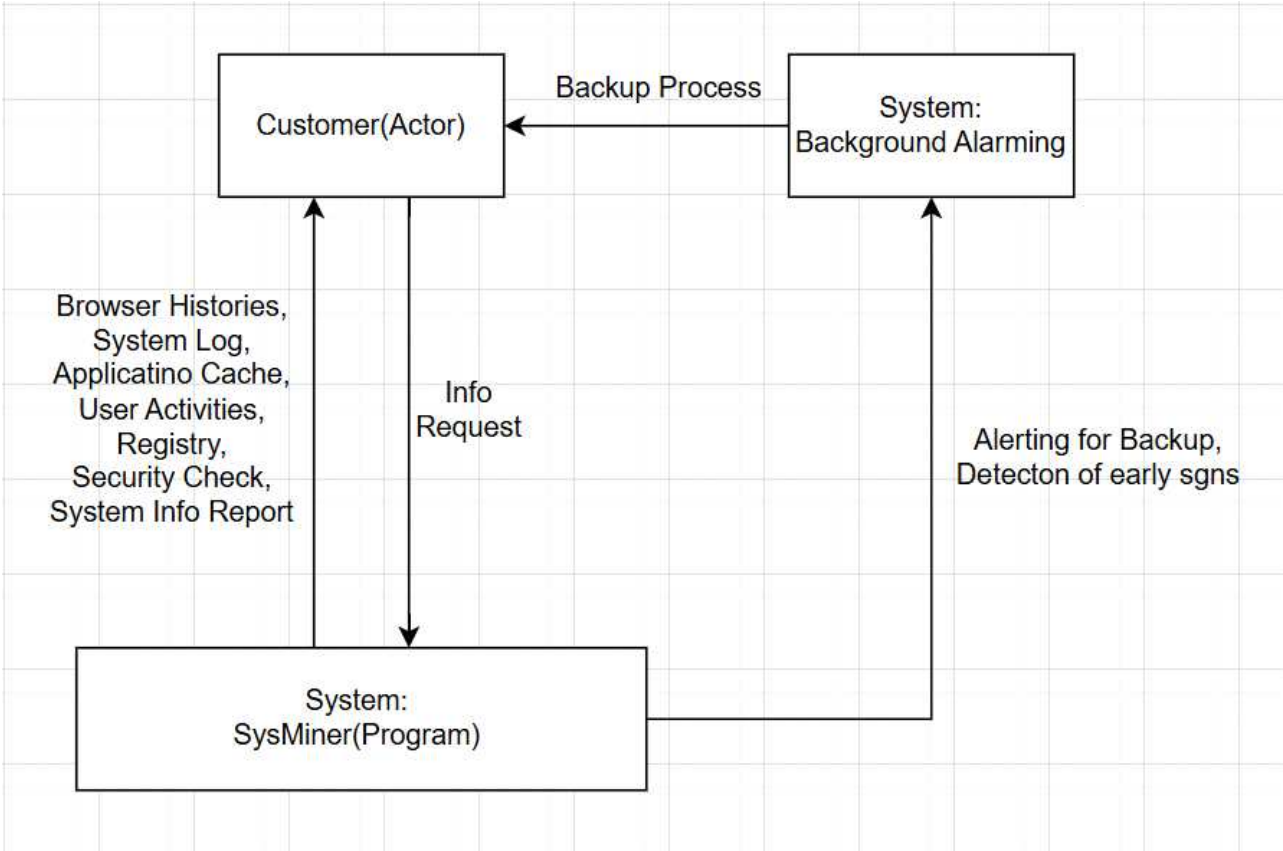
2) Goal

이 프로그램을 통해 이루고자 하는 목표는 컴퓨터가 공격을 받았을 때 즉각 조치를 취할 수 있게 도움을 주는 것이다. 컴퓨터 보안에 대한 지식이 없는 사람들이 대부분인데, 컴퓨터가 공격을 받게 되면 당황스러워하며, 어떤 행동을 취해야할지 모를 것이다. 이 프로그램이 공격당한 컴퓨터를 공격당하기 전의 상태로 돌려주는 것은 아니지만, 침해사고의 전조 증상을 알려주거나, 어떻게 대응해야할지, 또한 이 프로그램을 통해 현재 남아있는 파일이나 기록들이 더 손상되기 전에 전문가가 문제를 해결할 때 참고하는 파일들을 클릭 한번으로 추출하도록 도와줄 것이다. 또한 주기적으로 시스템정보를 추출하여 자동으로 백업하여 침해사고 후의 컴퓨터 정보와 비교해 볼 수 있도록 한다. 메인 GUI에 침해사고 예방법과 침해사고 발생시 대응 방법들을 제시하여 참고할 수 있도록 한다.

3) Target Market

컴퓨터 보안에 대한 지식이 없거나, 컴퓨터 공격을 받기 전 예방하고 싶은 사람과, 침해사고를 당했을 시에 대처를 빠르게 하고 싶은 사람을 대상으로 한다.

2. System context diagram



- Browser Hstories — 크롬, 엣지관련 기록 추출
- System Log — 이벤트로그, 시스템로그 추출
- Applicaton Cache — 프리패치, Srum 정보 추출
- User Activties — 바로가기, 휴지통, 최근파일 추출
- Security check — 방화벽 상태, 윈도우 업데이트, 설치된 소프트웨어, 패스워드 정책 추출
- Registry — 레지스트리 정보 추출
- System info Report — 추출 결과, 컴퓨터 기본 정보 관련 정보 종합 표
- Info Request — 추출 요청
- Backup Process — 정보 자동 추출 과정
- Alerting for Backup — 백업 기간 알림
- Detection for early signs — 침해사고 전조증상 알림

3. Use case list

1) GUI

Actor	Customer
Description	추출 가능한 파일을 나열하고, 소비자가 원하는 파일을 선택하여 그 파일을 추출하도록 추출하고자 하는 파일 선택 기능이다.

2) Browser Histories

Actor	Customer
Description	인터넷 브라우저 '크롬'과 '엣지'의 인터넷 기록, 캐시, 쿠키 데이터들을 추출한다.

3) System Log

Actor	Customer
Description	컴퓨터 사용 시에 발생한 이벤트로그, 방화벽 로그 정보들을 추출한다.

4) Application Cache

Actor	Customer
Description	컴퓨터 사용 시에 발생한 프리패치, srum 정보들을 추출한다.

5) User Activities

Actor	Customer
Description	사용자가 등록한 바로가기 목록, 최근 열어본 파일들, 휴지통 정보들을 추출한다

6) Registry

Actor	Customer
Description	사용자 컴퓨터들의 레지스트리의 키들을 통해 레지스트리 정보를 추출한다. HKEY CLASSES ROOT 파일, HKEY CURRENT USER 파일, HKEY LOCAL MACHINE 파일, HKEY USERS 파일을 추출한다.

7) Security Check

Actor	Customer
Description	사용자 컴퓨터의 방화벽 상태, 윈도우 업데이트 기록, 설치된 소프트웨어, 패스워드 정책 확인등, 파워쉘 명령어의 결과를 직접 입력해주고 그의 결과물을 텍스트로 저장시켜준다.

8) System Info Report

Actor	Customer
Description	사용자의 컴퓨터에 대한 기본적인 정보(호스트 이름, OS이름, OS버전, 모델, 종류 등)와 현재 실행중인 프로세스 수, 열린 포트 수, 추출 성공한 파일들의 목록과 추출 실패한 파일들의 추출 실패 사유등 프로그램 실행 결과를 한 눈에 확인할 수 있는 홈페이지를 제공한다.

9) Background Alarmng

Actor	System
Description	사용자가 마지막으로 시스템 정보를 추출한 지 사용자가 정한 시간만큼 지나고 나면 시스템 정보를 백업할 필요가 있다고 알람 메시지를 띄워주며, 침해사고 전조증상이 일어났을 시, 사용자에게 경고문구를 띄워준다.

4. Concept of operation

1) GUI

Purpose	이 프로그램을 어떻게 사용하는지 쉽게 파악할 수 있도록한다.
Approach	프로그램을 실행시키면 추출 가능한 정보들의 목록이 나열되고, 원하는 정보들만 추출할 수 있도록 체크박스가 있다. 체크박스에 체크된 정보들만 추출이될 수 있도록하며, 프로그램 실행 전, 실행 중, 실행 후 주의사항에 대해 알려준다. 또한, 정보들을 추출할 시, 정보들이 모여있는 폴더의 주소를 알려준다.
Dynamics	프로그램을 실행한 경우
Goals	사용자가 원활하게 사용할 수 있도록한다.

2) Browser Histories

Purpose	사용자가 인터넷 사용 중, 생성된 정보들을 추출한다.
Approach	인터넷 브라우저 '크롬'과 '엣지' 두 브라우저 모두, 사용자가 사용하는 동안 생성된 브라우저의 인터넷 기록, 쿠키, 캐시 정보들을 추출한다. 이 정보들을 추출하는 동안 현재 실행중인 인터넷 브라우저가 꺼질 수 있기 때문에 주의 메시지를 출력하여 사용자가 당황하지 않도록 한다.
Dynamics	Browser Histories 항목을 체크한 경우
Goals	인터넷 사용기록, 캐시, 쿠키 정보를 추출하기 위함이다.

3) System Log

Purpose	컴퓨터 사용시에 발생한 이벤트 로그, 방화벽 로그 정보들을 추출한다.
Approach	사용자가 컴퓨터를 사용하면서 생성된 이벤트 로그나 방화벽 로그들을 기록한 파일들을 찾기 쉽게 원래의 주소에서 프로그램 추출물이 모여있는 폴더로 복사해온다.
Dynamics	System Log 항목을 체크한 경우
Goals	폴더 깊숙한 곳에 있는 로그 파일들을 보기 쉬운 폴더 경로로 복사해온다.

4) Application Cache

Purpose	프리패치와 Srum 데이터들을 추출함으로써 사용된 애플리케이션들의 실행 이력이 담긴 정보를 쉽게 확인할 수 있도록 도와준다.
Approach	프리패치와 srum 데이터가 담긴 폴더를 대상으로 데이터를 추출한다. 관련 데이터들을 프로그램 추출물이 모여있는 위치로 안전하게 복사시킨다.
Dynamics	Application Cache 항목을 체크한 경우
Goals	시스템에서 프리패치와 Srum 데이터를 안정적으로 추출하여 보관한다.

5) User Activities

Purpose	사용자가 등록한 바로가기 목록, 최근 열어본 파일들, 휴지통 정보들을 추출하여 사용자 활동 이력을 분석하고 시스템 사용 패턴을 파악한다.
Approach	사용자의 작업 내역을 효과적으로 수집하고 분석할 수 있도록 지정된 시스템 디렉터리로 Quick Launch, Recent Files, Recycle Bin 데이터를 자동으로 복사하여 저장한다.
Dynamics	User Activities 항목을 체크한 경우
Goals	사용자 활동 기록 데이터를 안전하게 추출하고 보관하기 위함이다.

6) Registry

Purpose	레지스트리의 HKEY CLASSES ROOT, HKEY CURRENT USER, HKEY LOCAL MACHINE, HKEY USERS 데이터를 추출하여, 시스템 설정 및 사용자 환경 정보를 분석하고 보안 및 포렌식 조사에 활용한다.
Approach	Windows 명령어를 사용하여 각 주요 레지스트리 키를 안전하게 백업 및 저장한다.
Dynamics	Registry 항목을 체크할 경우
Goals	포렌식 분석에 활용할 수 있는 파일을 추출한다.

7) Security check

Purpose	사용자의 컴퓨터에서 방화벽 상태, 윈도우 업데이트 기록, 설치된 소프트웨어, 패스워드 정책 등의 보안 관련 정보를 추출하는 것을 목적으로 한다. 이를 통해 시스템의 보안 상태를 점검할 수 있는 정보를 제공한다.
Approach	PowerShell 명령어를 대신 실행해주어 그 결과 파일을 폴더로 모아준다.
Dynamics	Security Check 항목을 체크할 경우
Goals	사용자 컴퓨터의 상태를 확인할 수 있는 정보를 추출한다.

8) System Info Report

Purpose	프로그램이 동작 후 추출 결과, 추출 성공/실패한 목록들, 추출 실패 사유, 사용자 컴퓨터의 정보등 한 눈에 보기 쉽게 html 홈페이지를 통해 확인할 수 있도록 한다.
Approach	컴퓨터 정보와 추출 실패 성공한 목록들을 토대로 html에 작성한다.
Dynamics	프로그램이 동작이 끝난 후 안내표시가 뜨며 추출물들이 모여있는 폴더에 Report가 생성된다.
Goals	추출 결과를 한눈에 파악하기 쉽게 하기 위함이다.

9) Background Alarming

Purpose	백그라운드로 프로그램이 실행된 상태로, 사용자에게 최종 시스템 백업기간에서 너무 오랜 시간이 흘렀거나, 침해사고 전조증상을 감지하면 사용자에게 알람문구를 띄워준다.
Approach	CPU사용량을 조사하여 CPU사용량이 급등하거나, 특정 폴더의 확장자가 갑자기 바뀌면서 파일이 잠긴 것을 확인한다.
Dynamics	전조증상을 감지하거나, 마지막으로 시스템을 백업한 기간이 오랜 시간이 흘렀을 때
Goals	침해사고를 예방하며, 침해사고를 최대한 빠르게 대응할 수 있도록 한다.

5. Problem statement

'Sys Miner'는 침해사고가 발생하기 전, 사용자에게 컴퓨터 백업, 침해사고 전조증상 감지, 침해사고가 발생하고 난 후, 대응방법 등에 대해 자세하고 쉽게 알려 줄 필요가 있다.

따라서 이 프로그램은 다음과 같은 목적을 달성해야한다.

- **프로그램의 목적을 정확하게 전달**
- **비전공자도 쉽게 사용할 수 있는 GUI**
- **프로그램을 통한 사전 예방**
- **침해사고 감지 시 대응방법 제시**

1) Problem 1:

침해사고 해결에 직접적인 해결책을 알려주는 것이 아닌, 보조적인 도구 느낌의 프로그램임을 사용자에게 명백히 알려줄 필요가 있다.

2) Problem 2:

이미 컴퓨터가 완전히 장악되었다면, 프로그램에서 실행되는 명령어가 정상적으로 작동하지 않을 수가 있다. 이에, 프로그램을 설치했을 때 컴퓨터가 완전히 장악되기 전에 프로그램이 전조증상을 파악하여 사용자에게 알려주어 컴퓨터가 완전히 장악되기 전에 이 프로그램을 실행하라는 권고 메시지를 띄워줄 필요가 있다.

3) Problem 3:

이 프로그램이 동작 중에는 컴퓨터의 정보를 빼내오는 것이기 때문에, 컴퓨터 사용의 제한이 있을 수 있다. 사용자가 혼란을 겪지 않도록 사전에 충분히 권고해줄 필요가 있다.

4) Problem 4:

컴퓨터가 침해사고를 당했지만, 완전히 장악을 당하기 전이라면 네트워크 선을 뽑아 장악되는 것을 멈춘 후, 프로그램을 실행하도록 권고해주는 메시지가 필요하다.

6. Glossary

Terms	Description
캐시	자주 사용하는 데이터를 임시로 저장하여 빠르게 접근할 수 있도록 해주는 공간
쿠키	웹사이트 방문 시 생성되는 작은 데이터 파일로, 로그인 정보나 사용자 설정 정보를 저장
이벤트로그(Event Log)	Window에서 컴퓨터 사용 중, 프로그램 실행, 오류, 보안 관련 활동을 기록하는 로그 파일
방화벽로그(Firewall Log)	방화벽에서 허용 또는 차단한 네트워크 트래픽 기록을 저장하는 로그 파일
프리패치(Prefetch)	프로그램 실행 속도를 높이기 위해 Window에서 최근 실행한 프로그램 정보를 저장하는 폴더
Srum	Window가 실행된 프로그램과 네트워크 사용 기록을 추적하는 데이터베이스
레지스트리	여러개의 키(Key)로 구성되며, Window 운영체제의 설정과 프로그램 정보를 저장하는 데이터베이스
HKEY CLASSES ROOT	파일 확장자와 연결된 프로그램 정보를 저장하는 레지스트리 키
HKEY CURRENT USER	현재 로그인한 사용자의 환경 설정 및 소프트웨어 설정을 저장하는 레지스트리 키
HKEY LOCAL MACHINE	시스템 전체의 설정 및 설치된 소프트웨어 정보를 저장하는 레지스트리 키
HKEY USERS	모든 사용자 계정의 환경 설정을 저장하는 레지스트리 키
프로세스	실행 중인 프로그램 또는 작업 단위
포트	네트워크에서 데이터가 오가는 통로

7. References

1) Page 4

(1) 그림1 : https://www.hankyung.com/article/2021091303451