[논문 리뷰 보고서]

[윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구]

작성일	2025.05.26
작성자	안서진
검토자	김예은

목차

I. 개요

항목	내용
논문 제목	윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구
저자 및 연도	위다빈, 김한결, 박명서. (2024)
출처	한국정보보호학회/https://www.dbpia.co.kr/pdf/pdfView.do?nodeId=NODE11956128&googleIPSandBox=false&mark=0&minRead=15&ipRange=false&b2cLoginYN=false&icstClss=010000&isPDFSizeAllowed=true&accessgl=Y&language=ko_KR&hasTopBanner=true
분석 대상 프로그램	JANDI(잔디)
관련 아티팩트 유형	메신저 아티팩트, 시스템 설치/실행, 사용자 행위

[표 1. 논문 개요표]

II. 논문 요약

이 논문에서는 협업 도구를 사용하는 과정에서 발생하는 다양한 아티팩트의 수집과 분석의 어려움을 해결하고자, 윈도우 환경에서 잔디의 아티팩트 수집 방법과 데이터 분석 기법을 제시하는 것을 연구 목적로 삼았다.

연구 결과, 잔디의 로컬 저장 데이터와 API 요청 재구성을 통해 주요 메시지, 채팅 기록, 사용자 활동 로그 등을 수집할 수 있었으며, 이를 활용하여 디지털 포렌식적 분석이 가능함을 보여줬다. 이를 통해, 기업 내 협업 도구 활용 시 보안 확보와 디지털 수사에 기여할 수 있다는 결론을 도출하였다.

이 연구는 윈도우 환경에서 수집할 수 있는 아티팩트의 범위를 확장하고, API 기반 데이터 획득 방법을 적용하여 기존의 한계를 극복하는 데 의의가 있다. 다만, 일부 데이터는 클라우드 서버에 저장된 경우 수집이 어려운 한계가

존재하며, 향후 클라우드 데이터 분석 및 실시간 수집 방안을 모색할 필요가 있다.

III. 상세 경로

항목	경로
JANDI	C:₩Users₩[USERNAME]₩AppData₩Roaming₩JANDI
사용자 행위 정보	Cache와 Local Storage 폴더 하위에 존재
메신저 아티팩트	Cache 폴더

[표 2. 아티팩트별 상세 경로표]

IV. 방향성

1. 잔디 내 특정 악용이 가능한 기능 탐색

기존 논문에서는 클라우드 서버의 한계를 지적했으나, 클라우드 서버 분석은 본 프로젝트 주제에 맞지 않다고 판단하여, 프로그램 내부의 비정상 트래픽을 Fiddler와 Wireshark로 분석하여 네트워크 행위를 분석하는 방향을 제시하고자 한다.
추후 툴 개발에서는 정상 활동과 악성 활동 간의 네트워크 및 파일 시스템 접근 패턴을 학습하여, 이상 행위를 자동으로 탐지하고 분석하는 자동화 도구를 개발할 수 있을 것이다.
그 결과로 정상 프로그램을 악용한 공격 시도에 대한 조기 탐지 및 대응이 가능할 것이다.

V. 참고 문헌

[1] 위다빈, 김한결, 박명서,「 윈도우 환경에서의 협업 도구 잔디 아티팩트 수집 및 분석 연구」, 정보보호학회논문지 제34권 제5호, 2024.10, 915-925