[논문 리뷰 보고서]

[메신저형 협업툴 어플리케이션 아티팩트 분석 - ChannelTalk을 중심으로]

작성일	2025.05.26
작성자	김신아
검토자	김예은

목차

Ⅰ. 개요

항목	내용
논문 제목	메신저형 협업툴 어플리케이션 아티팩트 분석 - ChannelTalk을 중심으로
저자 및 연도	홍리나(아주대) , 손태식(아주대) / 2024.03
출처	디지털 포렌식 연구 제18권 제1호 (p.79-96)
분석 대상 프로그램	ChannelTalk
관련 아티팩트 유형	메신저, 네트워크, 사용자 행위, 시스템 설치/실행

[표1. 논문 개요]

Ⅱ. 논문 요약

1. 논문 요약

이 논문에서는 어플리케이션 아티팩트 분석을 통해 보안 사고 발생 시 증거 수집의 중요성을 해결하고자 모바일 환경에서의 사용자 행위 및 사용 내역 분석을 통해, 기업 내부 정보 유출 및 개인정보 보호 침해와 같은 문제를 해결하는 것을 목표로 하였습니다.

실험 결과, 사용자 계정 정보, 채팅 기록, 파일 공유 기록이 중요한 증거 자료로 활용될 수 있음을 보여주었으며, 특히 팀 메신저와 같은 도구는 공격자에게 필요한 정보를 직관적으로 제공할 수 있다는 점에서 주의가 필요하다는 사실을 확인하였습니다. 이러한 아티팩트들은 기업의 내부 정보가 오고갈 가능성이 높다는 점에서, 보안 사고 발생 시 중요한 증거 수집의 기초가 될 수 있음을 입증하였습니다.

연구는 루팅된 Android 9 버전의 Galaxy Note 8을 사용하여 아티팩트 분석을 수행하였으며, 이는 특정 환경에 국한된 결과를 초래할 수 있다는

한계를 가지고 있었으며, 인터넷 연결이 없는 상태에서의 데이터 분석이 불가능하다는 점은 연구의 한계로 제시되었습니다.

후속 연구로는 다양한 모바일 환경과 인터넷 연결이 없는 상태에서도 접근 가능한 데이터에 대한 분석을 포함하여, 보다 포괄적인 아티팩트 분석이 이루어져야 합니다. 다양한 협업 툴과의 비교 분석을 통해 보안 취약점을 더욱 심층적으로 이해할 필요가 있습니다.

2. 주요 아티팩트 분석 내용

Path	찾을 수 있는 정보
com.zoyi.channel.desk.android.databases	사용자 계정, 채팅 등 데이터베이스
com.zoyi.channel.desk.android.cache.channel	채팅방 내에서 수/발신된 사진 캐시
com.zoyi.channel.desk.android.cache.image_cache	사용자 프로필 캐시 데이터
com.zoyi.channel.desk.android.cache.WebView.Defaul.HTTPCache	접근한 URL 관련 데이터
com.zoyi.channel.desk.android.shared_prefs	XML 형식의 파일로 사용자 설정, 환경 설정 및 간단한 데이터를 저장

[표2. 주요 경로별 수집 가능한 아티팩트 정보]

Ⅲ. 방향성

1. 채팅 로그, 첨부파일, 접속 이력 등 메신저 및 시스템 아티팩트를 중심으로 분석 진행
2. 유출 정황, 외부 접속 시도, 실행 기록 등을 포렌식적으로 재구성
3. 채팅 추출, MAC 타임 분석, 이상 접속 탐지를 지원하는 자동화 도구 개발

Ⅳ. 참고 문헌

[1] 홍리나, 손태식「메신저형 협업툴 어플리케이션 아티팩트 분석 - ChannelTalk을 중심으로」디지털포렌식연구, 18(1), 2024, 79-96