노션프로그램 아티팩트 분석을 통한 위협 분석 및 대응방안 제시

[1] 한주현, [2*]손태식

Threat analysis and response plan suggested through analysis of Notion program artifacts

[1]Juhyeon Han, [2*]Taeshik Shon

요 약

협업 프로그램은 여러 사람이 함께 일할 수 있도록 지원하여 협업과 의사소통의 효율성을 높이고, 업무 생산성을 향상시키며, 시간과 장소의 제약을 극복할 수 있도록 도와주는 도구이다. 엔데믹 시대에 접어들면서 많은 기업과 개인이 협업 프로그램을 선호하고 있다. 그러나 협업 프로그램은 업무 내용, 자료, 사용자 정보 등 유출 시 큰 피해를 초래할 수 있는 민감한 정보를 다수 포함하고 있다. 이 점을 악용하여 협업 프로그램을 사칭한 악성코드 공격, 협업 프로그램의 취약점 악용, 내부 토큰 탈취 등의 다양한 공격 사례가 발생하고 있다. 이러한 공격을 예방하기 위해서는 위협을 사전에 분석하고 대응할 필요가 있다. 본 논문에서는 대표적인 협업 프로그램인 Notion을 대상으로 PC 환경과 Android 환경에서 사용자와 관련된 정보 및 행위에 대한 아티팩트를 수집하고 분석한다. 수집한 데이터를 기반으로 중요한 정보를 분류하고, 발생 가능한 위협에 대해 논의하며 대응 방안을 제시한다.

Abstract

Collaborative programs are tools designed to support multiple people working together, enhancing collaboration and communication efficiency, improving productivity, and overcoming the constraints of time and place. In the endemic era, many companies and individuals prefer using collaborative programs. These programs often handle sensitive information, such as work content, documents, and user data, which can cause significant damage if leaked. Exploiting this, various attack scenarios have emerged, including malware attacks disguised as collaborative programs, exploiting vulnerabilities within these programs, and stealing internal tokens. To prevent such attacks, it is essential to analyze and respond to potential threats proactively. This paper focuses on Notion, a widely used collaborative program, to collect and analyze artifacts related to user information and activities in both PC and Android environments. Based on the collected data, we categorize critical information, discuss potential threats, and propose countermeasures.

Keywords: *Digital forensics, Android forensics, collaboration program, behavior analysis, Notion*

[1] *아주대학교 사이버보안학과 학부생 (ju6035@ajou.ac.kr)*
[2*] *교신저자 아주대학교 사이버보안학과 교수 (sshon@ajou.ac.kr)*

Received: Apr. 17, 2024, Revised: May. 24, 2024, Accepted: Jun. 07, 2024

I. 서론

코로나 팬데믹 이후 재택근무가 급증하면서 협업 프로그램 사용이 지속적으로 증가하고 비대면 문화가 확산되었다. 이후 엔데믹 시대에 도달하며 하이브리드 근무 환경이 새롭게 떠오르며, 서비스형 협업 프로그램이 필수적인 도구로 활용되고 있다[1]. 협업 프로그램은 여러 사람이 함께 작업할 수 있도록 도와주며, 협업과 소통의 효율성을 높이고 업무 생산성을 향상시키며 시간과 장소의 제약을 극복하는 데 도움을 준다.

체크포인트 소프트웨어에 따르면 2023 년도 증가하는 사이버 위협 사례 중 하나로 협업 도구를 악용한 피싱 공격이 꼽혔다. 대부분의 조직이 원격근무를 유지할 가능성이 높기 때문에 협업 도구를 겨냥한 탈취 공격이 고도화되고 지속적으로 이루어질 가능성이 높다는 점을 언급했다[2].

보안 뉴스에 따르면 비대면 업무 환경이 증가함에 따라 협업 도구의 사용이 증가하며, 이에 따른 보안 위협도 증가하고 있다고 이야기한다. 오픈소스 메시징 및 협업 도구인 Zimbra 의 경우, 취약점을 기반으로 이메일 서버를 공격하여 사용자에게 피싱 메일을 지속적으로 발송해 사용자 계정을 탈취하려는 시도가 있었다. 화상회의 솔루션인 ZOOM 의 경우, 접속 링크 URL 만으로 외부인이 무단 침입할 수 있는 보안 취약점이 존재했다. 협업 도구 Slack 의 경우, 종단 간 암호화 기능이 구축되지 않아 개발 과정에서 연동된 GitHub 토큰이 유출되어 내부 소스 코드가 유출되는 사례도 발생했다. 이처럼 협업 프로그램 내 보안 취약점을 활용한 공격이나 사용자 계정을 탈취하기 위한 피싱 공격 등이 지속적으로 이루어지고 있다[3].

2024 년 2 월 AhnLab 에서 발표한 MSIX 악성코드 분석 자료에 따르면, Notion 프로그램을 사칭해 악성코드를 유포하고 있음을 확인했다. 실제 Notion 홈페이지와 유사하게 구현된 피싱 페이지를 통해 설치 파일을 다운로드하면 악성코드가 설치된다. 해당 파일 실행 시 악성코드가 설치되면서 동시에 Notion 프로그램이 정상적으로 실행되어 피해자의 의심을 피하는 수법을 사용한다. Notion 외에도 Slack 등 협업 프로그램으로 위장한 악성 파일이 확인되었다[4].

이와 같이 세계적으로 협업 프로그램의 점유율이 증가함에 따라 프로그램과 사용자에 대한 해커의 공격이 끊임없이 발생하고 있다. 협업 프로그램을 통해 공유되는 업무 정보는 중요한 경우가 많기 때문에 정보 유출이 발생할 경우 큰 위험이 될 수 있다. 내부에서 유출이 발생한 경우 감사 과정에서 분석 가능한 대상이 될 가능성도 존재한다. 이외에도 관련 자료가 범죄 수단으로 악용되거나 보안 사고를 유발할 가능성도 있어 분석의 중요성이 대두되고 있다.

본 논문에서는 협업 프로그램으로 활용되고 있는 Notion 을 대상으로 PC 환경과 Android 환경에서 유출 가능한 사용자 정보와 사용자 행위에 대한 분석을 진행한다. 본 논문의 2 장에서는 관련 연구를 설명하고, 3 장에서는 Notion 아티팩트 분석에 필요한 실험 환경 및 시나리오를 제시한다. 4 장에서는 주어진 가상의 시나리오를 기반으로 Notion 의 아티팩트 및 데이터 분석을 수행하며, 5 장에서는 도출된 데이터를 기반으로 포렌식 관점에서의 보안 위협을 분석한다. 6 장에서는 결론, 향후 연구 계획 및 한계점을 다루며 본 논문을 마무리한다.

II. 관련 연구

Sumin Shin 등은 협업프로그램 슬랙과 디스코드에 대해 모바일과 PC 환경에서 메시지 수, 발신, 공유한 파일, 채팅방, 사용자 정보 등과 같은 아티팩트를 수집 및 분석하였다. 이를 통해 주요 데이터가 저장되는 위치와 파일을 분류 및 기밀 유출 시나리오를 기반으로 디지털 포렌식 관점에서 흩어진 대화내용을 복구하는 방안을 제시한다[5]. Sumin Shin 등은 협업프로그램 잔디와 네이버 웍스를 대상으로 Android 환경에서 아티팩트를 분석 및 데이터 복구 가능성 연구를 진행하였다. 분석된 정보는 패스워드 정보, 수/발신한 멀티미디어 파일, 드라이브 사용 시 저장한 파일의 원본 획득 여부와 삭제된 메시지 복구 가능성으로 분류한다. 두 대상 모두 주고받은 메시지가 데이터베이스에 기록되며 포렌식 관점에서 메시지 복구 방안을 제시한다[6]. Younghoon Kim 은 Microsoft Teams 협업 프로그램에 대해

윈도우즈 및 안드로이드 두가지 환경에서 확인가능한 아티팩트를 수집 및 각 속성을 분석했다. 가상 수사 시나리오를 통해 두가지 환경에서 도출된 아티팩트들을 활용해 수사 효율성을 높이는 방안을 제시한다[7]. Gwuieun Park 등은 네이버 웍스와 잔디를 IOS 환경에서 아티팩트를 분석하여 크리덴셜 데이터를 확인 및 활용방안에 대해 제시하였다[8]. 본 논문에서는 PC 환경에서 Notion 프로그램과 Android 에서의 Notion 앱에 대한 분석을 진행한다. 이를 통해 식별가능한 데이터를 분석 및 잠재적 위협 시나리오를 도출해 해결방안을 제시한다.

III. Notion 프로그램 분석 환경

Notion 은 소프트웨어로서 Windows, macOS, iOS, Android 등 다양한 운영체제와 플랫폼에서 사용된다. 프로그램의 구조는 크게 Workspace, Page, Block 으로 분류할 수 있다. Workspace 는 Notion 의 최상위 작업 공간으로 모든 항목을 포함하고 있다. Page 는 내용을 담는 기본 틀로서 사용되며, Block 은 Page 에 포함되는 요소로 모든 콘텐츠가 포함되며 구체적으로 텍스트, 이미지, 동영상, 파일 등이 포함된다[9]. 본 논문에서는 Windows 환경에서는 2023 년 12 월 기준 3.0.0 버전의 Notion 프로그램과 Android 환경에서 2024 년 2 월 2 일 기준 0.6.1907(7907) 버전의 Notion 앱을 분석한다.

3.1 Windows 분석 환경 및 도구

Windows 환경에서 사용된 분석 환경 및 도구는 아래 표 1 과 같다. 사용한 PC 의 OS 는 Windows 10 Pro (22H2-19045.4291) 버전이며, 분석 시 사용된 Notion 프로그램은 3.0.0 버전이다. Notion 폴더 내에 존재하는 데이터베이스 파일을 DB Browser 를 통해 사용자 정보와 행위 등을 분석한다.

Table 1. Analysis environment and tools for use on Windows
표 1. Windows 에서의 분석환경 및 사용 도구

	Version
OS	Windows 10 Pro 22H2 - 19045.4291
Notion	3.0.0
DB Browser for SQLite	3.12.2

3.2 Mobile 분석 환경 및 도구

분석에 사용된 Device 및 APP, 분석 도구는 아래 표 2 와 같다. Samsung Odin 을 활용해 Device 를 루팅하고 BusyBox 와 ADB 등을 통해 커널에 접근한다. 이후 데이터 이미지 파일을 추출해 FTK Imager 를 사용하여 이미지 파일을 분석한다. 애플리케이션 데이터베이스 파일을 확인하기 위해 DB Browser for SQLite 를 사용해 분석을 진행한다.

Table 2. Analysis environment and tools for use on Mobile
표 2. 모바일에서의 분석환경 및 사용 도구

	Version
Device	Galaxy Note 10
OS	Android 12
Samsung Odin	3.13
BusyBox 64	1.32.0
ADB	34.0.0
Notion	0.6.1907
DB Browser for SQLite	3.12.2
FTK Imager	4.7.1

3.3 실험 시나리오

Notion 아티팩트 분석을 위한 시나리오는 다음과 같다. 기존에 활동중인 개인 Workspace, 공유 WorkSpace 를 통해 파일 업로드, 글 삭제, 글 생성 등을 진행하여 유의미한 정보를 남긴다.

IV. Notion 아티팩트 분석

4.1. Windows 환경에서의 Notion 아티팩트 분석

Notion 은 사용자가 속해 있거나 생성한 Workspace, Page, Block 관련 데이터들이 로컬에 파일 형태로 저장된다. 저장된 DB 파일에는 사용자 계정 정보, 계정 사진, 계정 고유 ID, 권한, 업로드된 파일의 텍스트 내용 등과 같은 아티팩트들이 포함되어 있다. 이러한 아티팩트들은 아래 표 3 과 같은 위치에 저장된다.

Table 3. Notion Database file path
표 3. 노션 DB 파일 경로

Path	Data File
C:\Users\{UserID}\AppData\Roaming\Notion	notion.db

4.1.1 사용자 정보

사용자가 포함된 또는 생성한 Workspace 내에 접근 가능한 계정들에 대한 정보는 notion_user 테이블에서 확인할 수 있으며, 사용자가 생성한 Workspace 또는 접근 형태가 Guest 가 아닌 경우에는 추가로 space 테이블 내에 Workspace 관련 정보가 저장됩니다. 각 테이블에 저장된 주요 데이터는 표 4 와 같이 정리된다. 사용자가 Workspace 에 초대되거나 생성하는 경우, 초대된 사용자에 대한 정보가 notion_user 테이블에 저장된다.

notion_user 테이블에 저장되는 구체적인 데이터는 각 User 들의 고유한 ID 와 설정한 이름, 이메일 등이 암호화되지 않고 평문 형태로 저장되어 있다. space 테이블에서 확인 가능한 주요 데이터는 Workspace 이름과 각 Workspace 에 접근 가능한 user ID, 권한을 확인할 수 있으며, 생성된 시간, 생성한 User ID, 마지막으로 Workspace 를 수정한 시간과 마지막으로 수정한 User ID 등을 확인할 수 있다.

Table 4. Tables and data related to user information
표 4. 사용자 정보와 관련된 테이블 정보

Table	Column	value
notion_user	id	User ID
	name	User Name
	email	User Email
	profile_photo	User Profile_photo
space	name	Space Name
	permissions	Permitted User ID
	created_time	Space creation date
	last_edited_time	Last edited time
	created_by_id	User ID to create a space
	last_edited_by_id	Last edited user ID

또한 notion_user 테이블에는 스페이스에 참여했던 인원들에 대한 정보가 모두 기록되어 있다. notion_user 테이블에 저장된 profile_photo 데이터를 확인해보면 그림 1 과 같이 설정된 사용자 사진이 저장된 클라우드 서버 주소가 존재하는 것을 확인할 수 있다.

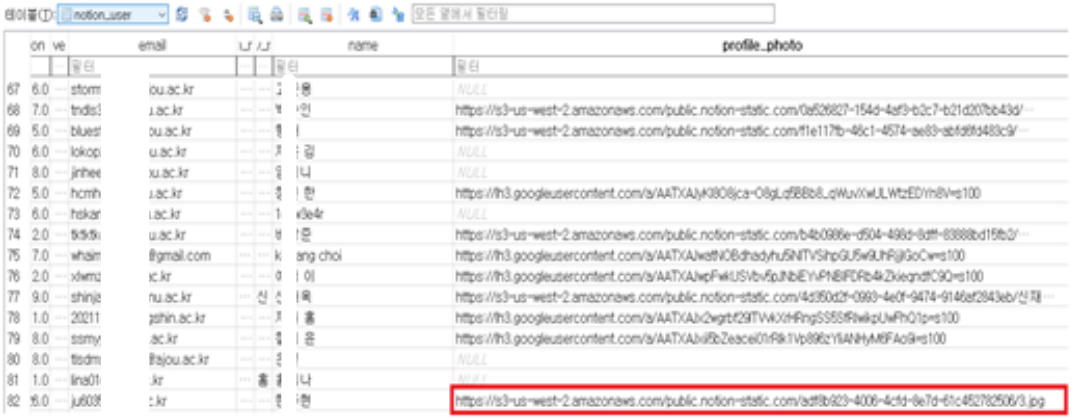

Figure 1. profile_photo data
그림 1. 프로필 정보

그림 2 와 같이 테이블에 저장된 데이터 URL 을 통해 접속하면 권한이 없음에도 불구하고 정상적으로 접근이 가능한 것을 확인할 수 있다. 또한 다른 계정의 profile_photo 역시 접근이 가능한 것으로 나타났다.

Figure 2. Unauthorized access to profile_photo data
그림 2. 프로필 데이터에 대한 무단 접근

4.1.2 사용자 행위 분석

Workspace 내에서 작성된 모든 행위는 block 테이블에 저장된다. 각 block 은 문장, 링크, 업로드된 파일 등과 같은 내용을 담고 있다. 특정 block 에 대한 comment 가 작성되었다면, 해당 comment 는 comment 테이블에 기록되며 각 테이블에 저장된 주요 데이터는 아래 표 5 에서 확인 가능하다.

block 테이블에 저장되는 주요 데이터에는 Workspace ID, block ID 등의 기본적인 ID 가 포함된다. 또한 block 이 파일로 업로드 되었는지, 이미지로 사용되었는지, 텍스트로 사용되었는지 등의 정보에 따라 type 이 달라진다. 각 block 은 페이지 내에서 한 줄로 사용되기에, 내용 전체는 properties 항목으로 포함되며, 세부 내용은 암호화되어 있지 않다. block 이 생성된 시간, 마지막 수정 시간, 생성한 User ID, 마지막으로 수정한 User ID, 로컬 PC 에 설치된 프로그램에 로그인한 사용자가 마지막으로 접근한 시간 등의 데이터가 여기에 포함된다. block 이 삭제되었는지 이동되었는지 여부도 확인할 수 있다.

두 테이블 모두 alive 라는 항목에서 삭제 여부를 확인하며, 실제 데이터가 삭제된 경우 값이 0 이 되지만 세부 내용은 데이터베이스 내에 그대로 유지된다.

Table 5. Tables and data related to user behavior
표 5. 사용자 행위와 관련한 데이터 및 테이블

Table	Column	value
block	id	Block ID
	space id	Workspace ID
	type	image, text, page, bulleted_list, file, numbered_list
	properties	block content
	created_time	block created time
	last_edited_time	last edited time
	alive	Whether to delete a block
	move	Whether to move a block
	created_by_id	Created user ID
	last_edited_by_id	Last edited user ID
	meta_last_access_timestamp	meta user last access timestamp
comment	id	comment ID
	space id	Workspace ID
	text	comment content
	created_time	comment created time
	last_edited_time	last edited time
	alive	Whether to delete a comment
	created_by_id	Created user ID

아래 그림 3 을 확인하면 block 테이블에서 Notion 에 업로드한 파일의 크기, 파일명, 저장된 위치를 확인할 수 있다. 그러나 실제로 파일 위치에 접근할 때, profile_photo 데이터와는 다르게 권한 없는 접근은 막혀 있다.

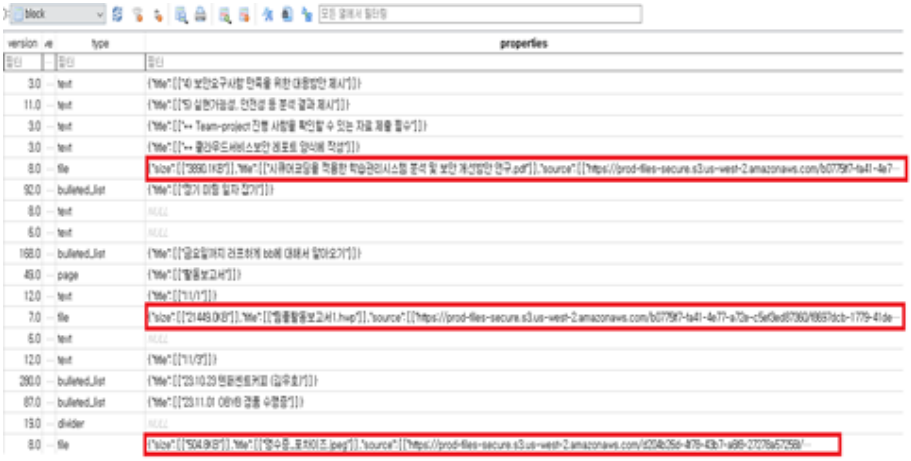

Figure 3. Analyzing block data
그림 3. Block 데이터 분석

4.2. 모바일 환경에서의 Notion 아티팩트 분석

모바일 분석에서 어플리케이션의 파일 저장 위치와 분석 폴더는 아래 표 6 에 저장된다. 모바일 분석 과정에서는 Notion 에 저장된 데이터베이스 파일, 캐시, 안드로이드 기본정보인 Shared.prefs 등의 아티팩트를 수집하고 분석하여 유의미한 정보를 찾아낸다.

Table 6. Path where Notion app data is stored
표 6. Notion app 데이터가 저장된 경로

Path	Data Folder
data/data/notion.id	databases
data/data/notion.id	cache
data/data/notion.id	shared_prefs
data/data/notion.id	files

4.2.1 사용자 정보

어플리케이션에서는 SharedPreferences 를 이용하여 간단한 데이터를 key 와 value 형태로 저장한다. 각 어플리케이션 저장소에는 XML 파일로 저장되며, 다른 어플리케이션과는 데이터를 공유할 수 없다. 주로 초기 설정 값과 같이 간단한 값이 저장된다.

수집한 정보는 아래 표 7 과 같이 정리된다. 사용된 어플리케이션의 버전 정보는 appid.xml 에서 확인할 수 있다. 사용자 이름, 이메일 주소, 대표 사진, 사용자 정보를 불러오는 API, 그리고 account_token 을 통해 상세 사용자 정보들이 signin.xml 파일에 저장된다. 어플리케이션에 처음 접근한 시간과 마지막으로 접근한 시간, 연결된 세션 ID, 사용된 기기의 OS 버전 등은 measurement.prefs.xml 에 저장되며, androidsdk.xml 에서는 사용자의 Notion 고유 ID 가 저장된다.

마지막으로 PersistedInstallation.json 에서는 Firebase 에서 관리하는 auth token, refresh token, 토큰 만료 기간, 생성 기간, 토큰 상태 등을 확인할 수 있다.

Table 7. Tables and data related to user information
표 7. 사용자 정보 관련한 데이터 및 테이블

Path	File Name	value
data/data/notion.id/shared_prefs	com.google.android.gms.appid.xml	App Version
	com.google.android.gms.signin.xml	givenName, displayName, email, photoUrl, userinfo api,account_token
	com.google.android.gms.measurement.prefs.xml	first_open_time, session_id, last_pause_time, os_version
	com.statsig.androidsdk.xml	notion_id
data/data/notion.id/files	PersistedInstallation	Auth_Token, Refresh_Token, exprired, Token status

또한 gms.signin.xml 에 저장된 profile_photo 데이터를 확인해보면 그림 1 과 같이 설정된 사용자 사진이 저장된 클라우드 서버주소가 존재하는 것을 확인할 수 있다.

Figure 4. Analyzing com.google.andorid.gms.signin.xml
그림 4. com.google.andorid.gms.signin.xml 분석

그림 4 와 같이 shared_prefs 폴더 내에 존재하는 signin.xml 파일을 분석한 결과, 사용자의 이메일 주소, 사용자 이름, 사용자 대표 사진 URL, 로그인에 사용된 API 등 사용자 관련 정보가 암호화되지 않고 평문으로 저장된 점을 확인할 수 있다.

```
{
  "alg": "RS256",
  "kid": "08bf5c3772dd4e7a727a101bf520f6575cac326f",
  "typ": "JWT"
}
```


Figure 5. Analyzing Token Header
그림 5. 토큰 Header 분석

주어진 토큰을 자세히 분석해보면 알고리즘과 토큰 종류, 내부 데이터를 나누어 확인할 수 있다. 그림 5 를 확인했을 때, 토큰에 사용된 알고리즘은 RS256 이며, 서명에 사용된 키 ID 는 JWT 형식이 사용되었다는 것을 알 수 있다.


```
{
  "iss": "https://accounts.google.com",
  "azp": "905154081809-
5e1mcr80o0ca1vclc1b2jg349pv7s7dc.apps.googleusercontent.
com",
  "aud": "905154081809-
858sm3f0qnalqd9d44d9gecjtrdji9tf.apps.googleusercontent.
com",
  "sub": "113943665729535185075",
  "hd": "ajou.ac.kr",
  "email": "ju6035@ajou.ac.kr",
  "email_verified": true,
  "name": "한주현",
  "picture":
"https://lh3.googleusercontent.com/a/ACg8ocJQDmLxseudQa1
hQ33IWYFZWKie-NEVbnbS4bihBTlv=s96-c",
  "given_name": "한주현",
  "locale": "ko",
  "iat": 1710133406,
  "exp": 1710137006
}
```


Figure 6. Analyzing Token Data
그림 6. 토큰 데이터 분석

그림 6 은 토큰 내부의 데이터를 보여준다. 자세히 확인해보면, iss 는 토큰 발급처로서 여기에서는 Google 계정 서비스가 토큰을 발급한다는 것을 나타낸다. azp 는 발급된 토큰을 받는 애플리케이션의 ID 를 나타내며, aud 는 토큰이 전달될 애플리케이션의 ID 를 의미한다. sub 는 사용자의 고유 식별자를 나타내며, 사용자의 전체 이름과 프로필 사진 URL, 이메일 정보, 사용자 국가, 토큰 발급 시간, 만료 시간 등을 확인할 수 있다.

이 토큰의 정보를 사용하여 Google 에서 Notion 으로 사용자를 인증하고 권한을 부여하는 역할을 한다. 이를 통해 사용자는 안전하게 Notion 서비스에 액세스할 수 있다.

Figure 7. Analyzing PersistedInstallation
그림 7. PersistedInstallation 분석

그림 7 은 PersistedInstallation.json 파일을 추출한 모습이다. 내부 내용을 확인해보면 총 6 가지의 필드가 존재한다. Fid 는 설치된 기기의 Firebase ID 를 나타내며, Status 는 토큰의 상태를 나타낸다. 여기서 3 은 활성화된 상태를 나타낸다. AuthToken 은 Firebase 에

액세스하기 위해 필요한 토큰으로, JWT 형식으로 표시된다. AuthToken 이 만료되었을 때 사용되는 RefreshToken 도 함께 포함되어 있다. 또한 토큰의 생성 및 만료 시간도 나타내어져 있다.


```
{
  "appId":
"1:30384045198:android:323c4e
a9d1b4f1ea",
  "exp": 1710738194,
  "fid":
"d85gz8CDTYSFlZR7_838eU",
  "projectNumber":
30384045198
}
```


Figure 8. Analyzing PersistedInstallation Auth Token
그림 8. PersistedInstallation 인증 토큰 분석

위의 그림 8 은 제공된 AuthToken 에 대한 자세한 내용을 보여준다. 여기서 appId 는 Firebase 프로젝트 내의 Android 앱에 할당된 고유 식별자를 나타내며, exp 는 토큰의 만료 시간을 나타낸다. fid 는 Firebase 설치 ID 로, 앱 인스턴스를 식별하는 고유한 식별자이다. projectNumber 는 Firebase 프로젝트의 번호를 나타내며, 해당 앱이 속한 프로젝트를 식별하는 데 사용된다.

현재 Notion 에서 사용되는 Firebase AuthToken 의 만료 기간은 그림 7 의 ExpiresInsecs 필드를 통해 7 일임을 확인할 수 있다.

4.2.2 사용자 행위 분석

모바일 환경에서도 Notion 의 데이터베이스 구조는 PC 환경과 동일하며 주요 차이점은 데이터 저장 우선순위에 있다. 모바일 환경에서는 사용자가 디스플레이에서 확인한 Space 및 block 정보가 먼저 DB 에 저장된다. 따라서 DB 에서 확인할 수 있는 내용은 PC 환경에서와 동일하며, 주로 표 5 에 정리된 데이터를 포함한다.

또한 모바일 환경에서는 PC 환경과는 달리 캐시 정보를 확인할 수 있다. 이 캐시 정보는 사용자의 행위를 분석하는 데 유용한 추가적인 데이터를 제공할 수 있다.

Table 8. Tables and data related to user behavior
표 8. 사용자 행위와 관련한 데이터와 테이블

Path	File Name	value
data/data/notion.id/cache/image_manager_disk_cache	disk cache file	cached images
data/data/notion.id/cache/Webview/Default/HTTP Cache	HTTP Cache file	network cache

이미지 관리자 디스크 캐시인 image_manager_disk_cache 에는 로드된 이미지를 저장한다. 이렇게 저장된 이미지는 나중에 동일한 이미지를 재로드할 때 네트워크 통신 없이 저장된 값을 사용하여 불러온다. 아래 그림 9 에서는 Notion 페이지에 저장된 배경 사진 중 하나가 저장된 것을 확인할 수 있다.

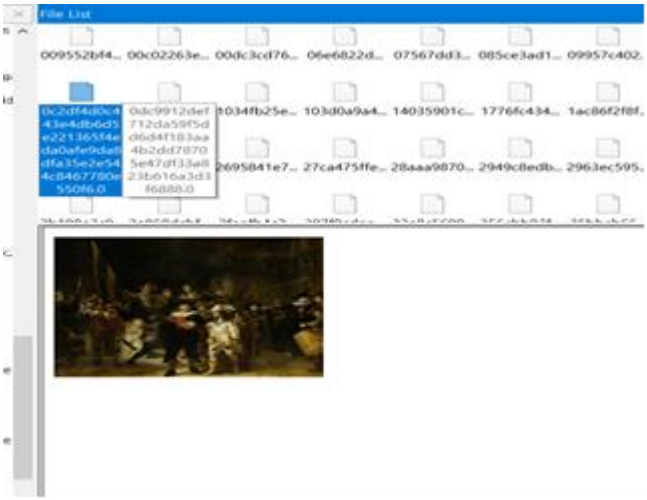

Figure 9. Analyzing image_manager_disk_cache
그림 9. image_manager_disk_cache 분석

그림 10 은 실제 네트워크 통신을 통해 캐시에 저장된 이미지를 나타낸다. 이 캐시는 불러올 이미지의 이전 위치 정보와 파일 데이터를 저장한다. 그림 10 에서 확인한 파일 주소로 접근하면 그림 9 에서 확인한 사진과 동일한 사진이 저장된 주소임을 확인할 수 있다. Notion 에 업로드될 때 AWS 클라우드에 저장된 자료의 경우 무단 접근이 불가능하지만, notion 사이트에 업로드된 자료에 대해서는 접근이 가능하다는 점도 확인할 수 있다.

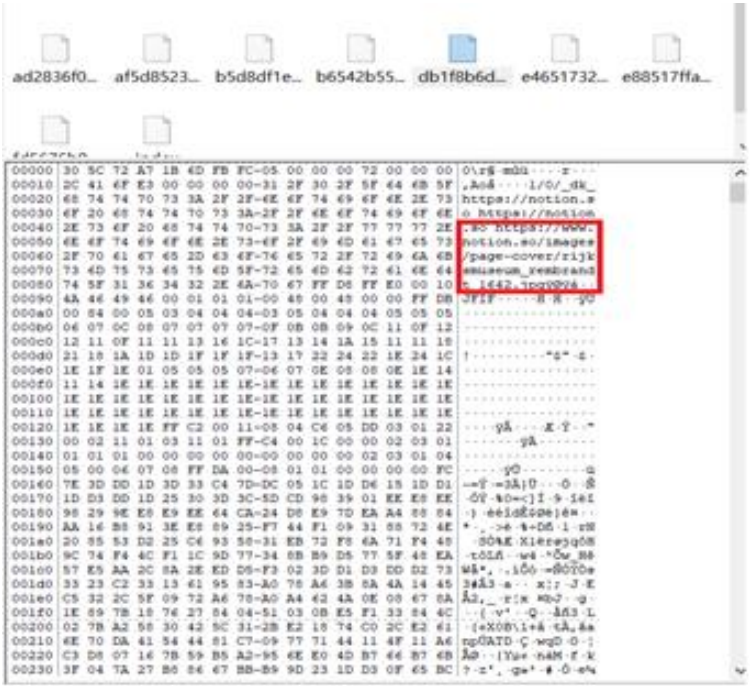

Figure 10. Analyzing HTTP Cache file
그림 10. HTTP Cache 파일 분석

V. 주요 아티팩트 정리 및 위협 분석

5.1 주요 아티팩트 정리

아래 정리된 표 9 는 PC 환경과 Mobile 환경에서 분석한 아티팩트 중 사용자 정보, 사용자 행위 두가지 분류로 나누어 주요한 아티팩트를 정리한 내용이다.

Table 9. Summary of major artifacts
표 9. 주요 아티팩트 정리

Environment	Artifact	
PC(Windows)	User Information	User ID, User Name, User Email, User Profile_photo,
	Behavior Information	Whether to move a block, Created user ID , Last edited user ID , meta user last access timestamp, block created time, last edited time, Whether to delete a block, Block contents
Mobile	User Information	givenName, displayName, email, photoUrl, userinfo api, account_token, Auth_Token, Refresh_Token, exprired, Token status
	Behavior Information	cached images, network cache

5.1.1 PC 환경 주요 아티팩트 분석

PC 환경에서 Notion 프로그램을 분석한 결과, 데이터베이스 파일에서 다양한 유의미한 아티팩트를 확인할 수 있었다. 사용자 정보와 관련된 정보 중에는 사용자 이름, 이메일, 사용자 ID 등 사용자가 설정한 정보뿐만 아니라 모든 사용자의 정보가 확인 가능했다. 특히 각 사용자가 설정한 대표 사진 정보는 무단으로 접근이 가능했다.

또한 Notion 의 구조를 이루는 Block 에 관련한 사용자 행위 대부분의 정보를 확인할 수 있었다. 각 Block 마다 생성한 사용자 ID, 마지막 수정자 ID, 마지막 접근 시간, Block 삭제 여부 및 세부 내용 등을 확인할 수 있었다. 파일이 업로드된 Block 의 링크가 암호화되지 않고 존재하는 것을 확인했으나, 무단 접근은 제한되어 있었다. 또한 Block 이 삭제된 경우에도 삭제 여부를 판별할 수 있었지만, Block 내용은 데이터베이스에 남아 있는 것을 확인할 수 있었다.

5.1.2 Mobile 환경 아티팩트 분석

모바일 환경에서 Notion 앱을 분석한 결과, PC 환경과 마찬가지로 데이터베이스 파일에 저장되어 있었다. 그러나 PC 환경과의 차이점은 Mobile Device 사용자와 관련된 정보가 추가로 저장되어 있다는 점이었다.

특히 사용자 정보와 관련된 정보뿐만 아니라 인증과 관련된 정보가 존재하는 것을 확인할 수 있었다. 사용자 정보를 가져오는 데 사용되는 API, 사용자 계정에 대한 토큰, 사용자를 인증하는 데 사용되는 토큰, 토큰 갱신에 사용되는 토큰, 토큰의 만료 여부를 나타내는 값, 토큰의 상태 등과 같이 외부에 유출되면 크리티컬한 문제가 발생할 수 있는 정보들이 암호화되지 않고 저장되어 있는 것을 확인할 수 있었다

5.2 위협 분석 및 대응 방안

5.2.1 사용자 정보 유출 위협

분석된 결과에 따르면, 사용자 이름, 이메일 주소, 프로필 사진 등의 개인 정보가 암호화되지 않고 저장되어 있어 유출 위협이 존재한다. 특히, 프로필 사진의 경우 다른 사용자가 무단으로 접근할 수 있는 취약점이 존재한다. 이러한 문제는 Notion 의 데이터 저장 방식에 근본적인 보안 취약점이 있음을 시사하며, 개인 정보 유출 가능성이 존재한다.

1. PC 환경의 유출 위협

사용자 정보: User name, User Email, User ID 등이 평문으로 저장되어 있다. 개인 정보 보호 관점에서 심각한 위협이 될 수 있다.

프로필 사진: 다른 사용자의 프로필 사진에 무단 접근이 가능하며, 개인의 사생활을 침해할 수 있다.

Workspace 정보: Workspace 에 참여한 모든 사용자의 정보가 저장되어 있어, Workspace 에 소속된 다수의 사용자의 정보가 한 번에 유출될 가능성이 높다.

2. Mobile 환경의 유출 위협

사용자 정보: 사용자 이름, 이메일 주소, 프로필 사진 URL, 로그인에 사용된 API, 계정 토큰 등이 암호화되지 않고 평문으로 저장되어 있다.

계정 토큰: 계정 토큰은 사용자 인증 및 권한 부여에 사용되는 중요한 정보이며, 이 토큰이 유출될 경우, 공격자는 피싱 공격이나 계정 도용 등의 악의적인 행위를 할 수 있다.

Firebase AuthToken: 이 토큰은 만료 기간이 7 일로 설정되어 있어, 유출될 경우 장기간 악용될 수 있다.

3. 구체적인 위협 정리

암호화되지 않은 사용자 이름과 이메일 주소는 피싱 공격의 표적이 될 수 있다. 공격자는 이 정보를 이용해 사용자에게 악성 이메일을 보내, 추가적인 개인 정보나 계정 비밀번호를 탈취하려 할 수 있으며 계정 토큰이 유출되는 경우, 공격자는 이를 통해 사용자의 계정에 무단 접근할 수 있다. 이는 개인 정보 유출 뿐만 아니라, Workspace 내에서의 악의적인 행위로 이어질 수 있다.

또한 프로필 사진이 무단으로 접근 가능하다는 것은 사용자의 사생활이 침해될 수 있음을 의미한다. 공격자는 이를 통해 사용자의 신상을 파악하고, 더 나아가 사회공학적 공격을 시도할 수 있다.

5.2.2 내용 유출 위협

작성된 문서, 업로드된 파일, 댓글 등의 작업 내용이 암호화되지 않고 데이터베이스 파일에 저장되어 있어 사용자의 PC 나 Mobile 이 침해당한 경우 작성한 내용이 유출될 위험이 존재한다. 이러한 위험은 Notion 의 데이터 저장 방식에서 기인한 것으로, 민감한 정보가 평문으로 저장되어 있기 때문에 발생한다.

1. PC 환경의 유출 위협

문서 및 댓글 작성 내용: 작성된 문서와 댓글의 내용이 암호화되지 않고 데이터베이스 파일에 저장되어 있다. 사용자의 PC 가 침해당했을 때 작성된 모든 내용이 유출될 수 있음을 의미한다.

삭제된 Block: 삭제된 Block 의 내용도 실제로는 삭제되지 않고 데이터베이스에 남아 있어 복구해 확인할 수 있다. 사용자가 삭제한 작업 내용이 유출될 수 있는 가능성이 존재한다.

업로드된 파일: 업로드된 파일의 링크가 암호화되지 않고 저장되며, 파일 제목과 크기 정보도 남아 있다. 외부에서 파일링크 접속시 접근이 제한되지만 파일의 간략한 정보를 알 수 있다.

2. Mobile 환경의 유출 위협

작업 내용: 작업 내용은 PC 환경과 동일하게 암호화되지 않고 저장되어 있다. 모바일 디바이스가 침해당한 경우에도 작성된 모든 내용이 유출될 수 있다.

캐시된 이미지 및 네트워크 캐시: Mobile 환경에서는 캐시된 이미지 및 네트워크 캐시에 과거 활동 내용이 저장되어 있다. 사용자가 과거에 접근한 작업내용에 대해 공격자가 확인할 수 있다.

3. 구체적인 위협 정리

작성된 문서와 댓글이 암호화되지 않고 저장되어 있기 때문에, 사용자의 디바이스가 침해당한 경우 민감한 정보가 포함된 문서가 유출될 수 있다. 사용자 개인 정보 유출 뿐만 아니라 기업에서 사용하는 경우 내부 정보 유출로 이어질 수 있다.

또한 삭제된 Block 의 내용도 데이터베이스에 남아 있어, 이를 복구해 확인할 수 있다. 사용자가 삭제한 민감한 정보가 여전히 유출될 수 있음을 의미한다.

5.2.3 대응 방안

위의 제시된 위협을 예방하기 위해 Notion 자체적으로 사용자 이름, 이메일 주소, 프로필 사진 등의 개인 정보, 작성된 문서, 업로드된 파일, 댓글 등의 작업 내용은 암호화하여 저장되어야 한다. 삭제된 데이터는 데이터베이스 파일에 기록이 남지 않도록 관리되어야 한다. 또한 사용자 측면에서는 사용자는 다중 인증 방식등을 사용하여 계정 보안을

강화해야 하며 중요한 작업 내용이나 파일은 별도의 저장 장치에 백업 및 관리하는 것이 중요하다.

Notion 은 기업내에서도 사용하는 협업 프로그램으로서 프로젝트 진행, 업무 등의 측면에서 사용된다. 내용 유출과 관련한 피해를 최소화하기 위해선 기업내 보안 정책 수립 및 교육, Notion 이용 제한 및 각 페이지에 대한 권한 설정, 데이터 유출 방지 및 복구 시스템 구축 등을 통해 기업 데이터 보안 강화에 힘을 써야한다. 이러한 위험을 방지 하기위해서는 space, block, comment 테이블에서 생성시간, 수정된 시간, 생성 및 수정에 관여한 User ID, alive 여부 등을 통해 행위를 파악하고 추적가능하며 또한 삭제 여부에 대한 지속적인 모니터링을 통해 의도적인 삭제, 유출 가능성을 사전에 감지해야한다. 이와 관련한 사고발생시 고유식별 ID 와 사용자 정보를 결합하여 행위자 식별, 행위 분석 및 사용자 정보 연관성을 통해 책임자 파악 및 감사 측면을 강화해야한다.

VI. 결론

본 논문에서는 협업 프로그램 중 대표적으로 사용되는 Notion 을 대상으로 PC 환경과 모바일 환경에서 사용자 정보, 사용자 행위에 대한 아티팩트를 수집 및 분석하였다. 수집된 데이터를 기반으로 크리티컬한 정보들을 분류하고 발생 가능한 위협에 대해 논의 및 대응 방안을 제시하였다. PC 환경에서 분석한 결과 사용자 계정 정보(사용자 ID, 사용자 이름, 사용자 이메일, 사용자 프로필 사진)는 평문으로 저장되며 사용자의 행위 정보 역시(블록 이동 여부, 생성자 ID, 마지막 편집자 ID, 마지막 접근 시간, 블록 생성 시간, 마지막 편집 시간, 블록 삭제 여부, 블록 내용) 데이터베이스에 평문형태로 저장된다.

모바일 환경에서 분석한 결과 사용자 계정 정보(이름, 표시 이름, 이메일, 사진 URL, 로그인 API, 계정 토큰, 인증 토큰, 갱신 토큰, 만료 시간, 토큰 상태)는 평문, 암호화되어 저장된 점을 확인할 수 있었으며 사용자 행위정보는 PC 환경과 동일하게 데이터베이스 파일에 저장된 것을 확인할 수 있었다. 이러한 사항들을 토대로 사용자 계정 정보 유출, 블록 내용 유출, 인증 토큰 악용등의 위협을 도출할 수 있었다. 본 논문에서는 추가적인 협업프로그램에 대한 아티팩트 분석, 실제 공격 시나리오를 통해 위협 실현 가능성에 대해 구체적으로 다루지 못했다는 아쉬운 점이 존재한다. 여러 협업프로그램의 보안을 위한 효과적인 대응 방안의 연구가 이루어져야 할것이다.

VII. 참고문헌

[1] Jisung Park, “Leading the rapid growth of the work environment, collaboration tools, and cloud market in the post-COVID-19 era”, KT Enterprise, Available: https://enterprise.kt.com/bt/dxstory/1890.do, 2023.12.01. confirmed.

[2] HyeKyeong kim, “The major cyber threats next year will be... ″Phishing attacks ′email→collaboration tool′ expand″”, inews24, Available: https://www.inews24.com/view/1545183, 2024.03.23. confirmed.

[3] Somi Lee, “[Useful Security Dictionary] This method targets zero trust weaknesses, ‘attacking internal collaboration tools’”, boannews, Available: https://boannews.com/media/view.asp?idx=121322&page=1&kind=5, 2024.03.23. confirmed.

[4] ASEC, “Spreading MSIX malware disguised as Notion installation file”, ASEC, Available: https://asec.ahnlab.com/ko/62324/ , 2024.03.23. confirmed.

[5] Sumin Shin, Eunhu Park, Soram Kim and Jongsung Kim, “Analysis of Slack and Discord messenger artifacts from a digital forensics perspective.”, Journal of Digital Content Society, 21(4), pp.799-809, 2020.

[6] Sumin Shin, Yongcheol Choi, Soram Kim and Jongsung Kim, “Artifacts Analysis and Data Recovery of Collaboration Tools”, Journal of Digital Forensics 15(2), pp.99-123, 2021.

[7] Young-hoon Kim, TaeKyung kwon, “A Study on the Analysis of Artifacts by User Behavior of Collaborative Tools - Using Different Forced Concepts according to the Operating Environment.”, a paper by the Information Protection Association 31.3, pp.353-363, 2021.

[8] Gwui-Eun Park, Min-Jeong Lee, Soo-Jin Kang, So-Ram Kim and Jong-Sung Kim, “A Study on Ar tifacts Analysis and Cr edential Utilization Method of Collabor ation Tools in iOS”, Journal of Digital Forensics 17(2), pp. 14-32, 2023.
[9] WIKIPEDIA, “Notion(productivity_software)”, Wikipedia, Available: https://en.wikipedia.org/wiki/Notion_(productivity_software), 2023.12.02. confirmed.

저자소개

한주현 (*Juhyeon Han*)

2019 년 ~ 현재 : 아주대학교 사이버보안학과 학부생

관심분야 : 정보보호, 디지털포렌식, 개인정보보호

손태식 (*Taeshik Shon*)

2005 년 : 고려대학교 정보보호대학원 졸업(박사)
2017 년 ~ 2018 년 : Illinois Institute of Technology 방문교수
2011 년 ~ 현재 :아주대학교 정보통신대학 사이버보안학과 교수

관심분야 : Digital Forensics, ICS/Automotive Security