마이크로소프트 클라우드 서비스 안정성 점검 및 분석

김영민 [1], 최형기 [2]
[1] 성균관대학교 소프트웨어학과 학부생
[2] 성균관대학교 소프트웨어융합대학 교수

jsa5219@g.skku.edu, meosery@skku.edu

Analysis and Verification for Cloud Services in Microsoft

Young-Min Kim[1], Hyoung-Kee Choi[2]
[1]Dept. of Software, Sung-Kyun-Kwan University
[2]College of Computing and Informatics, Sung-Kyun-Kwan University

요 약

OneDrive 는 Microsoft 에서 제공하는 클라우드 스토리지 서비스이다. OneDrive 데스크톱 앱은 사용자가 로그아웃한 이후 재로그인을 시도할 때 사용자 기기에 저장되어 있던 토큰을 사용해 로그인을 진행하며, 사용자의 패스워드를 추가로 요구하지 않는다. 이는 로그아웃한 사용자의 유효한 로그인 정보가 기기에 남아있음을 의미하며, 본 연구에서는 이를 활용해 OneDrive 의 토큰 저장소를 분석하고 토큰 이식 공격이 가능함을 보인다.

1. 서론

OneDrive 는 Microsoft 에서 제공하는 클라우드 스토리지 서비스이다. OneDrive 는 Windows 8 이후 Windows 기본 프로그램에 포함되었으며 모바일 애플리케이션의 경우 구글 플레이스토어 다운로드 수 10 억 회 이상의 영향력 있는 애플리케이션이다.

OneDrive 데스크톱 앱은 개인용 계정을 사용하는 사용자가 로그아웃 한 이후 재로그인을 시도할 때 사용자의 패스워드를 요구하지 않는다. 이는 인증을 위해 사용된 토큰이 사용자 로그아웃 이후에도 유효한 상태로 기기에 저장되어 있음을 의미한다. 따라서 해당 토큰을 공격자가 획득할 수 있다면 공격자는 피해자의 데이터에 자유롭게 접근할 수 있게 된다.

본 연구에서는 역공학을 통해 OneDrive 의 토큰 저장소를 분석하고, 공격자가 피해자의 패스워드 없이 피해자 계정으로 로그인하는 토큰 이식 공격이 가능함을 보여 OneDrive 토큰 관리 시스템의 취약점을 밝힌다.

2. 배경 지식

2.1 DPAPI

Windows 에서는 운영체제에서 제공하는 암호화 기능을 사용해 데이터를 보호하는 프로그래밍 인터페이스 Data Protection API(DPAPI)를 제공한다. DPAPI 는 주로 사용자의 인증 정보, 개인 키 등의 민감한 정보를 암호화하는데 사용되며 사용자의 로컬 패스워드 혹은 키를 기반으로 데이터를 암호화하여 다른 기기에서는 해당 데이터를 복호화 할 수 없다는 특징을 갖는다.

2.2 Junction

Junction 은 폴더 간에 하위 폴더와 파일을 공유하기 위한 링크로 soft link (symbolic link)와 유사하다. 하지만 junction 은 폴더 간에만 작동하며 soft link 는 폴더, 파일 등을 대상으로 사용할 수 있다. 또한 soft link 는 local path, remote path 에 대한 링크를 수행할 수 있는데 반해 junction 은 local path 에 대한 링크만 가능하다.

3. 분석 환경

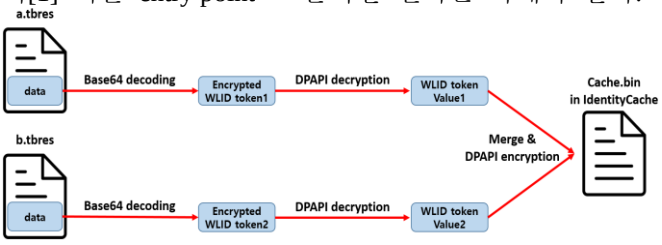
본 연구에서는 Windows 10 22H2 버전과 최신 OneDrive 버전(24.040.0225.0003 빌드)을 사용해 분석을 진행하였다. OneDrive 로그인 과정 분석을 위해서는 Wireshark 와 Frida 를 활용해 네트워크 패킷을 분석했으며 정적분석을 위해서는 IDA, 동적분석을 위해서는 WinDbg Preview 를 사용하였다.

4. 분석 내용

사용자가 OneDrive 데스크톱 앱에 로그인하는 경우 사용자의 id, pw 가 login.live.com 에 전달되고 refresh token 을 발급받는다. 이후 refresh token 을 사용해 암호화된 형태로 access token 을 발급받는다. 여기서 사용되는 access token 을 WLID token 이라고 한다. 사용

자가 재로그인을 시도하는 경우 기기에 저장된 WLID token 의 유효성을 검사하고 WLID token 이 유효한 경우 사용자의 pw 없이 로그인 절차가 진행된다.

WLID token 은 OneDrive Log file(ODL file)에 기록되며[1] 이를 entry point 로 분석한 결과는 아래와 같다.



(그림 1) WLID token derivation 과정 분석

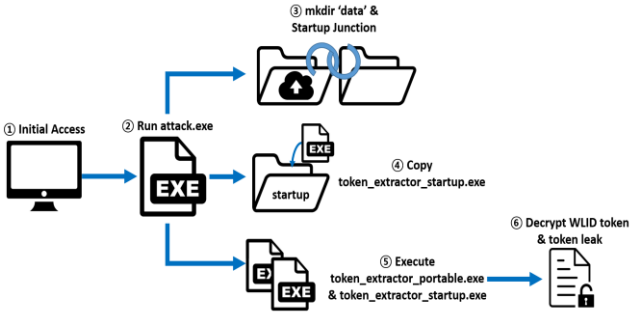
WLID token 값은 '%localappdata%\Microsoft\OneDrive \IdentityCache' 폴더 내 AT 폴더 내부에 DPAPI 암호화된 형태로 저장되며, 해당 데이터는'%localappdata% \Microsoft\OneDrive\Tokenbroker' 폴더로부터 base64 디코딩, DPAPI 복호화를 거쳐 캐싱된 결과로 생성됨을 확인했다.

이를 토대로 IdentityCache 폴더와 Tokenbroker 폴더 내 WLID token 이식을 시도하였다. 사용자가 OneDrive 에 로그인 하는 경우 Onedrive.exe 에서 IdentityCache 폴더 내 WLID token 의 존재와 유효성을 검증하고, 토큰이 유효한 경우에 사용자의 pw 없이 로그인 절차를 진행함을 검증했다. 결과적으로 IdentityCache 폴더 내 데이터를 피해자 기기에서 복호화 한 이후 공격자 기기에서 암호화하여 이식했을 때 토큰 이식 공격이 가능함을 확인했다.

5. 공격 시나리오

본 논문에서는 WLID token 저장소 분석 결과를 활용해 공격자가 피해자의 WLID token 을 갱신, 지속적으로 피해자 기기에 접근할 수 있는 공격 시나리오를 제안한다. 공격 시나리오는 3 단계로 구성된다.

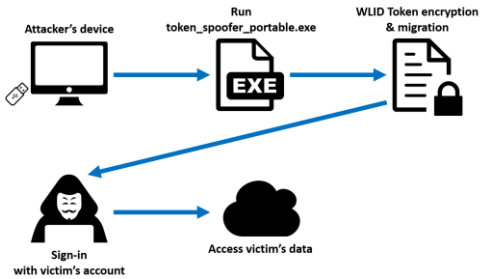
5.1 Phase1



(그림 2) Phase1 Overview

Phase1 은 공격자가 피해자의 토큰을 추출하는 과정이다. 공격자는 피해자 기기에 접근하여 attack.exe 를 실행한다. attack.exe 는 피해자의 OneDrive 에 data 폴더를 생성하고 시작프로그램 폴더를 junction 으로 OneDrive 에 동기화한다. 이후 피해자의 시작프로그램 폴더에 모니터링 프로그램을 복제하고 token extractor 를 실행하여 피해자 기기에 저장된 피해자의 계정정보와 WLID token 을 추출한다.

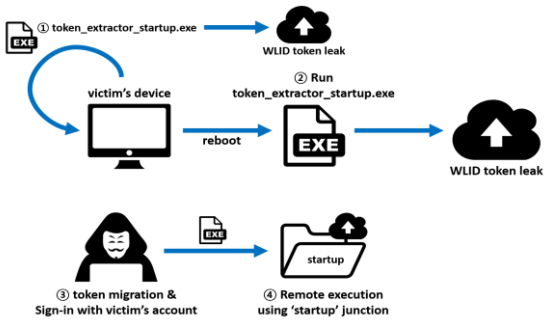
5.2 Phase2



(그림 3) Phase2 Overview

Phase2 는 추출된 피해자의 WLID token 을 공격자 기기에 이식하는 과정이다. 공격자는 자신의 기기에서 token spoofer 를 실행하여 피해자의 WLID token 을 이식한다. 토큰 이식 이후 Phase1 에서 추출된 피해자의 계정으로 Onedrive 데스크톱 앱에 로그인을 시도하면 pw 없이 로그인 절차가 진행되고 피해자의 데이터가 공격자 기기에 동기화 된다.

5.3 Phase3



(그림 4) Phase3 Overview

Phase3 에서는 피해자 기기에서 실행되는 백그라운드 프로세스를 통한 WLID token 갱신과 시작프로그램 폴더 junction 을 활용한 원격 실행을 수행한다. 앞서 Phase1 에서 공격자가 실행시킨 모니터링 프로그램이 일정 시간 간격으로 피해자 기기의 WLID token 을 복호화 하여 피해자의 OneDrive 에 업로드 한다. 피해자가 기기를 재부팅 하더라도 시작프로그램 폴더 내 모니터링 프로그램이 실행되어 WLID token 이 지속적으로 유출된다. 공격자는 피해자의 OneDrive 에서 갱신된 피해자의 WLID token 을 공격자 기기에 반복하여 이식함으로써 반영구적으로 토큰을 활용할 수 있다. 또한 공격자는 피해자의 OneDrive 내 시작프로그램 junction 을 활용해 피해자가 기기를 재부팅 할 때 공격자의 실행 파일을 원격으로 실행할 수 있다.

6. 결론

본 논문에서는 Microsoft OneDrive 의 WLID token 을 활용한 토큰 이식 공격과 토큰의 반영구적 갱신 및 원격 실행이 가능함을 보였다. 이를 통해 토큰을 활용한 공격의 확장성과 사용자 로그아웃 이후 토큰을 적절히 만료하는 것의 중요성을 재고하게 한다.

참고문헌

[1] Or Yair, "One Drive, Double Agent: Clouded OneDrive Turns Sides", Blackhat USA, Las Vegas, 2023