

302 – User Behavior Analysis

Team Information

Team Name : DogeCoin

Team Member : Dongbin Oh, Donghyun Kim, Donghyun Kim, Yeongwoong Kim

Email Address : dfc-dogecoin@naver.com

Instructions

Description The *image.ad1* is an image file of a virtual machine stored in Laptop of the ticket scalper. All files created by the ticket scalper for ticketing are stored in the *Download* folder. Answer the following questions by analyzing forensic artifacts stored in the image. (Note, the basis for your judgement must be detailed.)

Target	Hash (MD5)
image.ad1	d143860a40403a4cb809f64906c6b2d7

Questions

1. What is the macro file that the ticket scalper used for ticketing? (25 points)
2. What program did the ticket scalper use for the ticketing? (25 points)
3. What program did the ticket scalper use to edit the macro file? (125 points)
4. When did the ticket scalper execute the macro? (50 points)
5. What web browser(s) did the ticket scalper use to run the macro? (75 points)

Teams must:

- Develop and document the step-by-step approach used to solve this problem to allow another examiner to replicate team actions and results.
- Specify all tools used in deriving the conclusion(s).

Tools used:

Name:	REGA	Publisher:	4&6TECH
Version:	1.5.3		
URL:	http://forensic.korea.ac.kr/tools.html		

Name:	WinPrefetchView	Publisher:	NirSoft
Version:	1.35		
URL:	https://www.nirsoft.net/utils/win_prefetch_view.html		

Name:	PECmd	Publisher:	Eric Zimmerman
Version:	1.4.0.0		
URL:	https://ericzimmerman.github.io/		

Name:	BrowsingHistoryView	Publisher:	NirSoft
Version:	2.20		
URL:	https://www.nirsoft.net/utils/browsing_history_view.html		

Name:	LECmd	Publisher:	Eric Zimmerman
Version:	1.4.0.0		
URL:	https://ericzimmerman.github.io/		

Name:	Registry Explorer	Publisher:	Eric Zimmerman
Version:	1.6.0.0		
URL:	https://ericzimmerman.github.io/#!index.md		

Name:	JumpListsView	Publisher:	NirSoft
Version:	1.16		
URL:	https://www.nirsoft.net/utils/jump_lists_view.html		

Name:	FTK Imager	Publisher:	AccessData
Version:	1.16		
URL:	https://accessdata.com/products-services/forensic-toolkit-ftk/ftkimager		

Name:	WindowsTimeline Parser	Publisher:	Kacos2000
Version:	2.0.81.0		
URL:	https://github.com/kacos2000/WindowsTimeline		

Step-by-step methodology:

시스템 기본정보

설치 OS	Windows 10 Home
빌드 버전	19042
유저명	test
설치 시각	2021-03-16 08:47:05 (UTC+09:00)
System Root	C:\Windows

I. 티켓팅에 사용한 매크로 파일

1. 의심 파일 목록

티켓 암호상이 티켓팅을 위해 생성한 파일은 모두 Downloads 폴더에 저장되어 있다는 전제가 주어졌으므로 주어진 이미지 파일에서 Downloads 폴더를 먼저 분석하였다.

그림과 같이 표시한 5 개의 항목이 매크로를 위해 사용한 파일로 의심되었다.

AccessData FTK Imager 4.2.0.13

File View Mode Help

Evidence Tree

- Roaming
- Microsoft
- Windows
- Recent
- AutomaticDestinations
- CustomDestinations
- Downloads
 - 7z1900-x64.exe
 - AutoHotkey_1.1.33.06_setup.exe
 - BraveBrowserSetup.exe
 - csvfileview-x64
 - csvfileview-x64.zip
 - dnGREP_2.9.326.x64.msi
 - epp540_3430_64bit.exe
 - Macro-master
 - Macro-master.zip
 - MacroRecorderSetup.exe

File List

Name	Size	Type	Date Modified
PUBG-Macro-Assist-master	1	Directory	2021-04-19(월) 오전 2:05:01
nircmd-x64	1	Directory	2021-04-19(월) 오전 1:29:41
Macro-master	1	Directory	2021-04-19(월) 오전 2:06:12
csvfileview-x64	1	Directory	2021-03-29(월) 오전 4:54:07
확인된~1.CRD		\$I30 INDEX Entry	
VSCoUserSetup-x64-1.54.3.exe	71,420	Regular File	2021-03-29(월) 오전 3:19:13
Sublime Text Build 3211 x64 Setup.exe	10,675	Regular File	2021-04-19(월) 오전 1:36:18
python-3.9.2-amd64.exe	27,625	Regular File	2021-03-29(월) 오전 3:09:51
python-3.7.4-amd64.exe	26,056	Regular File	2021-03-29(월) 오전 3:21:16
PUBG-Macro-Assist-master.zip	545	Regular File	2021-04-19(월) 오전 2:03:07
npp.7.9.5.Installer.x64.exe	4,135	Regular File	2021-04-19(월) 오전 1:35:07
nircmd-x64.zip	153	Regular File	2021-04-19(월) 오전 1:29:04
MacroRecorderSetup.exe	18,397	Regular File	2021-04-19(월) 오전 2:00:47
Macro-master.zip	943	Regular File	2021-04-19(월) 오전 2:03:28
epp540_3430_64bit.exe	2,562	Regular File	2021-04-19(월) 오전 1:36:49
dnGREP_2.9.326.x64.msi	5,901	Regular File	2021-03-15(월) 오후 11:53:17
dfc_concert.ahk	8	Regular File	2021-04-19(월) 오전 3:01:51
desktop.ini	1	Regular File	2021-03-15(월) 오전 11:49:02
csvfileview-x64.zip	159	Regular File	2021-03-29(월) 오전 4:53:39
BraveBrowserSetup.exe	1,215	Regular File	2021-04-19(월) 오전 2:07:18
AutoHotkey_1.1.33.06_setup.exe	3,193	Regular File	2021-04-19(월) 오전 1:27:58
7z1900-x64.exe	1,414	Regular File	2021-04-19(월) 오전 2:05:36
\$I30	8	NTFS Index Allocation	2021-04-19(월) 오전 2:07:18

암표상은 dfc_concert.ahk 파일을 사용한 것으로 보인다. ahk 파일은 Autohotkey 프로그램의 스크립트 파일 확장자이다. Autohotkey 는 마우스나 키보드 조작, 프로그램 실행 등에 이르기까지 전방위적인 행위를 자동화할 수 있어 매크로에 주로 사용되며 ahk 확장자를 가진 스크립트 형태 혹은 exe 로 컴파일하여 실행될 수 있다.

2. 사용된 매크로 파일 - dfc_concert.ahk

dfc_concert.ahk 파일의 내용은 다음과 같이 티켓팅 페이지를 열고 목표 이미지를 찾아 클릭하도록 하고 있다.

```
;window.open('http://ticket.dfc2021.com/Book/BookSession.asp?GroupCode=210015758&Tiki=&Point=&PlayDate=20210501', '_self');

TARGET:=1
START_X:=99
START_Y:=180
LAST_X:=550
LAST_Y:=400

ST_X1:=700
ST_Y1:=400
ST_X2:=100
ST_Y2:=500

ENABLE_STAGE:=0
ENABLE_TABLE:=0
REVERSE_MODE:=1

IMG:="p.png"
IMG_S:="p.png"

TABLE MON X:=805
```

```

f7::
Main_Loop:
global stop
global interrupt
stop      := 0
interrupt := 0
Loop
{
    a:=search_split_by_group(TARGET,START_X,START_Y,LAST_X, LAST_Y,IMG,STDUNIT,STDUNIT)
    if(a>0){
        Move_And_Click(806,630)
        Alert_Audio()
        break ; 30 + 30 = 60ms
    }

    else{
        if(ENABLE_TABLE==1){
            Move_And_Click(817,189)
            sleep,TIME_SLEEP
            Move_And_Click(752,189)
            interrupt :=1
            sleep,TIME_SLEEP
        }
        else
        {
            Move_And_Click(590,110)
            Send, {up}
            Send, {Enter}
            sleep,TIME_SLEEP
            interrupt :=0
            Move_And_Click(590,110)
            Send, {down}
            Send, {Enter}
            sleep,TIME_SLEEP
        }
        if(stop==1){
            Send, ^!t ; exit threads signal
            Alert_Audio()
            break
        }
        interrupt :=0
    }
}
Return

```

3. 그 외 파일

PUBG-Macro-Assist-master 와 Macro-master 는 폴더명 마지막 부분에 -master 라는 문자열이 붙은 명명규칙이나, 같은 이름의 압축파일이 존재하는 것으로 보아 github 에서 master 브랜치를 다운로드 받은 후 압축 해제된 것으로 추측할 수 있다.

실제로 다음의 링크에서 같은 파일을 다운로드 받을 수 있었으며 다운로드 받은 zip 파일과 이미지상의 zip 파일의 해시값이 동일한 것을 확인하였다.

PUBG-Macro-Assist-master	GitHub - mgsweet/PUBG-Macro-Assist: Some macros for PUBG coded by autohotkey.	132CD3AC00D 3F6A4B1F1987 906EBF068
--------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------

Macro-master	GitHub - zhamlin/Macro: A macro program written in autohotkey	F6FF1B8450EA 91FF895B3091 6167DDF5
--------------	-------------------------------------------------------------------------------	------------------------------------------

PUBG-Macro-Assist-Master 는 유명 온라인 FPS 게임인 PLAYERUNKNOWN'S BATTLEGROUNDS 에 사용되는 매크로이며, Macro-Master 는 링크파일이 남아있지 않아 참조조차 하지 않은 것으로 확인되어 사용한 매크로가 아니라고 추정할 수 있었다.

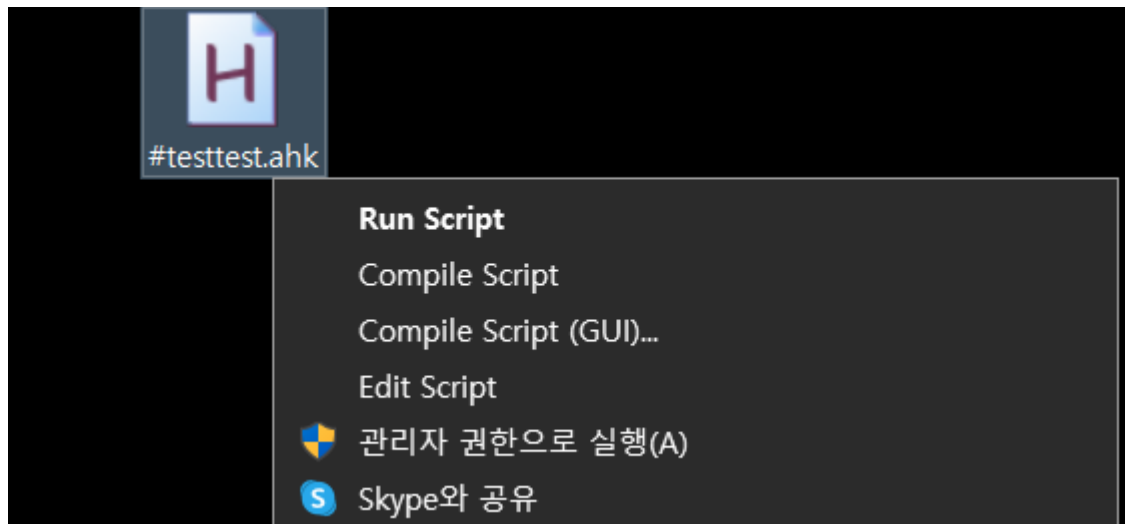
II. 티켓팅에 사용한 프로그램

1. 설치된 프로그램 목록

레지스트리상 설치된 프로그램 중 주요 프로그램을 선별하였다. 상술한 Autohotkey 와 MacroRecorder 를 제외, .ahk 파일 실행과 관련된 유의미한 프로그램은 추가적으로 발견되지 않았다.

2. 티켓팅에 사용한 프로그램

ahk 파일은 ahk 파일 그대로 실행하거나, exe 파일로 컴파일하여 실행할 수 있다. ahk 파일 그대로 실행할 경우 autohotkey.exe 프로그램이 실행되며 exe 파일로 컴파일하여 실행하면 exe 파일만 실행된다.



Exe 파일형태로 실행되었는지, 스크립트로 실행되었는지 확인하기 위하여 프리패치를 분석하였다. 프리패치 파일은 윈도우 XP 이후 운영체제에서 제공하는 메모리 관리 정책으로 인해 부팅 또는 응용프로그램을 시작할 때 성능 향상을 위해 구현된 기능이다. 프리패치 파일에 실행 파일이 사용하는 시스템 자원을 미리 저장하였다가 윈도우 부팅 시 프리패치 파일을 모두 메모리에 로드하여 실행 속도를 향상시킨다. 프리패치 파일을 분석하면 실행 파일 정보 (실행 파일명, 파일경로 등), 실행 파일의 실행 횟수, 실행 파일의 마지막 실행 시간, 실행 파일의 최초 실행 시간 등의 정보를 알 수 있다. 프리패치 파일은 %SystemRoot%\WinPrefetch 경로에 저장된다.

프리패치를 분석한 결과 dfc_concert 를 컴파일한 .exe 파일이 실행된 흔적을 확인할 수 없었으며, Autohotkey.exe 에서 dfc_concert.ahk 파일을 참조한 사실을 확인할 수 있었으므로 티켓팅에 사용한 프로그램은 Autohotkey.exe 이다.

III. 티켓 압표상이 매크로 파일 편집에 사용한 프로그램

매크로 파일(df_cconcert.ahk)의 편집 시각에 사용한 프로그램을 특정하기 위해서는 다음과 같은 정보가 필요하다.

- 편집을 위해 사용한 프로그램 정보
 - 편집이 가능한 프로그램 중 실행된 것
 - 편집 프로그램 실행 시각
- 매크로 파일의 MAC (수정, 접근, 생성) 시각
- 점프리스트와 Recent 에 기록된 매크로 파일의 시간 정보
 - Ink 파일의 생성 시각
 - Ink 내부에 기록된 매크로 파일의 MAC 시각
 - Ink 가 기록된 Entry 생성 시각 (Record time)
- 타임라인 Open File, In Use / Focus 행위의 시작과 종료

1. 매크로 파일 편집 프로그램 특정

파일을 편집할 수 있는 프로그램의 실행 흔적을 프리패치를 통해서 확인하였으며, 이를 정리하면 아래 표와 같다.

프로그램	매크로 파일 참조	출처
notepad.exe	X	프리패치
notepad++.exe	O	프리패치
editplus.exe	O	프리패치
sublimetext.exe	O	프리패치

2. 타임라인 작성 및 매크로 파일 편집한 프로그램 특정

매크로 파일의 생성 시각과 수정 시각을 범위로 아래와 같이 타임라인을 작성하였다.

시간 표현은 년, 월, 일 및 소수점을 생략했으며, 실행 프로그램 시각은 **2. 매크로 파일 편집 프로그램 특정**에서 파악한 편집 프로그램과 Autohotkey 에 대해서만 기록하였다.

시각	행위	자세히	아티팩트	시각 출처
10:28:36	프로그램 실행	Autohotkey	프리패치	실행 시각
10:28:36	프로그램 실행	Autohotkey	프리패치	실행 시각
10:55:20	생성	dfc_concert.ahk	파일시스템	생성 시각
10:55:20	생성	dfc_concert.ahk [Notepad]	점프리스트	Target 파일 생성 시각
10:55:20	생성	dfc_concert.ahk [Autohotkey]	점프리스트	Target 파일 생성 시각
10:55:20	생성	dfc_concert.ahk [Quick Access]	점프리스트	Target 파일 생성 시각
11:48:55	프로그램 실행	Autohotkey	프리패치	실행 시각
11:49:02	프로그램 실행	Notepad	프리패치	실행 시각
11:49:03	파일 열람	PUBG-Macro-Assist-masterWPUBG_Assist_v1.2.3.ahk [Notepad]	타임라인	시작 시각
11:49:12	프로그램 종료	PUBG-Macro-Assist-masterWPUBG_Assist_v1.2.3.ahk [Notepad]	타임라인	종료 시각
11:49:27	프로그램 실행	Notepad	프리패치	실행 시각
11:49:27	파일 열람	PUBG-Macro-Assist-masterWPUBG_Assist_v1.2.3.ahk [Notepad]	타임라인	시작 시각
11:50:12	프로그램 종료	PUBG-Macro-Assist-masterWPUBG_Assist_v1.2.3.ahk [Notepad]	타임라인	종료 시각
11:52:10	프로그램 실행	Sublime Text	프리패치	실행 시각
11:52:12	프로그램 실행	? [Sublime Text]	타임라인	시작 시각
11:52:25	프로그램 종료	? [Sublime Text]	타임라인	종료 시각
11:52:31	프로그램 실행	Notepad++	프리패치	실행 시각
11:52:31	프로그램 실행	Notepad++? [Notepad++]	타임라인	시작 시각
11:52:46	프로그램 종료	? [Notepad++]	타임라인	종료 시각
11:52:57	프로그램 실행	EditPlus	프리패치	실행 시각
11:52:57	프로그램 실행	? [EditPlus]	타임라인	시작 시각
11:52:59	프로그램 실행	? [EditPlus]	타임라인	시작 시각
11:52:59	프로그램 종료	? [EditPlus]	타임라인	종료 시각
11:53:01	프로그램 종료	? [EditPlus]	타임라인	종료 시각
11:53:02	프로그램 실행	? [EditPlus]	타임라인	시작 시각
11:53:34	프로그램 실행	? [EditPlus]	타임라인	시작 시각
11:53:36	프로그램 종료	? [EditPlus]	타임라인	종료 시각
11:53:44	프로그램 종료	? [EditPlus]	타임라인	종료 시각
11:55:03	프로그램 실행	Sublime Text	프리패치	실행 시각
11:55:03	프로그램 실행	? [Sublime Text]	타임라인	시작 시각
11:55:41	복사/붙여넣기	? [Sublime Text]	타임라인	시작 시각
11:55:48	프로그램 실행	Notepad++	프리패치	실행 시각

11:55:48	프로그램 실행	? [Notepad++]	타임라인	시작 시각
11:55:52	프로그램 종료	? [Notepad++]	타임라인	종료 시각
11:56:02	복사/붙여넣기	Notepad++	타임라인	시작 시각
11:57:10	프로그램 실행	Autohotkey	프리패치	실행 시각
11:57:14	파일 열람	Autohotkey? [Autohotkey]	타임라인	시작 시각
11:57:57	프로그램 실행	Notepad++	프리패치	실행 시각
11:57:57	프로그램 실행	? [Notepad++]	타임라인	시작 시각
12:00:02	프로그램 실행	EditPlus	프리패치	실행 시각
12:00:02	프로그램 실행	? [EditPlus]	타임라인	시작 시각
12:00:17	수정	dfc_concert.ahk [Notepad]	점프리스트	Target 파일 수정 시각
12:00:30	프로그램 종료	? [Sublime Text]	타임라인	종료 시각
12:00:33	프로그램 종료	? [EditPlus]	타임라인	종료 시각
12:00:44	프로그램 종료	? [Notepad++]	타임라인	종료 시각
12:01:03	프로그램 실행	Notepad	프리패치	실행 시각
12:01:09	생성	dfc_concert.ahk.lnk	파일시스템	생성 시각
12:01:09	파일 열람	dfc_concert.ahk [Notepad]	타임라인	시작 시각
12:01:09	접근	dfc_concert.ahk [Notepad]	점프리스트	Target 파일 접근 시각
12:01:15	복사/붙여넣기	dfc_concert.ahk [Notepad]	타임라인	시작 시각
12:01:51	마지막 수정	dfc_concert.ahk	파일시스템	수정 시각
12:01:51	수정	dfc_concert.ahk [Autohotkey]	점프리스트	Target 파일 수정 시각
12:01:51	수정	dfc_concert.ahk [Quick Access]	점프리스트	Target 파일 수정 시각
12:01:51	접근	dfc_concert.ahk [Autohotkey]	점프리스트	Target 파일 접근 시각
12:01:55	프로그램 종료	dfc_concert.ahk [Notepad]	타임라인	종료 시각
12:02:03	프로그램 실행	Autohotkey	프리패치	실행 시각
12:02:14	파일 열람	dfc_concert.ahk [Autohotkey]	타임라인	시작 시각
12:02:24	파일 열람	dfc_concert.ahk [Notepad]	타임라인	시작 시각
12:02:24	마지막 열람 시각	dfc_concert.ahk [Notepad]	점프리스트	Entry 기록 시각
12:02:34	프로그램 종료	dfc_concert.ahk [Notepad]	타임라인	종료 시각
14:51:14	프로그램 실행	? [EditPlus]	타임라인	시작 시각
14:51:51	프로그램 종료	? [EditPlus]	타임라인	종료 시각
14:53:59	마지막 접근	dfc_concert.ahk	파일시스템	접근 시각
14:53:59	마지막 수정	dfc_concert.ahk.lnk	파일시스템	수정 시각
14:53:59	마지막 접근	dfc_concert.ahk.lnk	파일시스템	접근 시각

14:53:59	프로그램 실행	Autohotkey	프리패치	실행 시각
14:53:59	마지막 열람 시각	dfc_concert.ahk [Autohotkey]	점프리스트	Entry 기록 시각
14:53:59	마지막 열람 시각	dfc_concert.ahk [Quick Access]	점프리스트	Entry 기록 시각
14:53:59	접근 시각	dfc_concert.ahk [Quick Access]	점프리스트	Target 파일 접근 시각

타임라인에서 대괄호 ([])로 표현된 것은 파일 열람을 위해 사용한 프로그램을 나타내며, 매크로 파일을 편집한 프로그램을 특정할 수 있는 구간을 **주황색** 행으로 표현하였다. 해당 구간에는 메모장(Notepad)가 실행되고 있었으며, 종료되기 직전에 매크로 파일의 수정 시각과 접근 시각이 12:01:51 로 동시에 갱신되었다. 메모장으로 매크로 파일을 편집한 것으로 추정할 수 있지만, 12:01:51 수정 이전에 다른 프로그램으로 편집했을 가능성을 살펴보았다.

다른 프로그램으로 편집했을 가능성이 존재하는 근거는 다음과 같다. → 쟁점 사항

근거 1. 점프리스트에서 파일을 열람했지만 기록되지 않는 경우가 있음

- A. 컨텍스트 메뉴(우 클릭)로 파일 열었을 때
- B. 프로그램을 먼저 실행하고, "파일 열기"로 열람했을 때

근거 2. 점프리스트에 기록된 매크로 파일의 생성 시각과 수정 시각 차이

- A. 메모장으로 열람 시, 생성 시각(10:55:20)과 수정 시각(12:00:17)
- B. Autohotkey 와 Quick Access 열람 시, 생성 시각(10:55:20)과 수정 시각(12:01:51)




근거 1 을 통해서 점프리스트에 기록된 메모장을 제외한 EditPlus, Sublime Text, Notepad++ 중 하나를 근거 1 의 A 또는 B 의 경우로 실행하여 편집할 수 있다. 또한, 근거 2 를 통해서 파일이 생성되면 일반적으로 생성, 수정, 접근 시각이 모두 동일한데, 본 매크로 파일은 생성 시각 10:55:20 이후로 수정 시각 12:00:17 과 12:01:51 을 통해서 2 번 수정되었다고 볼 수 있다.

우선, 가능성을 확인하기 전에 NTFS 파일시스템의 접근 시각 갱신 여부를 나타내는 값을 확인하였다. NtfsDisableLastAccessUpdate 의 설정 값에 따라 NTFS 파일시스템에 기록되는 접근 시각 갱신이 달라진다. 0x80000000 과 0x80000002 는 접근 시각이

갱신되고, 0x80000001 과 0x80000003 은 접근 시각이 갱신되지 않는다. 값의 의미는 다음과 같다.

- 0x80000000: 사용자 파일 및 폴더 대상. 접근 시각 갱신 활성화
- 0x80000001: 사용자 파일 및 폴더 대상. 접근 시각 갱신 비활성화
- 0x80000002: 시스템 (사용자 포함) 파일 및 폴더 대상. 접근 시각 갱신 활성화
- 0x80000003: 시스템 (사용자 포함) 파일 및 폴더 대상. 접근 시각 갱신 비활성화

아래 그림과 같이 주어진 시나리오에서는 0x80000002 (2147483650)이므로, 접근 시각 갱신이 활성화되어 있다. NTFS 에서 접근 시각은 갱신되고 나서 1 시간이 지나야 다시 갱신되며, 1 시간 내로 다시 접근하더라도 접근 시각은 갱신되지 않는다.

Value Name	Value Type	Data
		
NtfsDisable8dot3NameCreation	RegDword	2
NtfsDisableCompression	RegDword	0
NtfsDisableEncryption	RegDword	0
NtfsDisableLastAccessUpdate	RegDword	2147483650
NtfsDisableLfsDowngrade	RegDword	0

점점 사항 해결을 위한 NTFS 시간 값 규칙은 다음과 같다.

- 규칙 1. 접근 시각은 갱신되고 나서 1 시간이 지나야 다시 갱신됨
- 규칙 2. 파일 수정 시, 수정과 접근 시각이 동시에 갱신됨
- 규칙 3. 파일 수정으로 갱신된 접근 시각도 똑같이 법칙 1 의 영향을 받는다.

점프리스트에 기록된 매크로 파일의 시간 값을 아래 표와 같이 정리하였다.

CASE	시간 출처	Entry 갱신	수정 시각	접근 시각	생성 시각
1	점프리스트 [Notepad]	12:02:24	12:00:17	12:01:09	10:55:20
2	점프리스트 [Autohotkey]	14:53:59	12:01:51	12:01:51	10:55:20
3	점프리스트 [Quick Access]	14:53:59	12:01:51	14:53:59	10:55:20

CASE1 이 다른 프로그램으로 편집하면서 기록된 것이라면, 사용자는 다음과 같은 순서로 행위를 해야한다.

1. 12:00:17 이전에 다른 편집 프로그램으로 열람 (점프리스트에 안 남게)
2. 12:00:17 에 편집 → 수정 시각과 접근 시각이 12:00:17 로 갱신
3. 12:01:09 에 다시 열람
4. 그 후 메모장으로 다시 열람 후 매크로 파일 편집

시나리오에서 3 번 (12:01:09 에 다시 열람) 행위는 **NTFS 시간 값 규칙 3**을 만족하지 못하며, 12:00:17 시각에 매크로 파일을 편집했다고 보기에는 어렵다.

또한, 수정 시각과 접근 시각이 1 시간 이내로 차이나는 경우는 일반적이지 않음에도 불구하고, 본 시나리오에 나타난 이유는 다음과 같은 실험으로 확인하였다.

구성: NtfsDisableLastAccessUpdate 의 값이 0x80000002 로 설정된 가상머신
(본 시나리오 동일한 환경)

상황: 로컬에서 가상머신으로 파일이 복사될 때

- 생성 시각과 수정 시각 → 로컬 파일시스템의 시간 값을 따름
- 접근 시각 → 가상머신으로 복사된 순간으로 갱신됨
 - 1 시간 이내 다시 접근하여도 접근 시각이 갱신됨

모든 상황을 정리하면 다음과 같다.

- | | |
|------------------------------------|--------|
| 1. 10:55:20 - 매크로 파일 생성 | (로컬) |
| 2. 12:00:17 - 마지막으로 수정 | (로컬) |
| 3. 12:00:17 ~ 12:01:09 - 가상머신으로 복사 | |
| 4. 12:01:09 - 매크로 파일 열람 [Notepad] | (가상머신) |
| 5. 12:01:51 - 매크로 파일 수정 [Notepad] | (가상머신) |

답: 메모장 (Notepad)

IV. 매크로를 실행한 시각

Autohotkey 매크로를 실행하면 autohotkey.exe 가 실행되며, 프리패치 참조목록 상에도 기록이 남는다. 또한 점프리스트 상 엔트리 수정시각이 실행시각으로 수정된다. 프리패치 상 실행 시각과 점프리스트 수정시각을 비교하면 언제 어떤 파일을 실행했는지 알 수 있다.

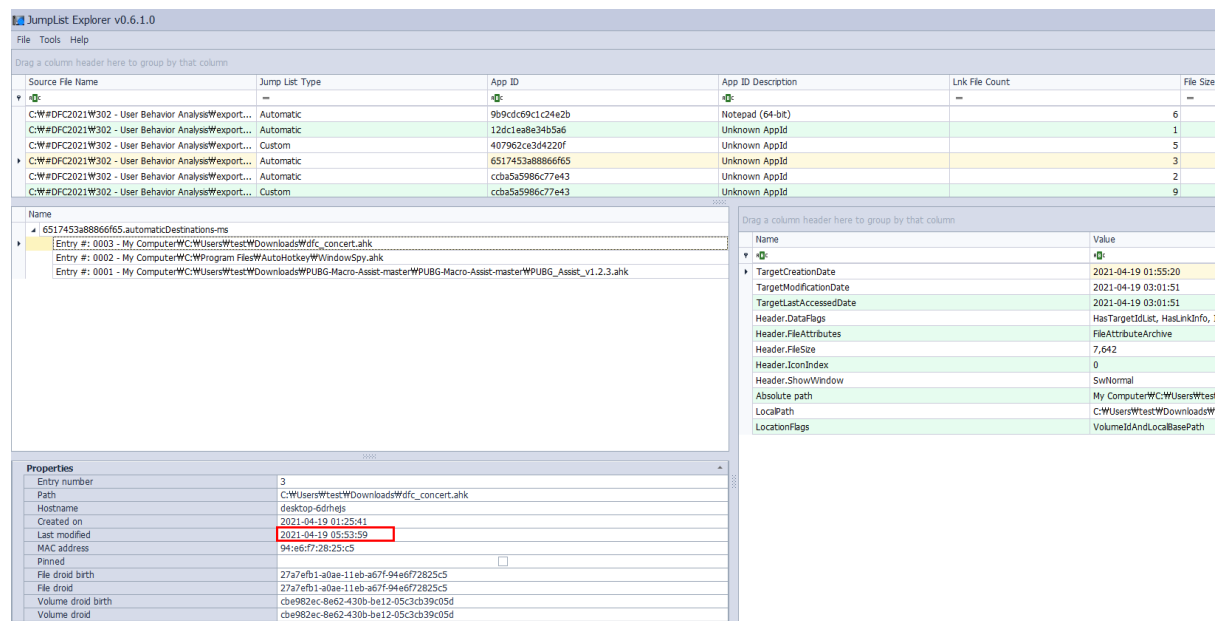


그림 1 Autohotkey 점프리스트

다음은 점프리스트와 프리패치를 비교하여 작성한 타임라인이다.

시간(utc+9)	행위	출처
2021.04.19 10:28:20	Autohotkey 설치	레지스트리
2021.04.19 10:28:36	Autohotkey 실행	프리패치
2021.04.19 10:55:20	Dfc_concert.ahk 생성	링크파일 target creation time
2021.04.19 11:48:55	Autohotkey 실행(PUBG_Assist_v1.2.3.ahk)	프리패치 점프리스트 Entry Last modified
2021.04.19 11:57:10	AutoHotkey.exe 실행(WindowSpy.ahk)	프리패치 점프리스트 수정시각
2021-04-19 12:00:17	Dfc_concert.ahk 수정	링크파일 TargetModificationTime
2021-04-19 12:01:51	Dfc_concert.ahk 수정	링크파일 TargetWriteTime
2021-04-19 12:02:03	AutoHotkey.exe 실행	프리패치
2021-04-19 14:51:48	MSEdge.exe 실행	프리패치

2021-04-19 14:53:40	Brave Browser 실행	프리패치
2021-04-19 14:53:45	Brave Browser 실행	프리패치
2021-04-19 14:53:59	AutoHotkey.exe 실행 (dfc_concert.ahk 실행)	프리패치, LNK AccessTime, TargetAccessTime, 점프리스트 Entry Last modified

Dfc_concert.ahk 가 작성된 후 4 번 실행된 Autohotkey 중 2 번은 각각 PUBG_Assist_v1.2.3.ahk, WindowSpy.ahk 가 실행되었고 dfc_concert.ahk 가 실행된 것으로 의심되는 시각은 12:02:03 과 14:53:59 이다. 그림 3 의 Autohotkey 점프리스트 기록을 보면 14:53:59 에 dfc_concert.ahk 가 실행된 것은 확인되나 12:02:03 에 실행되었는지는 확실히 알 수 없다. 이를 확인하기 위하여 추가적으로 windows10 타임라인 아티팩트에서 Autohotkey 관련 데이터를 선별하였다.

	Application	Display Name	File Opened	AppActivityId	Type	Group	ActivityType	StartTime	EndTime	Duration
209	{ProgramFilesX64}\AutoHotkey\AutoHotkey.exe	AutoHotkey	AutoHotkey	NaN	NaN	NaN	Open App/File/Url (5)	2021-04-19T02:57:14	NaN	NaN
210	{ProgramFilesX64}\AutoHotkey\AutoHotkey.exe	NaN	NaN	NaN	UserEngaged	NaN	App In Use/Focus (6)	2021-04-19T02:57:14	2021-04-19T02:57:40	00:00:16
219	{ProgramFilesX64}\AutoHotkey\AutoHotkey.exe	AutoHotkey	dfc_concert.ahk	{Local Downloads}\dfc_concert.ahk	NaN	NaN	Open App/File/Url (5)	2021-04-19T03:02:14	NaN	NaN
220	{ProgramFilesX64}\AutoHotkey\AutoHotkey.exe	NaN	NaN	{Local Downloads}\dfc_concert.ahk	UserEngaged	NaN	App In Use/Focus (6)	2021-04-19T03:02:14	2021-04-19T03:02:20	00:00:06

그림 2 Autohotkey 관련 타임라인

그림 4 를 보면 Autohotkey 가 12:02:14 에서 12:02:20 까지 초점상태임을 알 수 있다. 실험 결과 Autohotkey 스크립트는 실행 시 프리패치에 즉시 기록이 남으나 Timeline 에는 ExecuteOpen 으로 기록이 남지 않고 아래 그림 5 와 같이 실행중인 상태임을 알리는데, 해당 아이콘을 더블클릭하면 Autohotkey 화면이 올라오면서, 이때 타임라인에 기록된다. 따라서 12:02:03 에 매크로가 실행되고 실행 중 해당 아이콘을 12:02:14 에 클릭하여 Autohotkey 화면을 6 초간 보고 있었던 것을 알 수 있다. **매크로가 실행된 시각은 2021-04-19 12:02:03 과 2021-04-19 14:53:59 이다.**

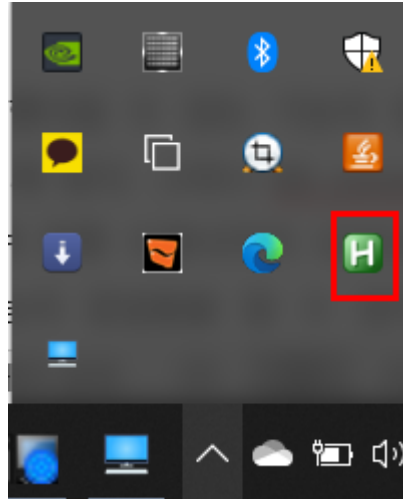


그림 3 실행중 상태

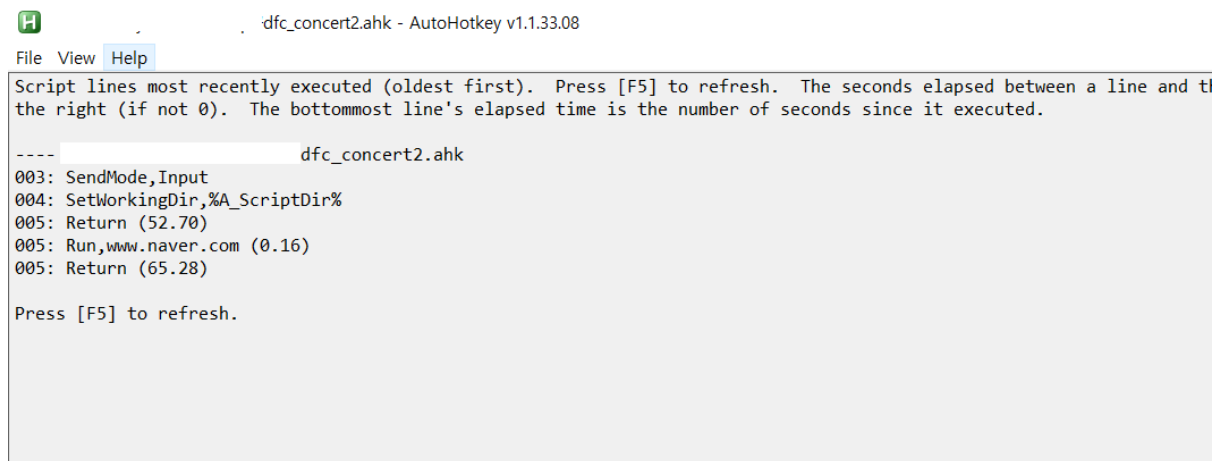


그림 4 더블클릭시 Autohotkey 화면

3. Timeline 분석

dfc_concert.ahk 는 마우스 매크로이다. 따라서 브라우저 상에서 작동하려면 브라우저가 화면에 떠있는 상태여야 한다. 상술했듯이 Windows10 Timeline 은 프로그램이 화면에 초점된 시각을 기록한다.

아래 그림 9 는 매크로 실행시각 전후의 브라우저 타임라인을 EndTime(화면 초점을 해제한 시각) 기준으로 정렬한 것이다.

214	MSEdge	NaN	NaN	UserEngaged	NaN	App In Use/Focus (6)	2021-04-19T02:58:37	2021-04-19T03:00:57
220	{ProgramFilesX64}\AutoHotkey\AutoHotkey.exe	NaN	NaN	UserEngaged	NaN	App In Use/Focus (6)	2021-04-19T03:02:14	2021-04-19T03:02:20
203	Brave	NaN	NaN	UserEngaged	NaN	App In Use/Focus (6)	2021-04-19T02:55:23	2021-04-19T03:03:40
226	Brave	NaN	NaN	UserEngaged	NaN	App In Use/Focus (6)	2021-04-19T05:53:40	2021-04-19T05:53:42
228	Brave	NaN	NaN	NaN	Snap	Copy/Paste (16)	2021-04-19T05:53:43	2021-04-19T05:53:43
229	Brave	NaN	NaN	NaN	Snap	Copy/Paste (16)	2021-04-19T05:53:48	2021-04-19T05:53:48
230	Brave	NaN	NaN	NaN	Snap	Copy/Paste (16)	2021-04-19T05:53:48	2021-04-19T05:53:48
227	Brave	NaN	NaN	UserEngaged	NaN	App In Use/Focus (6)	2021-04-19T05:53:42	2021-04-19T05:53:59

그림 7 매크로 실행시각 전후의 브라우저 타임라인

매크로가 브라우저 위에서 작동하기 위해서는 브라우저가 매크로 최초실행시각 이후의 시각까지는 화면에 초점상태여야 한다. 그림 9 를 보면 매크로 실행 시각인 12:02:03 이후까지도 화면 초점상태를 유지하고 있었던 브라우저는 Brave Browser 이므로 매크로를 실행한 브라우저는 **Brave Browser** 이다.

14:53:59 매크로 실행 당시에는 Brave Browser 와 Edge 브라우저 모두 초점 상태를 유지하고 있지 않았으므로 매크로가 실질적으로 작동하지 않았음을 알 수 있다.