



작성자	심주완
분석 일자	2024.05.23
작성 일자	2024.05.23
분석 대상	image.ad1
문서 버전	2.0
작성자 E-mail	rd002@naver.com

0. 목차

1. 문제 3

2. 분석 도구 3

3. 환경 3


4. Write-Up..... 4

5. Flag11

6. 별도 첨부12

7. Reference14

1. 문제

URL	-
문제 내용	<p>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.)</p> <p>(모든 문제 및 번역본은 별도첨부)</p>
문제 파일	 <p>image.ad1</p>
문제 유형	System Forensics
난이도	3 / 3

2. 분석 도구

도구명	다운로드 링크	Version
FTK Imager	https://www.exterro.com/digital-forensics-software/ftk-imager	4.7.1.2
JumpList Explorer	https://www.sans.org/tools/jumplist-explorer/	2.0.0.0
WinPrefetchView	https://www.nirsoft.net/utls/win_prefetch_view.html	1.37
Autopsy	https://www.autopsy.com/download/	4.20.0

3. 환경

OS
Windows 11 Home

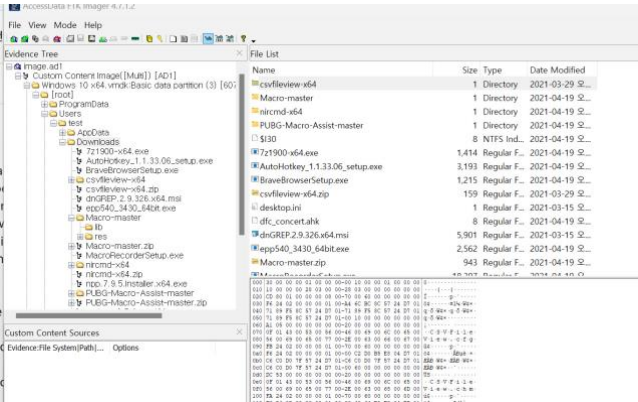
4. Write-Up

파일명	image.ad1
용량	602MB
SHA256	41a094f929963ac597e180ebf047817b5bbd9dc145fa8dd35dd16c3125166957
Timestamp	2021-04-21 11:02:56

한문제씩 문제를 풀어보자.

1. 암호상이 발견에 사용한 매크로 파일은 무엇입니까?

문제를 읽어보면 티켓팅에 사용한 파일은 Download 폴더에 저장되었다고 명시되어 있다. FTK Imager 를 통하여 파일을 확인해보자.



[그림 1] Download 폴더 내부

다음과 같은 파일들을 확인할 수 있었다. 폴더 내부를 조사하면서 의심되는 파일들을 추려보았다.

Name	Size	Type	Date Modified
csvfileview-x64	1	Directory	2021-03-29 오후 2:00
Macro-master	1	Directory	2021-04-19 오후 11:02
nircmd-x64	1	Directory	2021-04-19 오후 11:02
PUBG-Macro-Assist-master	1	Directory	2021-04-19 오후 11:02
\$I30	8	NTFS Ind...	2021-04-19 오후 11:02
7z1900-x64.exe	1,414	Regular F...	2021-04-19 오후 11:02
AutoHotkey_1.1.33.06_setup.exe	3,193	Regular F...	2021-04-19 오후 11:02
BraveBrowserSetup.exe	1,215	Regular F...	2021-04-19 오후 11:02
csvfileview-x64.zip	159	Regular F...	2021-03-29 오후 2:00
desktop.ini	1	Regular F...	2021-03-15 오후 11:02
dfc_concert.ahk	8	Regular F...	2021-04-19 오후 11:02
dnGREP.2.9.326.x64.msi	5,901	Regular F...	2021-03-15 오후 11:02
epp540_3430_64bit.exe	2,562	Regular F...	2021-04-19 오후 11:02
Macro-master.zip	943	Regular F...	2021-04-19 오후 11:02
MacroRecorderSetup.exe	18,397	Regular F...	2021-04-19 오후 11:02
nircmd-x64.zip	153	Regular F...	2021-04-19 오후 11:02
npp.7.9.5.Installer.x64.exe	4,135	Regular F...	2021-04-19 오후 11:02
PUBG-Macro-Assist-master.zip	545	Regular F...	2021-04-19 오후 11:02
python-3.7.4-amd64.exe	26,056	Regular F...	2021-03-29 오후 2:00
python-3.9.2-amd64.exe	27,625	Regular F...	2021-03-29 오후 2:00
Sublime Text Build 3211 x64 Setup.exe	10,675	Regular F...	2021-04-19 오후 11:02
VSCodeUserSetup-x64-1.54.3.exe	71,420	Regular F...	2021-03-29 오후 2:00
확인되~1.CRD	\$I30 IND...		

[그림 2] 의심되는 파일 목록

[WHS-2] .iso

그림 2 에서 강조한 부분이 의심되는 파일이고, 이에 관하여 한가지씩 짚어보겠다.

이 파일 중 dfc_concert.ahk 파일 내부는 다음과 같았다.

```

dfc_concert.ahk X
C:\Users> sim > OneDrive > 바탕 화면 > DFC > 2021 - 302 > dfc_concert.ahk
1 ;window.open('http://ticket.dfc2021.com/Book/BookSession.asp?GroupCode=210015758&Tiki=&Point=&PlayDate=20210501', 'self');
2
3 TARGET:=1
4 START_X:=99
5 START_Y:=100
6 LAST_X:=550
7 LAST_Y:=400
8
9 ST_X1:=700
10 ST_Y1:=400
11 ST_X2:=100
12 ST_Y2:=500
13
14 ENABLE_STAGE:=0
15 ENABLE_TABLE:=0
16 REVERSE_MODE:=1
17
18 IMG:="p.png"
19 IMG_S:="p.png"
20
21 TABLE_MON_X:=805
22 TABLE_MON:=245
23 TABLE_REN:=260
24
25 TIME:=70
26 TIME_SLEEP:=320
27
28 STDUNIT:=100
29
30 ; CONSTANT
31
32 PAY_X:=860
33 PAY_Y:=680
34
35 SMALLSIZE:=10
36 BIGSIZE:=25
  
```

[그림 3] dfc_concert.ahk 파일 내부 1

```

dfc_concert.ahk X
C:\Users> sim > OneDrive > 바탕 화면 > DFC > 2021 - 302 > dfc_concert.ahk
59 ; Search from image and pick up sth. And go to the next
60 Find_Img_Next(st_x,st_y,fi_x,fi_y,img_name){
61   imageSearch,ax,ay,st_x,st_y,fi_x,fi_y,*50 %img_name%
62   IF (ErrorLevel==0) {
63     mousemove,ax+2,ay+2,0
64     MouseClick,Left
65     MouseMove,840,679,0
66     MouseClick,Left
67     Return 1
68   }
69   Return 0
70 }
71 ; Search from image and pick up sth. And stay current (etha + 2)
72 Find_Img_Stay(st_x,st_y,fi_x,fi_y,img_name){
73   imageSearch,ax,ay,st_x,st_y,fi_x,fi_y,*50 %img_name%
74   IF (ErrorLevel==0) {
75     MouseMove,ax+2,ay+2,0
76     MouseClick,Left
77     Return 1
78   }
79   Return 0
80 }
81 ; Search from image and pick up sth. And stay current (etha +10)
82 Find_Img_Stay2(st_x,st_y,fi_x,fi_y,img_name){
83   imageSearch,ax,ay,st_x,st_y,fi_x,fi_y,*50 %img_name%
84   IF (ErrorLevel==0) {
85     MouseMove,ax+10,ay+10,0
86     MouseClick,Left
87     Return 1
88   }
89   Return 0
90 }
91 }
92
93 Move_And_Click(x,y){
94   mousemove,x,y,0
  
```

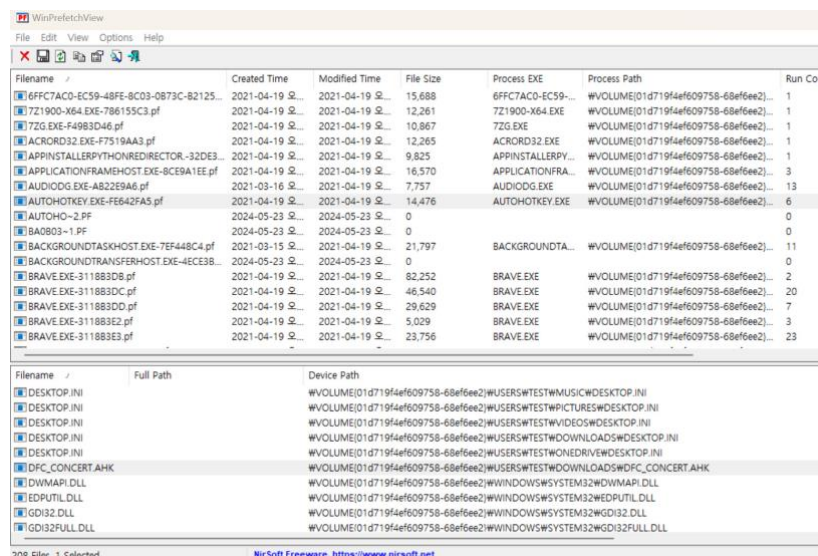
[그림 4] dfc_concert.ahk 파일 내부 2

간략하게 나타내자면, 지정된 페이지를 연 뒤 이미지를 찾아서 이를 클릭하는 프로그램이다. 이 프로그램이 범인이 사용한 매크로 파일일 것이다. 또한 ahk 파일은 Autohotkey 프로그램 파일의 확장자이다. 의심 파일이 Autohotkey setup 이 있는 것으로 보아 범인은 이 파일을 사용한 것으로 확정지을 수 있다. 또한 MacroRecorder를 통해서도 열 수 있다. 마찬가지로 MacroRecorder setup 또한 확인할 수 있겠다.

다음 문제를 살펴보자.

2. 암호상이 티켓팅에 사용한 프로그램은?

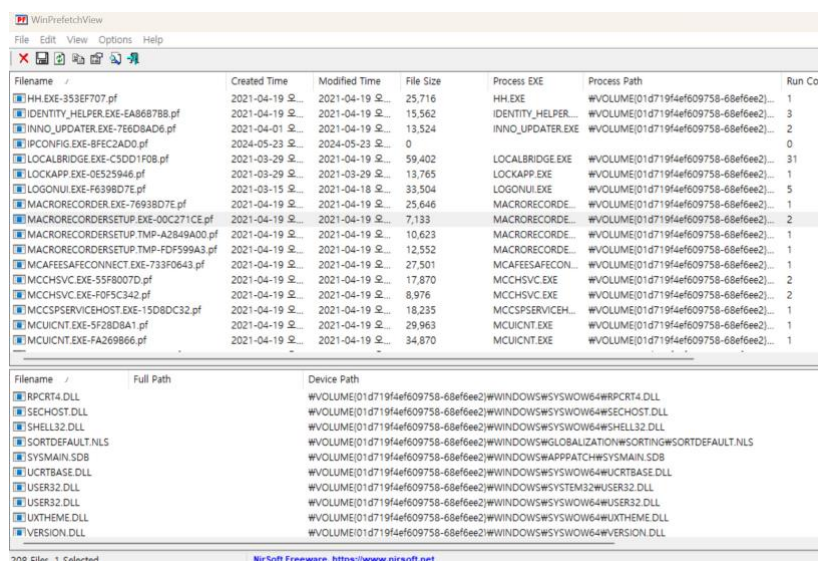
이를 확인하려면 범인이 사용한 파일인 dfc_concert.을 연 프로그램을 찾으면 된다. 추정을 하자면 1 번에서 확인했듯이 Autohotkey 를 통해서 열었을 확률이 있고, MacroRecorder 을 통해서 열었을 확률이 있다. 이를 확인하기 위해서 프리패치를 조사할 수 있는데, WinPrefetch 란 툴을 통해서 어떤 프로그램이 몇시에 어떤 파일을 몇번 연지 등등의 로그가 들어있는 프리패치 파일을 조사할 수 있다. **Image.ad1 에서도 프리패치 파일이 들어있는 Prefetch 폴더를 추출하여 WinPrefetch 를 통하여 조사할 수 있다. 여기서 Autohotkey 와 MacroRecorder 가 어떤 파일들을 실행시켰는지 조사하여 dfc_cocert 를 실행시킨 이력이 있는지 확인하면 되겠다.**



Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Count
6FFC7AC0-EC59-48FE-8C03-0873C-B2125...	2021-04-19 0...	2021-04-19 0...	15,688	6FFC7AC0-EC59...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
721900-X64.EXE-786155C3.pf	2021-04-19 0...	2021-04-19 0...	12,261	721900-X64.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
7ZG.EXE-F4983D46.pf	2021-04-19 0...	2021-04-19 0...	10,867	7ZG.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
ACRORD32.EXE-F7519AA3.pf	2021-04-19 0...	2021-04-19 0...	12,265	ACRORD32.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
APPINSTALLER\PYTHONREDIRECTOR-320E3...	2021-04-19 0...	2021-04-19 0...	9,825	APPINSTALLERPY...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
APPLICATIONFRAMEWORK\HOST.EXE-BC9A1EE.pf	2021-04-19 0...	2021-04-19 0...	16,570	APPLICATIONFRA...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	3
AUDIODG.EXE-AB223E94.pf	2021-03-16 0...	2021-04-19 0...	7,757	AUDIODG.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	13
AUTOHOTKEY.EXE-F642FA5.pf	2021-04-19 0...	2021-04-19 0...	14,476	AUTOHOTKEY.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	6
AUTOHO-2.PF	2024-05-23 0...	2024-05-23 0...	0			0
BA0B03-1.PF	2024-05-23 0...	2024-05-23 0...	0			0
BACKGROUND\TASKHOST.EXE-7F448C4.pf	2021-03-15 0...	2021-04-19 0...	21,797	BACKGROUND.TA...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	11
BACKGROUND\TRANSFER\HOST.EXE-4ECE3B...	2024-05-23 0...	2024-05-23 0...	0			0
BRAVE.EXE-311883D8.pf	2021-04-19 0...	2021-04-19 0...	82,252	BRAVE.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	2
BRAVE.EXE-311883DC.pf	2021-04-19 0...	2021-04-19 0...	46,540	BRAVE.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	20
BRAVE.EXE-311883DD.pf	2021-04-19 0...	2021-04-19 0...	29,629	BRAVE.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	7
BRAVE.EXE-311883E2.pf	2021-04-19 0...	2021-04-19 0...	5,029	BRAVE.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	3
BRAVE.EXE-311883E3.pf	2021-04-19 0...	2021-04-19 0...	23,756	BRAVE.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	23

Filename	Full Path	Device Path
DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}\USERS\WTEST\MUSIC\DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}...
DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}\USERS\WTEST\PICTURES\DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}...
DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}\USERS\WTEST\VIDEOS\DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}...
DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}\USERS\WTEST\DOWNLOADS\DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}...
DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}\USERS\WTEST\WONDRIVE\DESKTOP.INI	W:\VOLUME{01d7194ef609758-68ef6ee2}...
DFC_CONCERT.AHK	W:\VOLUME{01d7194ef609758-68ef6ee2}\USERS\WTEST\DOWNLOADS\DFC_CONCERT.AHK	W:\VOLUME{01d7194ef609758-68ef6ee2}...
DWMAPI.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\WDMAPI.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
EDPUTIL.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\EDPUTIL.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
GD32.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\GD32.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
GD32FULL.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\GD32FULL.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...

[그림 5] AUTOHOTKEY.EXE 프리패치 조사



Filename	Created Time	Modified Time	File Size	Process EXE	Process Path	Run Count
HH.EXE-353EF707.pf	2021-04-19 0...	2021-04-19 0...	25,716	HH.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
IDENTITY_HELPER.EXE-EA86878B.pf	2021-04-19 0...	2021-04-19 0...	15,562	IDENTITY_HELPER...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	3
INNO_UPDATER.EXE-7E6D8AD6.pf	2021-04-01 0...	2021-04-19 0...	13,524	INNO_UPDATER.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	2
IPCONFIG.EXE-8FEC2ADD.pf	2024-05-23 0...	2024-05-23 0...	0			0
LOCALBRIDGE.EXE-CS0D1F0B.pf	2021-03-29 0...	2021-04-19 0...	59,402	LOCALBRIDGE.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	31
LOCKAPP.EXE-0E325946.pf	2021-03-29 0...	2021-03-29 0...	13,765	LOCKAPP.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
LOGONUI.EXE-F6398D7E.pf	2021-03-15 0...	2021-04-18 0...	33,504	LOGONUI.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	5
MACRORECORDER.EXE-7693BD7E.pf	2021-04-19 0...	2021-04-19 0...	25,646	MACRORECORDER...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
MACRORECORDER\SETUP.EXE-00C271CE.pf	2021-04-19 0...	2021-04-19 0...	7,133	MACRORECORDER...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	2
MACRORECORDER\SETUP.TMP-A2849A00.pf	2021-04-19 0...	2021-04-19 0...	10,623	MACRORECORDER...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
MACRORECORDER\SETUP.TMP-FD599A3.pf	2021-04-19 0...	2021-04-19 0...	12,552	MACRORECORDER...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
MCAFEE\SAFECONNECT.EXE-733F0643.pf	2021-04-19 0...	2021-04-19 0...	27,501	MCAFEE\SAFECON...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
MCCHSVX.EXE-5F8007D.pf	2021-04-19 0...	2021-04-19 0...	17,870	MCCHSVX.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	2
MCCHSVX.EXE-F0F8C342.pf	2021-04-19 0...	2021-04-19 0...	8,976	MCCHSVX.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	2
MCCSPSERVICE\HOST.EXE-15D8DC32.pf	2021-04-19 0...	2021-04-19 0...	18,235	MCCSPSERVICE...	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
MCUCINT.EXE-5F28DBA1.pf	2021-04-19 0...	2021-04-19 0...	29,963	MCUCINT.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1
MCUCINT.EXE-FA26966.pf	2021-04-19 0...	2021-04-19 0...	34,870	MCUCINT.EXE	W:\VOLUME{01d7194ef609758-68ef6ee2}...	1

Filename	Full Path	Device Path
RPCRT4.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\RPCRT4.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
SECHOST.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\SECHOST.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
SHELL32.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\SHELL32.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
SORTDEFAULT.NLS	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\GLOBALIZATION\SORTDEFAULT.NLS	W:\VOLUME{01d7194ef609758-68ef6ee2}...
SYSDMMAIN.SDB	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\APPATCH\SYSDMMAIN.SDB	W:\VOLUME{01d7194ef609758-68ef6ee2}...
UCRTBASE.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\UCRTBASE.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
USER32.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\USER32.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
USER32.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\USER32.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
UXTHEME.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\UXTHEME.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...
VERSION.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}\WINDOWS\SYSTEM32\VERSION.DLL	W:\VOLUME{01d7194ef609758-68ef6ee2}...

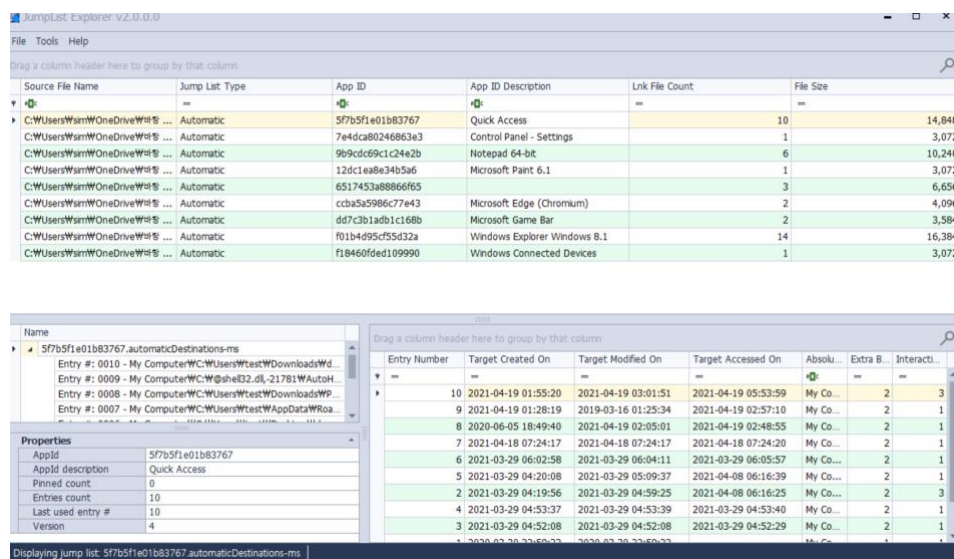
[그림 6] MACRORECORDER.EXE 프리패치 조사

[WHS-2] .iso

AUTOHOTKEY 가 실행한 파일에서 사진의 하이라이트를 보면 DFC_CONCENT.AHK 파일을 실행 것을 볼 수 있다. 따라서 **사용한 프로그램은 AutoHotKey 이다.**

3. 암호상이 매크로 파일을 편집하기 위해 사용한 프로그램은?

다음 문제를 풀이하기 위하여 풀이자가 분석할 수 있는 파일은 점프리스트 파일의 내용을 분석할 수 있다. 점프리스트 파일은 응용 프로그램을 사용할 때 남는 로그를 저장하는 파일이다. 점프리스트에서 어떤 파일로 통하여 매크로 파일을 열었는지 확인할 수 있다. **그 말은 즉, 해당 프로그램을 통하여 매크로 파일을 편집하였다는 말이 된다.**

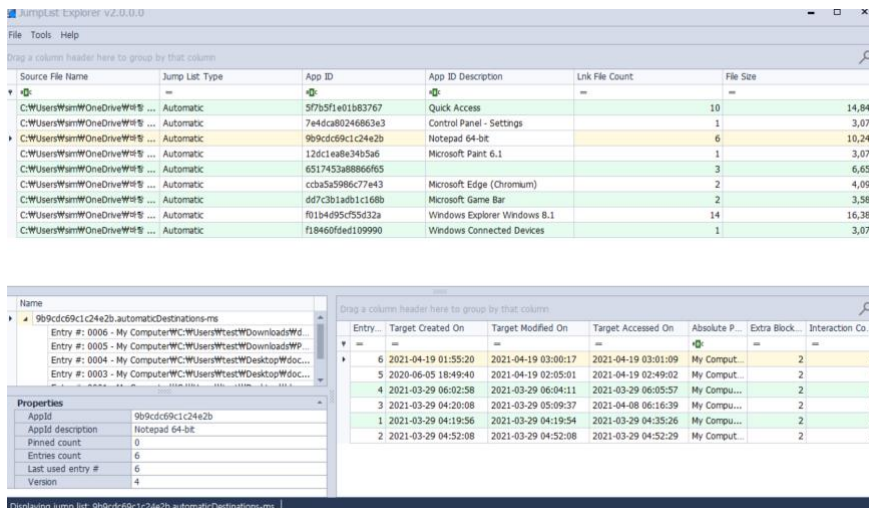


Source File Name	Jump List Type	App ID	App ID Description	Lnk File Count	File Size
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	5f7b5f1e01b83767	Quick Access	10	14,848
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	7e4dca80246863e3	Control Panel - Settings	1	3,072
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	9b9dc69c1c24e2b	Notepad 64-bit	6	10,240
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	12d1eae34b5a6	Microsoft Paint 6.1	1	3,072
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	6517453a8866f65	Microsoft Edge (Chromium)	3	6,656
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	cba3a5986c77e43	Microsoft Game Bar	2	4,096
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	dd7c3b1ad01c168b	Windows Explorer Windows 8.1	2	3,584
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	f01b4695c55d32a	Windows Connected Devices	14	16,384
C:\Users\Wsm\OneDrive\... \Automatic	Automatic	f18460fed109990		1	3,072

Name	Entry #	Target	Created On	Modified On	Accessed On	Absolu...	Extra B...	Interacti...
5f7b5f1e01b83767.automaticDestinations-ms	0010	My Computer\W\Users\Wsm\Downloads\Wd...	2021-04-19 01:55:20	2021-04-19 03:01:51	2021-04-19 05:53:59	My Co...	2	3
	0009	My Computer\W\Users\Wsm\Downloads\Wd...	2021-04-19 01:55:20	2021-04-19 03:01:51	2021-04-19 05:53:59	My Co...	2	3
	0008	My Computer\W\Users\Wsm\Downloads\Wd...	2021-04-19 01:55:20	2021-04-19 03:01:51	2021-04-19 05:53:59	My Co...	2	3
	0007	My Computer\W\Users\Wsm\Downloads\Wd...	2021-04-19 01:55:20	2021-04-19 03:01:51	2021-04-19 05:53:59	My Co...	2	3

[그림 7] Quick Access jump list 분석

먼저 확인할 수 있었던 것은 Quick Access 즉 바로가기에서 확인할 수 있었다. 주황색으로 하이라이트 되어있는 것이 매크로 파일을 실행하였던 기록이다. 바로가기 파일은 파일의 생성과 동시에 같이 생성되는 아이콘과 같다고 생각하면 된다. **하지만 여기서 수상한 점이 보인다. 수정 시각이 생성 시각과 다르다는 점이다. 매크로 파일의 내용이 수정되었기 때문에 바로가기 내용 또한 수정되었다고밖에 할 수가 없다.** 그렇다면 2021-04-19 03:01:51 주위에서 수정이 이루어졌을 것이다. 점프리스트에 찍히는 파일을 수정할만한 프로그램을 찾아보면 되겠다.



Source File Name	Jump List Type	App ID	App ID Description	Link File Count	File Size
C:\Users\Wan\OneDrive\... Automatic	Automatic	5f7b5f1e01b83767	Quick Access	10	14,848
C:\Users\Wan\OneDrive\... Automatic	Automatic	7e4dc80246863e3	Control Panel - Settings	1	3,072
C:\Users\Wan\OneDrive\... Automatic	Automatic	9b9cde9c1c24e2b	Notepad 64-bit	6	10,240
C:\Users\Wan\OneDrive\... Automatic	Automatic	126c1e49e3405a6	Microsoft Paint 6.1	1	3,072
C:\Users\Wan\OneDrive\... Automatic	Automatic	6517433a8866f65	Microsoft Edge (Chromium)	3	6,656
C:\Users\Wan\OneDrive\... Automatic	Automatic	c3ba5a596c77e43	Microsoft Game Bar	2	4,096
C:\Users\Wan\OneDrive\... Automatic	Automatic	6d7c3b1a0b1c168b	Windows Explorer Windows 8.1	2	3,584
C:\Users\Wan\OneDrive\... Automatic	Automatic	f01b4d95c55d32a	Windows Connected Devices	14	16,384
C:\Users\Wan\OneDrive\... Automatic	Automatic	f18460f9ed109990	Windows Connected Devices	1	3,072

[그림 8] Notepad 64-bit jump list 분석

틀을 찾는다고 해도 점프리스트에 많은 내용이 담겨있지 않아 Notepad 즉, 메모장밖에 보이지 않았다. 그리고 역시나 Target Accessed On 항목에 2021-04-19 03:01:09 에 매크로 파일을 연 것으로 보인다. 이 정보들을 정리를 하자면,

2021-04-19 01:55:20 -> target(dfcc_conert) 파일 생성

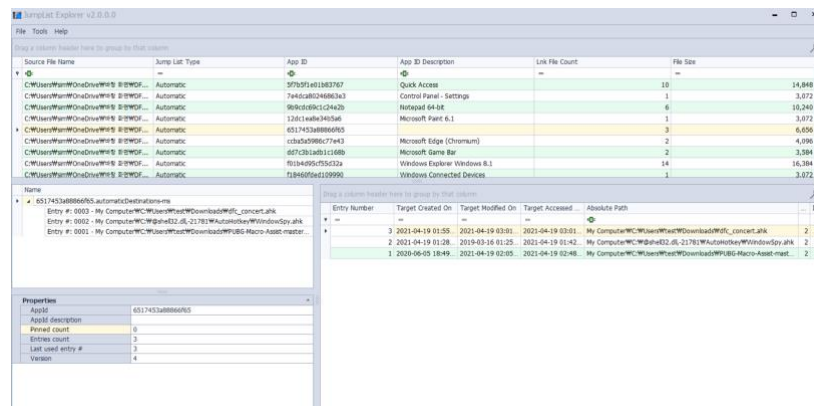
2021-04-18 03:01:09 -> Notepad(메모장)으로 target 파일 수정

2021-04-18 03:01:51 -> Quick Access 수정(범인이 수정을 마치고 저장함)

으로 나타낼 수 있다. 그렇다면 범인이 사용한 편집 프로그램은 Notepad(메모장)이 되겠다.

4. 암호상이 매크로를 실행한 시점은?

점프리스트 파일을 분석하던 중에 ID 가 나와있지 않았지만 AutoHotKey 프로그램인 것으로 의심되는 파일이 검출되었다.



Source File Name	Jump List Type	App ID	App ID Description	Link File Count	File Size
C:\Users\Wan\OneDrive\... Automatic	Automatic	5f7b5f1e01b83767	Quick Access	10	14,848
C:\Users\Wan\OneDrive\... Automatic	Automatic	7e4dc80246863e3	Control Panel - Settings	1	3,072
C:\Users\Wan\OneDrive\... Automatic	Automatic	9b9cde9c1c24e2b	Notepad 64-bit	6	10,240
C:\Users\Wan\OneDrive\... Automatic	Automatic	126c1e49e3405a6	Microsoft Paint 6.1	1	3,072
C:\Users\Wan\OneDrive\... Automatic	Automatic	6517433a8866f65	Microsoft Edge (Chromium)	3	6,656
C:\Users\Wan\OneDrive\... Automatic	Automatic	c3ba5a596c77e43	Microsoft Game Bar	2	4,096
C:\Users\Wan\OneDrive\... Automatic	Automatic	6d7c3b1a0b1c168b	Windows Explorer Windows 8.1	2	3,584
C:\Users\Wan\OneDrive\... Automatic	Automatic	f01b4d95c55d32a	Windows Connected Devices	14	16,384
C:\Users\Wan\OneDrive\... Automatic	Automatic	f18460f9ed109990	Windows Connected Devices	1	3,072

[그림 9] No-Name jump list 분석

매크로 프로그램에 연결한 프로그램은 바로가기, 메모장, No-Name(해당 프로그램) 3개였다. 생성하는 즉시 바로가기가 생겼을 것이고, 메모장은 편집은 가능하나 해당 매크로 프로그램을 실행시킬 순 없다. 그렇다면 이 매크로 프로그램을 실행시킬 수 있는 프로그램은 이 No-Name 프로그램이고, 2번 문항에 정답에 의거하여 이 프로그램은 AutoHotKey 프로그램일 것이다. 그렇다면 사용 툴인 Jumplist Explorer의 기능을 사용하여 해당 프로그램을 실행시킨 시간을 알 수 있다.

JmpLst Explorer v2.0.0.0

File Tools Help

Drag a column header here to group by that column

Source File Name	Jump List Type	App ID	App ID Description	Link File Count	File Size
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	9f7d5f1e01b83767	Quick Access	10	14,848
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	74dc4bc024686a3	Control Panel - Settings	1	3,072
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	96dc0c69c1c24e20	Notepad 64-bit	6	10,240
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	12dc1ea8e34b5a6	Microsoft Paint 6.1	1	3,072
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	6517453a88666f65		3	6,656
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	cbsa5a996c7e43	Microsoft Edge (Chromium)	2	4,096
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	d3bd13db1c16bb	Microsoft Game Bar	2	3,584
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	f01b4695c5c32a	Windows Explorer Windows 8.1	14	16,384
C:\Users\Wan\OneDrive\Work\Documents\Wdfc_concert_ahk	Automatic	f18460fed109990	Windows Connected Devices	1	3,072

Name

- 6517453a88666f65.automaticDestinations.ms
 - Entry #: 0003 - My Computer\WC:\Users\Wan\Downloads\Wdfc_concert_ahk
 - Entry #: 0002 - My Computer\WC:\Users\Wan\Downloads\Wdfc_concert_ahk
 - Entry #: 0001 - My Computer\WC:\Users\Wan\Downloads\Wdfc_concert_ahk

Properties

Entry number: 3

Path: C:\Users\Wan\Downloads\Wdfc_concert_ahk

Host name: desktop-6djhjs

Destination created on: 2021-04-19 01:25:41

Destination last modified: 2021-04-19 05:53:59

MAC address: 94-e6-f7-28-25-c3

TargetCreationDate: 2021-04-19 01:55:20

TargetModificationDate: 2021-04-19 03:01:51

TargetLastAccessedDate: 2021-04-19 03:01:51

Header.DataTags: HasTargetUrl, HasLinkInfo, IsUnicode, DisableKnownFolderTracing, AllowLinkT...

Header.FileAttributes: FileAttributeArchive

Header.FileSize: 7,642

Header.IconIndex: 0

Header.ShowWindow: Siformal

Absolute path: My Computer\WC:\Users\Wan\Downloads\Wdfc_concert_ahk

Local path: C:\Users\Wan\Downloads\Wdfc_concert_ahk

LocationFlags: VolumeIsAndLocalBasePath

[그림 10] AutoHotKey 프로그램 분석

연결시간과 수정시간이 다르면 문제가 있겠지만 다행히 시간이 같았다. **범인이 실행을 위해서 매 크로 프로그램을 AutoHotKey를 통하여 2021-04-19 03:01:51에 실행시켰음을 확인할 수 있다.**

5. 암호상이 매크로를 실행하기 위해 사용한 웹 브라우저는 무엇입니까?

간단하게 암호를 티켓팅 하기 위한 상황을 시뮬레이션 해보자. 먼저, 완성된 매크로 프로그램을 실행시킬 것이다. (2021-04-19 03:01:51) 그리고 웹 브라우저를 통하여 불법적으로 티켓팅을 진행하는 것이 순서이다. 그렇다면 타임라인에는 AuoHotKey가 실행되고 다음으로 웹 브라우저의 기록이 남을 것이다. 타임라인의 시간은 타임스탬프 형식이기 때문에 프로그램을 실행한 시간을 타임스탬프 시간으로 변환하면 1618813111이다. 이를 먼저 찾아보자.

[illegible]

[그림 11] 타임라인 분석 1

[WHS-2] .iso

역시나 빨간색 하이라이트 부분에 AutoHotKey를 실행시킨 흔적이 있다. 이제 타임라인을 따라가며 어떤 브라우저를 사용하였는지 찾아보자.

"application": "16080037-64FD-448-19E57-37FC02000000\\WindowsExplorer\\WindowsExplorer.exe", "platform": "windows_win32", "appid": "win32m-EC32AF_5_1", "BLOB Dat...	16080034_3621393504_BLOB Dat_1...	getGisC...	01680010
"application": "16080037-64FD-448-19E57-37FC02000000\\WindowsExplorer\\WindowsExplorer.exe", "platform": "windows_win32", "appid": "win32m-EC32AF_5_1", "BLOB Dat...	16080034_3621393504_BLOB Dat_1...	getGisC...	01680010
"application": "1AC4E77-02E7-45D0-6147-2E61A5E19879\\WinHttpd.exe", "platform": "windows_win32", "application": "D65383B_61u5uHY_...", "BLOB Dat...	16080034_3621393504_BLOB Dat_1...	getGisC...	01680010
"application": "Microsoft Windows Explorer", "platform": "windows_win32", "application": "Microsoft Windows Explorer", "platform": "win32m-EC32AF_5_1", "BLOB Dat...	160800427_1621395427_BLOB Dat_3...	getGisC...	01680014
"application": "16080037-64FD-448-19E57-37FC02000000\\WindowsExplorer\\WindowsExplorer.exe", "platform": "windows_win32", "application": "U3bnkag_...", "BLOB Dat...	16080034_3621393504_BLOB Dat_1...	getGisC...	01680010
"application": "Microsoft Windows Explorer", "platform": "windows_win32", "application": "Microsoft Windows Explorer", "platform": "win32m-EC32AF_5_1", "BLOB Dat...	1608001535_1621403670_BLOB Dat_3...	getGisC...	01680015
"application": "Microsoft Windows Explorer", "platform": "windows_win32", "application": "Microsoft Windows Explorer", "platform": "win32m-EC32AF_5_1", "BLOB Dat...	1608001537_1621403587_BLOB Dat_3...	getGisC...	01680015
"application": "Brave", "platform": "windows_win32", "application": "package1", "platform": "win32m-EC32AF_5_1", "BLOB Dat...	1608001622_1621403022_BLOB Dat_3...	getGisC...	01680016
"application": "Brave", "platform": "windows_win32", "application": "package1", "platform": "win32m-EC32AF_5_1", "BLOB Dat...	1608001623_1621404123_BLOB Dat_3...	getGisC...	01680016
"application": "Brave", "platform": "windows_win32", "application": "package1", "platform": "win32m-EC32AF_5_1", "BLOB Dat...	1608001629_1621404123_BLOB Dat_3...	getGisC...	01680016

[그림 12] 타임라인 분석 2

다음과 같이 범인은 Brave 브라우저를 사용하여 불법적으로 티켓팅을 진행하였음을 확인할 수 있다.

6. Flag

1. dfc_concert.ahk
2. AutoHotKey
3. Notepad
4. 2021-04-19 03:01:51
5. Brave 브라우저

7. 별도 첨부

문제 원본:

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.)

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)

번역본:

image.ad1 은 가상 시스템의 이미지 파일입니다

암표상의 노트북, 암표상이 만든 모든 파일은

티켓팅은 다운로드 폴더에 저장됩니다. 다음에 답하세요

이미지에 저장된 법의학 유물을 분석하여 질문합니다. (참고로

당신의 판단 근거가 상세해야 합니다.)

1. 암표상이 발권에 사용한 매크로 파일은 무엇입니까? (25 포인트)
2. 암표상이 티켓팅을 위해 사용한 프로그램은? (25 포인트)
3. 암표상이 매크로 파일을 편집하기 위해 사용한 프로그램은? (125 포인트)
4. 암표상이 매크로를 실행한 시점은? (50 점)
5. 암표상이 매크로를 실행하기 위해 사용한 웹 브라우저는 무엇입니까? (75 점)

8. Reference

- <https://dotaky99.tistory.com/9>
- <https://whitesnake1004.tistory.com/597>
- <http://forensic-proof.com/archives/3779>