



작성자	김서영
분석 일자	2024.05.22.~
작성 일자	2024.05.22.~2024.05.23.
분석 대상	KimPC_64GB_NVME.E01
문서 버전	1.0
작성자 E-mail	sykim1802@naver.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3

4. Write-Up.....4

5. Flag.....9

6. 별도 첨부 10

7. Reference 11

1. 문제

URL	
문제 내용	<p>Kim was using a password management tool recommended by an Information Security Specialist. One day, Kim found out through an email that account was stolen. Kim asked a Digital Forensics Specialist to analyze Kim's PC. Analyze Kim's PC to determine the cause.</p> <ol style="list-style-type: none"> 1) What is the name and version of the password management tool that Kim used? (20 points) 2) Submit SHA1 of the malware used in the attack. (30 points) 3) How many PCs were attacked in total? (50 points) 4) What is the ID and password that Kim saved using the password management tool? (150 points)
문제 파일	
문제 유형	Disk forensics
난이도	2 / 3

2. 분석 도구

도구명	다운로드 링크	Version
HxD	HxD - Freeware Hex Editor and Disk Editor mh-nexus	2.5.0.0
Autopsy	Autopsy - Download	4.21.0
PEstudio	Winitor	9.58

3. 환경

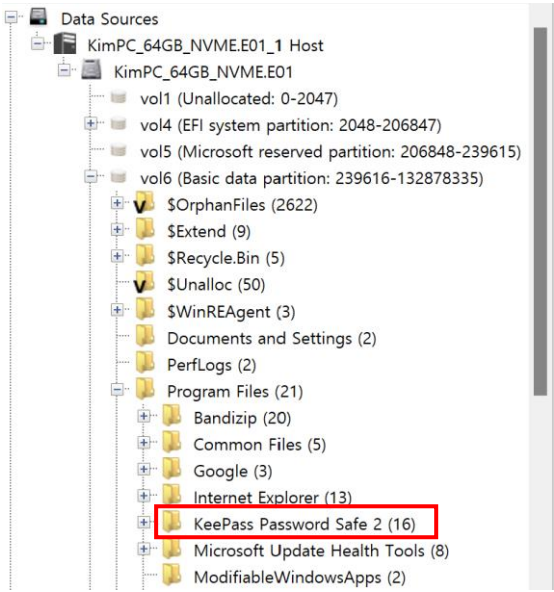
OS
Windows11 x64

4. Write-Up

파일명	KimPC_64GB_NVME.E01
용량	10,174,316kb
SHA256	b549bbe59c7c1f5d36651787240402305fe3a944593b2db8f78cda9c6679fa48
Timestamp	2023-07-12 15:54:56

1. 비밀번호 관리 프로그램

먼저 Autopsy로 열고, 프로그램 파일들 목록을 살펴보았다.



[사진 1] Directory tree로 확인한 프로그램 파일 목록

[사진 1]에서 KeePass Password Safe 2를 찾았다. 이름부터 대놓고 비밀번호 관리 프로그램으로 보였다. 이 프로그램을 다운로드 받았다면 기록이 남아있을 것이라고 생각하여 Web History를 열어 보았다.

Web History									
66 Results									
Source Na...	S	C	O	URL	Date Accessed	Referrer URL	Title	Program Name	Domain
History	1			https://www.google.com/search...	2023-05-26 15:05...	https://www.google.com/search?	비밀번호 관리 프로그램 - Google 검색	Google Chrome	google
History	1			https://www.google.com/search...	2023-05-26 15:05...	https://www.google.com/search?	비밀번호 관리 프로그램 - Google 검색	Google Chrome	google
History	1			https://namu.wiki/w/KeePass	2023-05-26 15:05...	https://namu.wiki/w/KeePass	KeePass - 나무위키	Google Chrome	namu.v
History	1			https://namu.wiki/w/KeePass	2023-05-26 15:05...	https://namu.wiki/w/KeePass	KeePass - 나무위키	Google Chrome	namu.v
History	1			https://www.google.com/search...	2023-05-26 15:06...	https://www.google.com/search?	keepass - Google 검색	Google Chrome	google
History	1			https://www.google.com/search...	2023-05-26 15:06...	https://www.google.com/search?	keepass - Google 검색	Google Chrome	google
History	1			https://www.google.com/search...	2023-05-26 15:06...	https://www.google.com/search?	keepass - Google 검색	Google Chrome	google
History	1			https://www.google.com/search...	2023-05-26 15:06...	https://www.google.com/search?	keepass - Google 검색	Google Chrome	google
History	1			https://keepass.info/	2023-05-26 15:08...	https://keepass.info/	KeePass Password Safe	Google Chrome	keepas
History	1			https://keepass.info/news/n230...	2023-05-26 15:08...	https://keepass.info/news/n2301...	KeePass 2.53 released - KeePass	Google Chrome	keepas
History	1			https://keepass.info/download.h...	2023-05-26 15:09...	https://keepass.info/download.htm	Downloads - KeePass	Google Chrome	keepas
History	1			https://sourceforge.net/projects...	2023-05-26 15:09...	https://sourceforge.net/projects/...	Download KeePass-2.53.1-Setup.exe (K...	Google Chrome	sourcef
History	1			https://sourceforge.net/projects...	2023-05-26 15:09...	https://sourceforge.net/projects/...	find out more about KeePass Sourcef...	Google Chrome	sourcef
History	1			https://sourceforge.net/projects...	2023-05-26 15:09...	https://sourceforge.net/projects/...	KeePass download SourceForge.net	Google Chrome	sourcef

[사진 2] Web history

[WHS-2] .iso

Web Downloads						
Table Thumbnail Summary						
Save Table as						
Source Name	S	C	...	Path	URL	△ Date Accessed
History		1		C:\Users\ppp\Downloads\ChromeSetup.exe	https://dl.google.com/tag/s/appguid%3D%7B8A69...	2023-05-22 13:50:54 KST
History		1		C:\Users\ppp\Downloads\BANDIZIP-SETUP-STD-X64.EXE	https://kr.bandisoft.com/bandizip/dl.php?web	2023-05-22 13:50:57 KST
History		1		C:\Users\ppp\Downloads\BANDIZIP-SETUP-STD-X64.EXE	https://dl.bandisoft.com/bandizip.std/BANDIZIP-SET...	2023-05-22 13:50:57 KST
History		1		C:\Users\ppp\Downloads\KeePass-2.53.1-Setup.exe	https://downloads.sourceforge.net/project/keepass/...	2023-05-26 15:09:08 KST
History		1		C:\Users\ppp\Downloads\KeePass-2.53.1-Setup.exe	https://jaist.dl.sourceforge.net/project/keepass/Kee...	2023-05-26 15:09:08 KST
History		1		C:\Users\ppp\Downloads\viewer.exe	https://blog.kakaocdn.net/dn/GqlhD/btshv1Cn43T/...	2023-05-26 16:11:07 KST

[사진 3] Web downloads

KeePass 프로그램 검색 기록과 다운로드 기록을 찾았다.

그런데 이름이 제각각이라 확실한 틀명을 알고자 Data Artifacts – Installed Programs 를 들어가 확인했다.

Installed Programs						
Table Thumbnail Summary						
Source Name	S	C	O	△ Program Name	Date/Time	Data Source
SOFTWARE			0	IEData	2022-05-07 05:27:59 KST	KimPC_64GB_NVME.E01
SOFTWARE			0	IEData	2022-05-07 05:27:59 KST	KimPC_64GB_NVME.E01
SOFTWARE			0	KeePass Password Safe 2.53.1 v.2.53.1	2023-05-26 06:09:36 KST	KimPC_64GB_NVME.E01
SOFTWARE			0	MPlayer2	2022-05-07 10:51:46 KST	KimPC_64GB_NVME.E01

[사진 4] Installed Programs 목록

정확한 이름은 KeePass Password Safe 이고, 버전이 2.53.1 이라는 것을 확인할 수 있다.

2. SHA1 of the malware used in the attack.

문제 내용에 따르면 비밀번호 관리자를 사용 중 비밀번호가 계정이 탈취됐다는 것을 알았으니 선 후관계가 KeePass 다운로드(선) – malware 다운로드(후) 로 추측할 수 있다.

따라서 [사진 3] 웹 다운로드 기록에서 KeePass 이후에 다운로드 된 프로그램 viewer.exe을 의심 해보았다.

Table Thumbnail Summary							
Name							
	S	C	O	Modified Time	Change Time	Access Time	Created Time
vmcompute.exe				2022-09-25 11:42:29 KST	2023-05-22 14:10:54 KST	2023-05-25 16:44:37 KST	2022-09-25 11:34:48 KST
vm3service.exe				2022-11-03 07:54:38 KST	2023-05-22 13:51:17 KST	2023-05-25 16:41:25 KST	2022-11-03 07:54:38 KST
vm3service.exe				2022-11-03 07:54:38 KST	2023-05-22 14:50:22 KST	2023-05-26 14:54:30 KST	2022-11-03 07:54:38 KST
vm3service.exe				2022-11-03 07:54:38 KST	2023-05-22 14:50:22 KST	2023-05-26 14:54:30 KST	2022-11-03 07:54:38 KST
vm3service.exe				2022-11-03 07:54:38 KST	2023-05-22 14:50:22 KST	2023-05-26 14:54:30 KST	2022-11-03 07:54:38 KST
viewer.exe				2023-05-26 16:11:14 KST	2023-05-26 16:11:45 KST	2023-05-26 16:12:58 KST	2023-05-26 16:11:07 KST
vfpctrl.exe				2023-05-03 09:23:32 KST	2023-05-22 14:09:40 KST	2023-05-25 16:45:17 KST	2023-05-22 14:05:09 KST

[사진 5] viewer.exe를 추출하기 위한 경로

[WHS-2] .iso

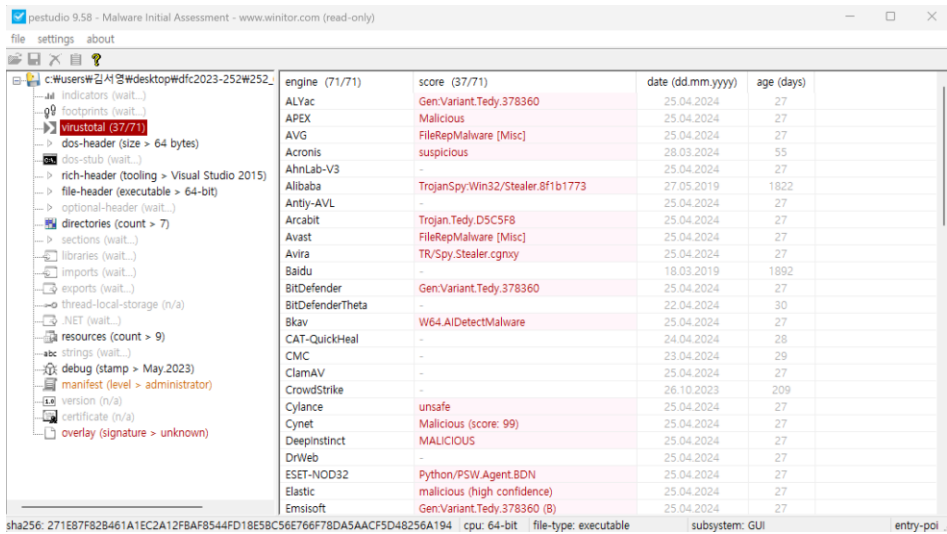
[사진 5]에서 Viewer.exe를 찾아 export하였다.



[사진 6] viewer.exe의 아이콘

아이콘을 보고 Viewer.exe는 python을 사용하여 만들어졌음을 알았다.

악성코드에 자주 사용되는 것들을 빨간색으로 표시해주고, 위험한 정도와 항목들을 알려주는 Pestudio를 사용하여 viewer.exe를 열어보았다.



engine (71/71)	score (37/71)	date (dd.mm.yyyy)	age (days)
ALYac	Gen.Variant.Tedy.378360	25.04.2024	27
APEX	Malicious	25.04.2024	27
AVG	FileRep/Malware [Misc]	25.04.2024	27
Acronis	suspicious	28.03.2024	55
AhnLab-V3	-	25.04.2024	27
Alibaba	Trojan.Spy.Win32/Stealer.8f1b1773	27.05.2019	1822
Antiy-AVL	-	25.04.2024	27
Arcabit	Trojan.Tedy.D5C5F8	25.04.2024	27
Avast	FileRep/Malware [Misc]	25.04.2024	27
Avira	TR/Spy.Stealer.cgnxy	25.04.2024	27
Baidu	-	18.03.2019	1892
BitDefender	Gen.Variant.Tedy.378360	25.04.2024	27
BitDefenderTheta	-	22.04.2024	30
Bkav	W64.AIDetect/Malware	25.04.2024	27
CAT-QuickHeal	-	24.04.2024	28
CMC	-	23.04.2024	29
ClamAV	-	25.04.2024	27
CrowdStrike	-	26.10.2023	209
Cylance	unsafe	25.04.2024	27
Cynet	Malicious (score: 99)	25.04.2024	27
Deepinfect	MALICIOUS	25.04.2024	27
DrWeb	-	25.04.2024	27
ESET-NOD32	Python/PSW.Agent.BDN	25.04.2024	27
Elastic	malicious (high confidence)	25.04.2024	27
Emsisoft	Gen.Variant.Tedy.378360 (B)	25.04.2024	27

[사진 7] Pestudio 결과창

굉장히 많은 빨간색과 위험도 score 로 malicious 를 받은 항목들이 많다는 것을 볼 수 있다. 이를 통해 viewer.exe 가 malware 라고 확신했다.

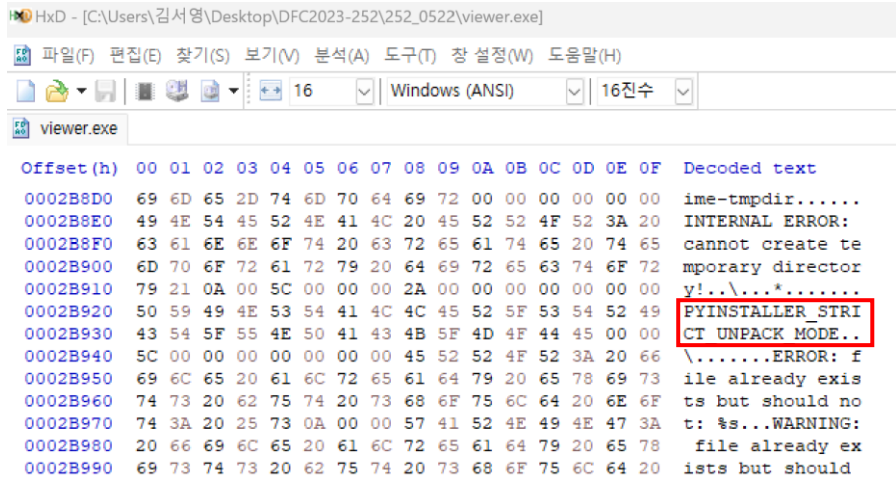
```
C:\Users\김서영\Desktop\DFC2023-252\252_0522>certutil -hashfile viewer.exe SHA1
SHA1의 viewer.exe 해시 :
fc8113603a8f611ddfd964ffefdec674f9f2367a
CertUtil: -hashfile 명령이 성공적으로 완료되었습니다.
```

[사진 8] viewer.exe의 SHA1 값

3. How many PCs were attacked in total?

Viewer.exe 를 HxD 로 열어보았다.

[WHS-2] .iso



[사진 9] HxD에서 보이는 String

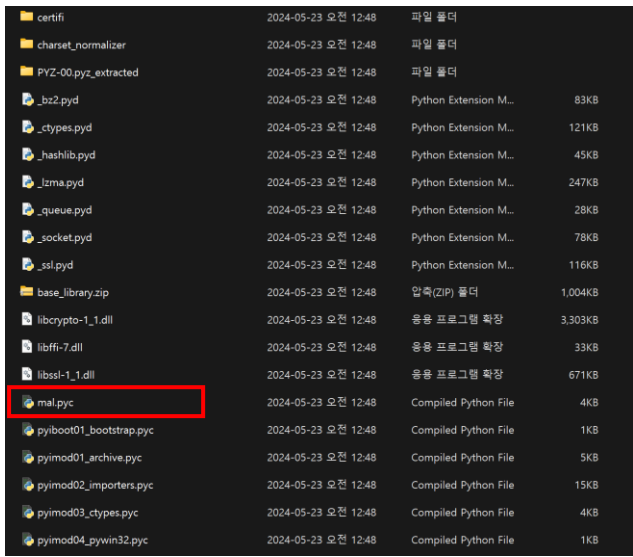
Pyinstaller로 exe파일이 만들어졌다는 것을 알 수 있었다.

따라서 PyInstaller Extractord 인 pyinstxtractor 를 다운 받아 viewer.exe 에 내장된 zip 파일과 pyc 파일들 등을 추출했다. ([extremecoders-re/pyinstxtractor: PyInstaller Extractor \(github.com\)](https://github.com/extremecoders-re/pyinstxtractor))

```
C:\Users\김서영\Desktop\DFC2023-252\252_0522>python pyinstxtractor.py viewer.exe
[+] Processing viewer.exe
[+] Pyinstaller version: 2.1+
[+] Python version: 3.8
[+] Length of package: 5758370 bytes
[+] Found 27 files in CArchive
[+] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap.pyc
[+] Possible entry point: mal.pyc
[!] Warning: This script is running in a different Python version than the one used to build the executable.
[!] Please run this script in Python 3.8 to prevent extraction errors during unmarshalling
[!] Skipping pyz extraction
[+] Successfully extracted pyinstaller archive: viewer.exe

You can now use a python decompiler on the pyc files within the extracted directory
```

[사진 10] pyinstxtractor로 viewer.exe 내장 파일 추출



[사진 11] 추출된 파일 목록(viewer.exe_extracted)

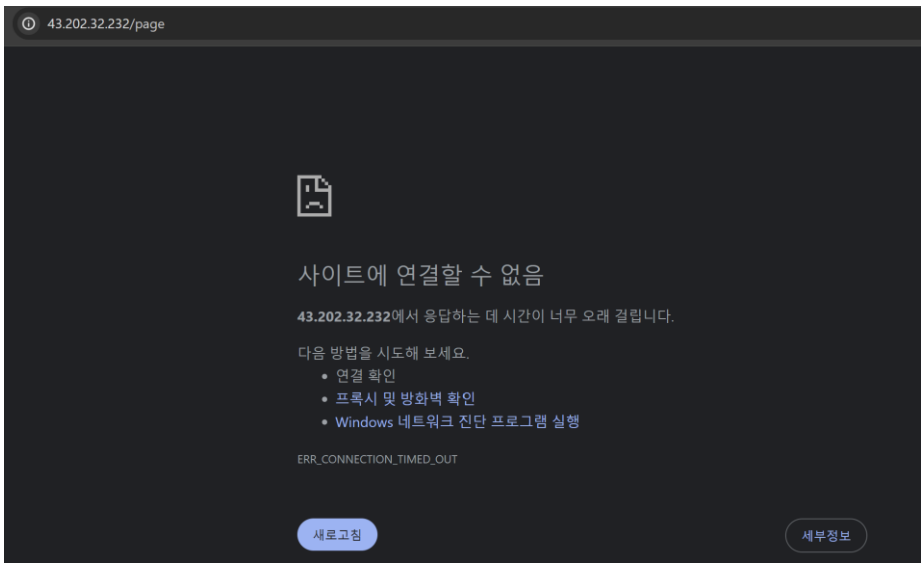
[WHS-2] .iso

[사진 11]에서 이름부터 수상한 mal.pyc 를 찾았다. HxD 로 열어보았다.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000B40	FA	01	7E	DA	09	44	6F	63	75	6D	65	6E	74	73	29	02	ú.~Ú.Documents).
00000B50	DA	03	6D	61	63	DA	09	6D	61	73	74	65	72	6B	65	79	Ú.macÚ.masterkey
00000B60	72	45	00	00	00	72	18	00	00	00	7A	19	68	74	74	70	rE...r....z.http
00000B70	3A	2F	2F	34	33	2E	32	30	32	2E	33	32	2E	32	33	32	://43.202.32.232
00000B80	2F	70	61	67	65	29	02	DA	05	66	69	6C	65	73	72	24	/page).Ú.filesr\$
00000B90	00	00	00	29	0A	72	19	00	00	00	72	10	00	00	00	72	...).r....r....r

[사진 12] mal.pyc 내 수상한 url링크

url 링크를 입력했지만 사이트가 열리지 않았다.



Mal.pyc 파일을 디컴파일하기 위해 디컴파일러를 다운받았지만, 현재 디컴파일이 되지 않아 5 시간 동안 시도 중이다...

5. Flag

1. KeePass Password Safe, 2.53.1
2. fc8113603a8f611ddfd964ffefdec674f9f2367a

6. 별도 첨부

7. Reference

-