

252 – Password Stealer

Team Information

Team Name _____

Team Member _____

Email Address _____

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:		Publisher:	
Version:			
URL:			

Step-by-step methodology:

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

(FTK Imager의 캡처가 정상 동작하지 않아 글로 대체한다.)

[KimPC_64GB_NVME.E01\Basic data partition (3)\NONAME\root\Users\wppp\Downloads]에 위치해 있는 KeePass-2.53.1-Setup.exe 파일을 발견했다.

[KimPC_64GB_NVME.E01\Basic data partition (3)\NONAME\root\Windows\Prefetch]에 위치해 있는 KEEPASS-2.53 1-SETUP.EXE와 KEEPASS-2.53 1-SETUP.TMP 파일을 발견했다.

구글링을 해 본 결과, KeePass password safe는 무료 오픈 소스 비밀번호 관리자이다.

KeePass 2.53.2

메모 포함[오전1]: Kim이 사용한 암호 관리 도구의 이름과 버전은 무엇입니까?

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

[KimPC_64GB_NVME.E01\Basic data partition (3)\NONAME\root\Users\wppp\Downloads] 위치에 있었던 파일들을 하나씩 export(우클릭-Export Files) 해보던 와중 viewer.exe파일을 윈도우 보안 시스템이 계속해서 삭제한다는 사실을 발견했다.

메모 포함[오전2]: 공격에 사용된 악성 코드의 SHA1을 제출하세요.

악성코드인지 파악하기 위해 Virustotal에 업로드하였다.

37/71 security vendors and no sandboxes flagged this file as malicious

271e87f82b461a1ec2a12fbaf8544fd18e5bc56e766f78da5aac5d48256a194

viewer.exe

Size: 5.80 MB | Last Modification Date: 1 month ago

Community Score: 37/71

peexe detect-debug-environment overlay checks-network-adapters 64bits

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label: trojan.tedy.stealer | Threat categories: trojan | Family labels: tedy, stealer, cgray

Security vendors' analysis

Vendor	Detection
Acronis (Static ML)	Suspicious
ALYac	Gen.Variant.Tedy.378360
Avast	FileRep.Malware [Misc]
Avira (no cloud)	TR/Spy.Stealer.cgray
Bkav Pro	W64.AIDetect.Malware
Cynet	Malicious (score: 99)
Elastic	Malicious (high Confidence)

악성코드로 판단하였다.

Basic properties

MD5: ecd1817d4967b8ae912e99d58e3736ae

SHA-1: fc8113603a8f611ddfd964ffefdec674f9f2367a

SHA-256: 271e87f82b461a1ec2a12fbaf8544fd18e5bc56e766f78da5aac5d48256a194

Vhash: 066076655d1555157550401330065mz11fr

Authentic hash: 7a187e02cf1b0a7de2640a5f3b0881ab94e61f3f07d1e0a397654fd42be99

Imp hash: 0b5552dcd9db834cea55c0c8fc05be

Rich PE header hash: fcbaaae938213136618c21de16e8605

SSDEP: 98304:ow9IFVQWJuhwoV5eQAVco0Ahd5y0Naxxv8lqDDAxNeRWH5yl_g6lGqXPGTqcuq:ofuWJysO5oyMxxvjDDAxhST2xy

TLSH: TJF756334596D00EDAF9B74039D9A09401D677B4230B05D88B43B4963A6F23F1AE7EFA1

File type: Win32 EXE (executable) | windows | win32 | pe | peexe

Magic: PE32+ executable (GUI) x86-64, for MS Windows

File size: 5.80 MB (6079906 bytes)

이 파일의 SHA-1은 **fc8113603a8f611ddfd964ffefdec674f9f2367a**이다.


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


```
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..
0002B940 5C 00 00 00 00 00 00 00 45 52 52 4F 52 3A 20 66 \.....ERROR: f
0002B950 69 6C 65 20 61 6C 72 65 61 64 79 20 65 78 69 73 ile already exis
```

메모 포함[오전3]: 총 몇 대의 PC가 공격을 받았습니
까?

viewer.exe 파일을 HXD로 살펴보면 PYINSTALLER라는 텍스트가 보인다.

이는 파이썬으로 작성된 py 파일이 아닐까 의심이 들어, pyinstxtractor라는 툴을 다운받았다.

 pyinstxtractor.py

 viewer.exe

기존의 파일과 툴을 같은 폴더에 위치시킨 후, cmd창을 켜준다.



























```
C:\Windows\System32\cmd
Microsoft Windows [Version 10.0.22631.3593]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HANNA\Desktop\pyinstaller>python pyinstxtractor.py viewer.exe
[*] Error: Could not open viewer.exe

C:\Users\HANNA\Desktop\pyinstaller>python pyinstxtractor.py viewer.exe
[*] Processing viewer.exe
[*] Pyinstaller version: 2.1+
[*] Python version: 308
[*] Length of package: 5758370 bytes
[*] Found 27 files in CArchive
[*] Beginning extraction...please standby
[+] Possible entry point: pyiboot01_bootstrap
[+] Possible entry point: mal
[!] Warning: The script is running in a different python version than the one used to build the executable
    Run this script in Python308 to prevent extraction errors(if any) during unmarshalling
[!] Unmarshalling FAILED. Cannot extract PYZ-00.pyz. Extracting remaining files.
[*] Successfully extracted pyinstaller archive: viewer.exe

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

python pyinstxtractor.py viewer.exe 라는 명령어를 입력하면 extracted된 폴더가 생긴다.

이름	수정된 날짜	유형	크기
 certifi	2024-06-06 오후 3:53	파일 폴더	
 charset_normalizer	2024-06-06 오후 3:53	파일 폴더	
 PYZ-00.pyz_extracted	2024-06-06 오후 3:53	파일 폴더	
 .bz2.pyd	2024-06-06 오후 3:53	Python Extension ...	83KB
 .ctypes.pyd	2024-06-06 오후 3:53	Python Extension ...	121KB
 .hashlib.pyd	2024-06-06 오후 3:53	Python Extension ...	45KB
 .lzma.pyd	2024-06-06 오후 3:53	Python Extension ...	247KB
 .queue.pyd	2024-06-06 오후 3:53	Python Extension ...	28KB
 .socket.pyd	2024-06-06 오후 3:53	Python Extension ...	78KB
 .ssl.pyd	2024-06-06 오후 3:53	Python Extension ...	116KB
 base_library.zip	2024-06-06 오후 3:53	압축(ZIP) 파일	1,004KB
 libcrypto-1_1.dll	2024-06-06 오후 3:53	응용 프로그램 확장	3,303KB
 libffi-7.dll	2024-06-06 오후 3:53	응용 프로그램 확장	33KB
 libssl-1_1.dll	2024-06-06 오후 3:53	응용 프로그램 확장	671KB
 mal	2024-06-06 오후 3:53	파일	4KB
 pyiboot01_bootstrap	2024-06-06 오후 3:53	파일	1KB
 pyimod01_archive	2024-06-06 오후 3:53	파일	5KB
 pyimod02_importers	2024-06-06 오후 3:53	파일	15KB
 pyimod03_ctypes	2024-06-06 오후 3:53	파일	4KB
 pyimod04_pywin32	2024-06-06 오후 3:53	파일	1KB
 python38.dll	2024-06-06 오후 3:53	응용 프로그램 확장	4,086KB
 PYZ-00.pyz	2024-06-06 오후 3:53	Python Zip Applic...	1,046KB
 select.pyd	2024-06-06 오후 3:53	Python Extension ...	27KB
 struct	2024-06-06 오후 3:53	파일	1KB
 unicodedata.pyd	2024-06-06 오후 3:53	Python Extension ...	1,071KB
 VCRUNTIME140.dll	2024-06-06 오후 3:53	응용 프로그램 확장	88KB

폴더를 살펴보다가 대부분이 파이썬 프로그램이거나, 확장자가 존재하는데 mal, struct는 유독 파일이 깨끗해 보여서 HXD로 열어보았다.

0x0	struct	mal															
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	E3	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	ã.....
00000010	00	08	00	00	00	40	00	00	00	73	38	00	00	00	64	00@...s8...d.
00000020	64	01	64	02	64	03	64	04	64	05	64	06	64	07	67	08	d.d.d.d.d.d.d.g.
00000030	5A	00	64	08	64	09	6C	01	54	00	64	08	64	0A	6C	01	Z.d.d.l.T.d.d.l.
00000040	6D	02	5A	02	01	00	64	08	64	0B	6C	01	6D	03	5A	03	m.Z...d.d.l.m.Z.
00000050	01	00	64	0C	53	00	29	0D	DA	08	63	61	6C	63	73	69	..d.S.).Û.calcsi
00000060	7A	65	DA	04	70	61	63	6B	DA	09	70	61	63	6B	5F	69	zeÛ.packÛ.pack_i
00000070	6E	74	6F	DA	06	75	6E	70	61	63	6B	DA	0B	75	6E	70	ntoÛ.unpackÛ.unp
00000080	61	63	6B	5F	66	72	6F	6D	DA	0B	69	74	65	72	5F	75	ack_fromÛ.iter_u
00000090	6E	70	61	63	6B	DA	06	53	74	72	75	63	74	DA	05	65	npackÛ.StructÛ.e
000000A0	72	72	6F	72	E9	00	00	00	00	29	01	DA	01	2A	29	01	rroré...).Û.*)).
000000B0	DA	0B	5F	63	6C	65	61	72	63	61	63	68	65	29	01	DA	Û.clearcache).Û
000000C0	07	5F	5F	64	6F	63	5F	5F	4E	29	04	DA	07	5F	5F	61	._doc_N).Û._a
000000D0	6C	6C	5F	5F	DA	07	5F	73	74	72	75	63	74	72	0B	00	ll_Û.structz..
000000E0	00	00	72	0C	00	00	00	A9	00	72	0F	00	00	00	72	0F	..r....@.r....r.
000000F0	00	00	00	7A	09	73	74	72	75	63	74	2E	70	79	DA	08	...z.struct.pyÛ.
00000100	3C	6D	6F	64	75	6C	65	3E	03	00	00	00	73	16	00	00	<module>....s...
00000110	00	02	00	02	00	02	00	02	00	02	01	02	03	02	03	02
00000120	F7	04	0C	08	01	0C	01										÷.....[]

struct에는 별다른 점이 없다.

Offset (h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000B10	09	64	06	7C	05	7C	02	64	07	8D	03	7D	06	57	00	35	.d. . .d...}.W.S
00000B20	00	51	00	52	00	58	00	71	2C	64	00	53	00	29	08	4E	.Q.R.X.q,d.S.) .N
00000B30	FA	01	7E	DA	09	44	6F	63	75	6D	65	6E	74	73	29	02	ú.~Ú.Documents).
00000B40	DA	03	6D	61	63	DA	09	6D	61	73	74	65	72	6B	65	79	Ű.macŰ.masterkey
00000B50	72	45	00	00	00	72	18	00	00	00	7A	19	68	74	74	70	rE...r...z.http
00000B60	8A	2F	2F	34	33	2E	32	30	32	2E	33	32	2E	32	33	32	://43.202.32.232
00000B70	2F	70	61	67	65	29	02	DA	05	66	69	6C	65	73	72	24	/page).Ű.filesr\$
00000B80	00	00	00	29	0A	72	19	00	00	00	72	10	00	00	00	72	...).r...r...r

mal 파일에는 <http://43.202.32.232/page> 라는 url이 있었다.



사이트에 연결할 수 없음

43.202.32.232에서 응답하는 데 시간이 너무 오래 걸립니다.

다음 방법을 시도해 보세요.

- 연결 확인
- 프록시 및 방화벽 확인
- Windows 네트워크 진단 프로그램 실행

ERR_CONNECTION_TIMED_OUT

상단의 url대로 접속해보았지만 연결이 불가능했다.

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

메모 포함[오전4]: Kim이 암호 관리 도구를 사용하여 저장한 ID와 암호는 무엇입니까?

The deadline for this problem is July 31.

Please do not post your write-up before the deadline for fair competition!

* Delete this box when submitting your answer.