



작성자	박혜미
분석 일자	2024.05.10
작성 일자	2024.05.10
분석 대상	MemoryDump(SuNiNaTaS)
문서 버전	2
작성자 E-mail	parkm0708@naver.com

0. 목차

1. 문제3

2. 분석 도구3

3. 환경3


4. Write-Up.....4

5. Flag.....8

6. 별도 첨부9

7. Reference 10

1. 문제

URL	http://suninatas.com/challenge/web30/web30.asp
문제 내용	<p>해커가 김장군의 PC에 침투한 흔적을 발견하였다. 사고 직후 김장군의 PC에서 획득한 메모리 덤프를 제공받은 당신은 해커가 한 행동을 밝혀내야한다.</p> <p>1. 김장군 PC의 IP 주소는? 2. 해커가 열람한 기밀문서의 파일명은? 3. 기밀문서의 주요 내용은? 내용속에 "Key"가 있다.</p> <p>인증키 형식 : lowercase(MD5(1번답+2번답+3번키))</p>
문제 파일	 MemoryDump(Su NiNaTaS).zip
문제 유형	메모리 포렌식
난이도	2 / 5

2. 분석 도구

도구명	다운로드 링크	Version
volatility	https://volatilityfoundation.org/	2.6

3. 환경

OS
Windows 11 Home

4. Write-Up

파일명	MemoryDump(SuNiNaTaS)
용량	1GB
SHA256	844d22a0481fd931d100a3e64721aa5852871dc47bde2e25c403bd1dd69edbbba
Timestamp	2024-05-10 18:00:47

메모리 덤프 파일을 분석하는 문제이기 때문에 volatility 도구를 사용한다.

```
C:\Users\LG\OneDrive\문서\화이트햇 2기\.iso 프로젝트\Write-Up\1w\SuNiNaTaS-30>volatility_2.6_win64_standalone.exe -f "MemoryDump(SuNiNaTaS)" imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
      Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x86, Win7SP1x86
                           AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                           AS Layer2 : FileAddressSpace (C:\Users\LG\OneDrive\문서\화이트햇 2기\.iso 프로젝트\Write-Up\1w\SuNiNaTaS-30\MemoryDump(SuNiNaTaS))
                           PAE type : PAE
                           DTB : 0x185000L
                           KDBG : 0x82f6cc28L
      Number of Processors : 1
      Image Type (Service Pack) : 1
                           KPCR for CPU 0 : 0x82f6dc00L
                           KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2016-05-24 09:47:40 UTC+0000
      Image local date and time : 2016-05-24 18:47:40 +0900
```

[그림 1] imageinfo

[volatility_2.6_win64_standalone.exe -f "MemoryDump(SuNiNaTaS)" imageinfo] 명령어를 사용하여 운영체제 정보를 확인한다. 운영체제는 [Win7SP1x86_23418], [Win7SP0x86], [Win7SP1x86]이다. 해당 명령어는 메모리 파일의 운영체제 profile 정보를 확인하는 명령어이며 사용 방법은 [volatility_2.6_win64_standalone.exe -f [파일명] imageinfo]이다. -f 로 파일을 선택하고 imageinfo 플러그인을 적용하겠다는 뜻이다.



[WHS-2] .iso

0x3de3e008	TCPv4	192.168.197.138:49174	23.49.155.27:80	CLOSED	-1	
0x3de61548	TCPv4	192.168.197.138:49247	113.29.189.142:80	ESTABLISHED	-1	
0x3e1e2008	TCPv4	192.168.197.138:49252	61.111.58.11:80	ESTABLISHED	-1	
0x3ee4f9e8	TCPv4	192.168.197.138:49173	23.43.5.163:80	CLOSED	-1	
0x3ee7d688	TCPv4	192.168.197.138:49163	211.233.62.122:80	ESTABLISHED	-1	
0x3ee7d910	TCPv4	192.168.197.138:49167	121.189.57.82:80	ESTABLISHED	-1	
0x3f26e5f0 2016-05-24 09:22:27 UTC+0000	UDPv4	192.168.197.138:138	*,*		4	System
0x3f270768 2016-05-24 09:22:27 UTC+0000	UDPv4	192.168.197.138:137	*,*		4	System
0x3f270450	TCPv4	192.168.197.138:139	0.0.0.0:0	LISTENING	4	System
0x3f430b70	TCPv4	192.168.197.138:49168	216.58.197.132:80	ESTABLISHED	-1	
0x3f7854b8	TCPv4	192.168.197.138:49164	211.233.62.122:80	ESTABLISHED	-1	
0x3f78bd68	TCPv4	192.168.197.138:49179	59.18.34.167:443	ESTABLISHED	-1	
0x3f7deb30	TCPv4	192.168.197.138:49184	114.108.157.50:80	ESTABLISHED	-1	
0x3fc5f998	TCPv4	192.168.197.138:49178	59.18.34.167:443	ESTABLISHED	-1	
0x3fc6d638	TCPv4	192.168.197.138:49172	172.217.25.67:443	ESTABLISHED	-1	
0x3fc77df8	TCPv4	192.168.197.138:49176	172.217.25.67:443	ESTABLISHED	-1	
0x3fc84348	TCPv4	192.168.197.138:49169	216.58.197.132:80	ESTABLISHED	-1	
0x3fc86008	TCPv4	192.168.197.138:49175	59.18.35.55:80	CLOSED	-1	
0x3fc8b5f0	TCPv4	192.168.197.138:49251	61.111.58.11:80	ESTABLISHED	-1	
0x3fc8d4a0	TCPv4	192.168.197.138:49177	172.217.25.67:443	ESTABLISHED	-1	
0x3fc90df8	TCPv4	192.168.197.138:49265	59.18.44.44:80	ESTABLISHED	-1	
0x3fc98738	TCPv4	192.168.197.138:49182	59.18.44.226:443	ESTABLISHED	-1	
0x3fc9fbe8	TCPv4	192.168.197.138:49181	59.18.44.226:443	ESTABLISHED	-1	
0x3fca8828	TCPv4	192.168.197.138:49180	59.18.35.55:80	CLOSED	-1	
0x3fcbbbb0	TCPv4	192.168.197.138:49237	180.70.93.13:80	CLOSED	-1	

[그림 2] netscan

IP 주소를 획득하기 위하여 nmap 플러그인을 사용한다. 사용한 명령어는

```
[volatility_2.6_win64_standalone.exe -f "MemoryDump(SuNiNaTaS)" --profile=Win7SP0x86 nmap]
```

이다. **김장군의 PC IP 는 192.168.197.138** 인 것을 확인할 수 있다. 해당 명령어는 네트워크 연결 정보를 확인할 수 있는 명령어이며 사용 방법은

```
[volatility_2.6_win64_standalone.exe -f [파일명] --profile=[운영체제] nmap]
```

이다.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Offset/P	#Ptr	#Hnd	Access Name																				
0	0x00000000	0xa0c6b	2	0 RW-rwd	Device\HarddiskVolume1\$Directory																		
4	0x00000000	0x3da4f90	8	0 R-rwd	Device\HarddiskVolume1\$ProgramData\Microsoft\Windows\Start Menu\Programs\Accessories\Math Input Panel\Ink																		
8	0x00000000	0x3da0768	4	0 R-rwd	Device\HarddiskVolume1\$Windows\System32\wraspl.dll																		
6	0x00000000	0x3da0c38	2	0 RW-rwd	Device\HarddiskVolume1\$Directory																		
10	0x00000000	0x3da0cb10	1	0 RW-rwd	Device\HarddiskVolume1\$PrepareToShrinkFileSice																		
8	0x00000000	0x3da0cb8	0	0 R-r-r-d	Device\HardiskVolume1\$Users\training\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5RW0A18HP\Folder_mkdir[1].gif																		
8	0x00000000	0x3da0ce40	8	0 R-rwd	Device\HardiskVolume1\$Windows\System32\WindowsPowerShell\v1.0\WPSEvents.dll																		
10	0x00000000	0x3da0e5b8	6	0 R-rwd	Device\HardiskVolume1\$Windows\System32\Winapi2.dll																		
11	0x00000000	0x3da0dec8	6	0 R-rwd	Device\HardiskVolume1\$Windows\System32\shsvcsrv.dll																		
12	0x00000000	0x3da0fce0	7	0 R-rwd	Device\HardiskVolume1\$Windows\System32\wpchpt.dll																		
10	0x00000000	0x3da10170	7	0 R-rwd	Device\HardiskVolume1\$Windows\System32\wbtsvc.dll																		
14	0x00000000	0x3da106d0	1	0 R-r-r-d	Device\HardiskVolume1\$Users\training\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5W39F85WL7\plugin[1].gif																		
5	0x00000000	0x3da10db8	5	0 R-rwd	Device\HardiskVolume1\$Windows\System32\mpm.exe																		
10	0x00000000	0x3da10d40	5	0 R-r-d	Device\HardiskVolume1\$Windows\System32\mapsp2.dll																		
17	0x00000000	0x3da11be0	6	0 R-rwd	Device\HardiskVolume1\$Windows\System32\wfapl.dll																		
18	0x00000000	0x3da12bd0	1	1 -----	Device\Adf\Endpoint																		
19	0x00000000	0x3da121c0	1	1 R-rw-	Device\HardiskVolume1\$Windows\winssrx\86_microsoft.windows.common-controls_6595b64144cdf1df_6.0.7601.17514_none_41e6975eb2b6f2b2																		
3	0x00000000	0x3da13100	3	1 -----	Device\Adf\Endpoint																		
8	0x00000000	0x3da13ba0	8	0 R-rwd	Device\HardiskVolume1\$Windows\System32\Setuptapi.dll																		
22	0x00000000	0x3da13ed0	8	0 RW----	Device\HardiskVolume1\$Users\training\AppData\Local\ow\Microsoft\CryptnetUI\Cache\MetaData#00B59EA0D3148774EF093BCFC8369_5ODE0AC3B0CBCE79BD877FBZC3962B18																		
5	0x00000000	0x3da14b80	5	0 R-r-r-d	Device\HardiskVolume1\$Windows\System32\catroot2\127D0AD1D-4EF2-11D1-8608-00C0AF4295EE\acadb																		
24	0x00000000	0x3da14e00	8	1 R-r-r-d	Device\HardiskVolume1\$Windows\System32\Kio-KR\mshtml.dll.mui																		
25	0x00000000	0x3da15650	1	1 R-r-r-d	Device\HardiskVolume1\$Windows\Registration\R00000000000000.cab																		
26	0x00000000	0x3da15c48	9	1 R-r-r-d	Device\HardiskVolume1\$Windows\System32\Kio-KR\msdtc\Vspres.dll.mui																		
27	0x00000000	0x3da15eb8	1	1 R-r-r-d	Device\HardiskVolume1\$Windows\System32\Kio-KR\miang.dll.mui																		
28	0x00000000	0x3da16150	6	0 R-rwd	Device\HardiskVolume1\$Windows\System32\Wdcom.exe																		
5	0x00000000	0x3da16640	5	0 R-rwd	Device\HardiskVolume1\$Windows\System32\Wpdhul.dll																		
30	0x00000000	0x3da172d8	1	1 R-rw-	Device\HardiskVolume1\$Windows\winssrx\86_microsoft.windows.common-controls_6595b64144cdf1df_6.0.7601.17514_none_41e6975eb2b6f2b2																		

[그림 3] filescan

[WHS-2] .iso

해커가 열람한 기밀문서의 파일명을 찾기 위해 filescan 플러그인을 사용한다. 또한 확인하기 편하기 위해 .csv 형태로 파일을 저장한다. 사용한 명령어는 [volatility_2.6_win64_standalone.exe -f "MemoryDump(SuNiNaTaS)" --profile=Win7SP0x86 filescan >> filescanFile.csv]이다. 해당 명령어는 메모리 내에 존재하는 모든 파일들의 리스트를 .csv 파일 형태로 출력한다. 사용 방법은 [volatility_2.6_win64_standalone.exe -f [파일명] --profile=[운영체제] filescan >> [저장할 파일명]]이다.

하지만 문제점이 있다. [그림 3]를 보니 파일이 너무 많다. 이러면 해커가 열람한 기밀문서가 어떠한 파일인지 찾기 어렵다. 해커가 기밀문서를 연 것이라면 cmd 를 사용하지 않았을까 하는 생각에 cmdscan 플러그인을 사용해 보기로 했다.

```
C:\Users\LG\OneDrive\문서\화이트햇 2기\iso 프로젝트\Write-Up\lw\SuNiNaTaS-30>volatility_2.6_win64_standalone.exe -f "MemoryDump(SuNiNaTaS)" --profile=Win7SP0x86 cmdscan
Volatility Foundation Volatility Framework 2.6
*****
CommandProcess: conhost.exe Pid: 2920
CommandHistory: 0x2b8328 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 3 LastAdded: 2 LastDisplayed: 2
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #0 @ 0x2ad590: notepad C:\Users\training\Desktop\SecreetDocumen7.txt
Cmd #1 @ 0x2a3348: nc
Cmd #2 @ 0x2a30b8: netstat -na
Cmd #33 @ 0xfdddc797: ??????????
*****
CommandProcess: conhost.exe Pid: 1980
CommandHistory: 0x107700 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x5c
Cmd #33 @ 0xfdddc797: ??????????
```

[그림 4] cmdscan

[volatility_2.6_win64_standalone.exe -f "MemoryDump(SuNiNaTaS)" --profile=Win7SP0x86 cmdscan] 명령어를 사용했다. 확인해 보니 cmd 로 notepad 를 열어 [SecreetDocumen7.txt]라는 딱 봐도 비밀스러운 파일을 열어본 것을 알 수 있었다. 따라서 **해커가 열람한 기밀문서의 파일명은 [SecreetDocumen7.txt]**이다. 해당 명령어는 cmd 에서 실행한 명령을 보여주며 사용 방법은 [volatility_2.6_win64_standalone.exe -f [파일명] --profile=[운영체제] cmdscan]이다.

기밀문서의 주요 내용을 확인하기 위해선 해당 [SecreetDocumen7.txt] 파일을 복구해야 한다. 파일 복구를 위해선 dumpfiles 플러그인을 사용해야 하는데, 해당 명령어를 사용하기 위해선 메모리 주소 값을 알아야 한다. 메모리 주소는 아까 저장해둔 [filescanFile.csv]의 Offset 목록에서 확인할 수 있다.

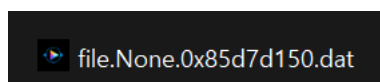
[WHS-2] .iso

1074	0x00000000129220	8	0 RW-r-- WDevice\HarddiskVolume1\Users\training\AppData\Local\Microsoft\Windows\
1075	0x000000003df2ddd8	8	0 RW-r-- WDevice\HarddiskVolume1\Users\training\Desktop\SecreetDocumen7.txt
1076	0x00000000129220	8	0 RW-r-- WDevice\HarddiskVolume1\Users\training\AppData\Local\Microsoft\Windows\

[그림 5] 메모리 주소 값 찾기

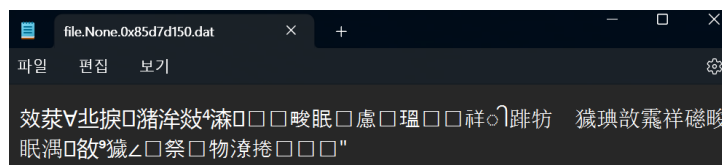
엑셀의 기능 중 하나인 찾기를 사용하여 [SecreetDocumen7.txt]를 찾아보니
0x000000003df2ddd8 이라는 메모리 주소를 찾을 수 있었다.

메모리 주소를 찾아냈으니 dumpfiles 명령어를 사용해 [SecreetDocumen7.txt] 파일을 복구할 수
있다. 사용한 명령어는 [volatility_2.6_win64_standalone.exe -f "MemoryDump(SuNiNaTaS)" --
profile=Win7SP0x86 dumpfiles -Q 0x000000003df2ddd8 -D ./]이다. 사용 방법은
[volatility_2.6_win64_standalone.exe -f [파일명] --profile=[운영체제] dumpfiles -Q [메모리 주소] -D
[저장할 디렉토리]이다.



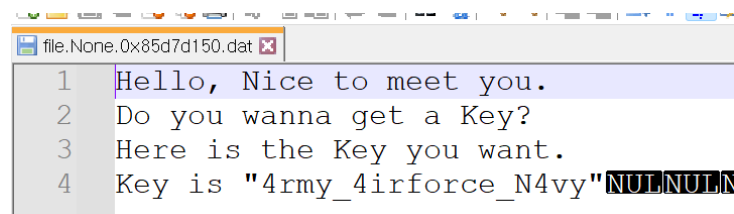
[그림 6] 기밀문서 복구

저장한 디렉토리에 [file.None.0x85d7d150.dat]이라는 파일이 생성되었다.



[그림 7] 깨진 기밀문서

해당 파일을 메모장으로 연결하여 확인해 보니 [그림 7]과 같이 글자가 깨진 것을 확인했다.



[그림 8] notepad++로 확인

메모장으로 확인할 수 없어 notepad++로 열어보니 메모장과 다르게 글씨가 깨지지 않았다.
Key 값은 4rmy_4irforce_N4vy이다.

5. Flag

Q1. 192.168.197.138

Q2. SeccretDocumen7.txt

Q3. 4rmy_4irforce_N4vy

위의 값을 합쳐 MD5 해시 값을 구한다. 참고로 SeccretDocumen7 에 꼭 .txt 까지 붙여야 한다.
붙이지 않으면 flag 값이 틀리다고 나온다.

(사용 사이트: https://tools.web-max.ca/encode_decode.php)

Specify data to encode / decode

c152e3fb5a6882563231b00f21a8ed5f

Encode / hash / encryption or decode / decryption results:

[c152e3fb5a6882563231b00f21a8ed5f](#)

[그림 9] flag 획득

flag 값은 **c152e3fb5a6882563231b00f21a8ed5f**이다. lowercase()를 붙이면 인증이 되지 않는다.

6. 별도 첨부



7. Reference

- volatility 사용법
 - <https://su0-0su.tistory.com/65>
 - <https://aaasssddd25.tistory.com/54>