

BOB7_유동민

사용Tool : volatility (<https://github.com/volatilityfoundation/volatility>)

사건개요 : 악의적인 공격자가 사용자의 볼륨을 암호화하고 사용자의 암호를 변경하였다. 메모리 덤프 파일을 분석하여 변경된 사용자 암호화 암호화 된 볼륨의 키를 얻어서 해결하라

파일

Memory : 메모리 덤프 파일

시스템 : Win7SP1x86

```
C:\Users\YooDongMin\Desktop\memory>vol.exe -f E:\디지털 포렌식채널지\VOL200\memory 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 (E:\디지털 포렌식채널지\VOL200\memory)
      PAE type : PAE
      DTB : 0x185000L
      KDBG : 0x82d72c28L
      Number of Processors : 1
      Image Type (Service Pack) : 1
      KPCR for CPU 0 : 0x82d73c00L
      KUSER_SHARED_DATA : 0xffdf0000L
      Image date and time : 2018-08-06 08:41:18 UTC+0000
      Image local date and time : 2018-08-06 17:41:18 +0900

C:\Users\YooDongMin\Desktop\memory>
```

Secret : bitLocker로 암호화된 디스크파일

0000FFE0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
0000FFF0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00010000	EB 58 90 2D 46 56 45 2D	46 53 2D 00 02 08 00 00	ëX -FVE-FS-
00010010	00 00 00 00 00 F8 00 00	3F 00 FF 00 80 00 00 00	ø ? ý
00010020	00 00 00 00 E0 1F 00 00	00 00 00 00 00 00 00 00	à
00010030	01 00 06 00 00 00 00 00	00 00 00 00 00 00 00 00	
00010040	80 00 29 00 00 00 00 4E	4F 20 4E 41 4D 45 20 20) NO NAME
00010050	20 20 46 41 54 33 32 20	20 20 33 C9 8E D1 BC F4	FAT32 3ÉÎÑúó
00010060	7B 8E C1 8E D9 BD 00 7C	A0 FB 7D B4 7D 8B F0 AC	{ Ä Ü½ ú}´}!ä~
00010070	98 40 74 0C 48 74 0E B4	0E BB 07 00 CD 10 EB EF	!@t Ht ´ » Í ëï
00010080	A0 FD 7D EB E6 CD 16 CD	19 00 00 00 00 00 00 00	ý}ëæÍ í
00010090	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000100A0	3B D6 67 49 29 2E D8 4A	83 99 F6 A3 39 E3 D0 01	;ÖgI).0J öf9&Ð
000100B0	00 00 10 02 00 00 00 00	00 A0 FA 0B 00 00 00 00	ú
000100C0	00 50 E5 15 00 00 00 00	00 00 00 00 00 00 00 00	Pä
000100D0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000100E0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000100F0	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00010100	0D 0A 52 65 6D 6F 76 65	20 64 69 73 6B 73 20 6F	Remove disks o
00010110	72 20 6F 74 68 65 72 20	6D 65 64 69 61 2E FF 0D	r other media.ý
00010120	0A 44 69 73 6B 20 65 72	72 6F 72 FF 0D 0A 50 72	Disk errorý Pr
00010130	65 73 73 20 61 6E 79 20	6B 65 79 20 74 6F 20 72	ess any key to r
00010140	65 73 74 61 72 74 0D 0A	00 00 00 00 00 00 00 00	estart
00010150	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00010160	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00010170	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
00010180	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	

Bitlocker : bdeinfo -o \$((512*128)) Secret

```
root@kali: ~/fo
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
Unable to set volume offset.
bdeinfo: system_string_copy_from_64_bit_in_decimal: unsupported character value: * at index:
3:4041271dc54175c5 : 4e3ef340dd377cea9c643951ce1e56c6
info_handle_set_volume_offset: unable to copy string to 64-bit decimal.
root@kali: ~/fo# bdeinfo -o $((512*128)) Secret
bdeinfo 20180806

BitLocker Drive Encryption information:
  Encryption method      : AES-CBC 128-bit with Diffuser
  Volume identifier      : cc0fd037-5775-452e-bd6d-f4da4b2b4b94
  Creation time          : Aug 06, 2018 08:39:41.946913000 UTC
  Description            : ROCKANDROLL-PC Secret 2018-08-06
  Number of key protectors : 2

Key protector 0:
  Identifier             : 4c438260-f1fe-40f7-b5da-5bff78061147
  Type                   : Password

Key protector 1:
  Identifier             : 168f1291-82c1-4bf2-b634-9cccec63e9ed
  Type                   : Recovery password

Unable to unlock volume.
root@kali: ~/fo#
```

버전 : 2.0 암호화 방법 : AES 128 with Diffuser

사용자 암호 복구 : 두가지 방법

1) 볼라틸리티 플러그인 사용 (mimikatz.py)

```
root@root:~/dongmin# volatility --plugins=plugin -f memory --profile=Win7SP1x86 mimikatz
Volatility Foundation Volatility Framework 2.6
Module  User      Password
-----  -
wdigest RockAndRoll RockAndRoll-PC rock_and_roll_babe^^^!@#~
wdigest ROCKANDROLL-PC$ WORKGROUP
root@root:~/dongmin#
```

RickAndRoll password : rock_and_roll_babe^^^!@#~

Bitlocker 암호 복구 : 볼라틸리티 플러그인 사용 (bitlocker.py)

```
C:\Users\YooDongMin\Desktop\memory>vol.exe --plugins=E:\디지털포렌식챌린지\VOL200 -f E:\디지털포렌식챌린지\VOL200\memory --profile=Win7SP1x86 bitlocker
Volatility Foundation Volatility Framework 2.6
*** Failed to import volatility.plugins.mimikatz (ImportError: No module named construct)

Address : 0x86863bc8
Cipher  : AES-128
FVEK    : 7c9e29b3708f344e4041271dc54175c5
TWEAK   : 4e3ef340dd377cea9c643951ce1e56c6

C:\Users\YooDongMin\Desktop\memory>
```

Address : 0x86863bc8

Cipher : AES-128

FVEK : 7c9e29b3708f344e4041271dc54175c5

TWEAK : 4e3ef340dd377cea9c643951ce1e56c6

bdemount -k 7c9e29b3708f344e4041271dc54175c5: 4e3ef340dd377cea9c643951ce1e56c6 -o
\$((512 * 128)) Secret /crypt

