Memory Mystery - HACKTORIA

Always use a dedicated computer or isolated VM when you "Forensic"

OS detection
Lists process memory ranges that potentially contain injected code
List processes in a tree
List process command line args
List sessions
Find the offset file to dump
Dump the file
Looking for the zip file
Dumps user hashes from memory
Looking into the registry
Dump the registry to get SAM
Get the Hint :)
THE END - crack the zip with the new hint

≣ BRIEFING

Greetings Special Agent,

We have received some catastrophic news from our sources about a cyber attack had hit a high-profile organization. Our sources have informed us that the attackers may have overlooked to remove some volatile traces contained in the compromised systems.

Based on our sources, the cyber attack was done by an Avanced Persistent Threat group called APT777. They managed to stay off radar for some time, but we believe that we can trace them back this time.

We have attached a memory dump file of one of the most critical compromised systems that needs to be analyzed using your digital forensics skills to gather more information on this group, and trace them using the evidences that you may find in the memory dump. Hope your ROCK spirit and technical skills help you this time too.

We understand that this mission will not be easy, but we have faith in your abilities. If you choose to accept this mission, you will be provided with all the necessary resources to complete it. Good luck, Agent. The fate of the cyber world rests in your hands.

As always, Special Agent K. The Contract is yours, if you choose to accept.

≣ MATERIALS

Download the file here:

https://drive.google.com/drive/folders/1HdSmyAUW-oOrbEoEZZCpkRQlfKrDpJfG

OS detection

```
volatility3 -f CompromisedSystemMem.vmem windows.info
```

```
Kernel Base     0x82851000
DTB     0x185000
Symbols file:///root/.local/share/pipx/venvs/volatility3
Is64Bit False
IsPAE   True
layer_name      0 WindowsIntelPAE
memory_layer    1 FileLayer
KdDebuggerDataBlock     0x8297bc28
NTBuildLab      7601.17514.x86fre.win7sp1_rtm.10
CSDVersion      1
KdVersionBlock  0x8297bc00
Major/Minor     15.7601
MachineType     332
KeNumberProcessors      1
SystemTime      2023-04-24 14:59:30
NtSystemRoot    C:\Windows
NtProductType   NtProductWinNt
NtMajorVersion  6
NtMinorVersion  1
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  1
PE Machine      332
PE TimeDateStamp        Sat Nov 20 08:42:49 2010
```

PE from 2010!!! Old stuff. Windows 7 is the OS so we'll use the proper plugins

Lists process memory ranges that potentially contain injected code

```
volatility3 -f CompromisedSystemMem.vmem windows.malfind|grep exe
```

```
[Aug 22, 2024 - 12:32:42 (CEST)] exegol-thm memory-mystery # volatility3 -f CompromisedSystemMem.vmem windows.malfind|grep exe
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to
he same file name, e.g. CompromisedSystemMem.vmem and CompromisedSystemMem.vmss.
776gresssvchost.exe	0xde0000	0xde1fff	VadS	PAGE_EXECUTE_READWRITE	2	1	Disabled	N/A
1052	svchost.exe	0x610000	0x611fff	VadS	PAGE_EXECUTE_READWRITE	2	1	Disabled	N/A
1312	explorer.exe	0x1e80000	0x1e81fff	VadS	PAGE_EXECUTE_READWRITE	2	1	Disabled	N/A
1312	explorer.exe	0x3130000	0x3130fff	VadS	PAGE_EXECUTE_READWRITE	1	1	Disabled	N/A
2316	wmpnetwk.exe	0x970000	0x971fff	VadS	PAGE_EXECUTE_READWRITE	2	1	Disabled	N/A
2956	notepad.exe	0x2a00000	0x2a00fff	VadS	PAGE_EXECUTE_READWRITE	1	1	Disabled	N/A
2956	notepad.exe	0x2bd0000	0x2bd1fff	VadS	PAGE_EXECUTE_READWRITE	2	1	Disabled	N/A
[Aug 22, 2024 - 12:32:52 (CEST)] exegol-thm memory-mystery #
```

Not so much! what the heck is gresssvchost.exe
Notepad has been used

List processes in a tree

```
volatility3 -f CompromisedSystemMem.vmem windows.pstree
```

```
504	396	winlogon.exe	0x82511580	3	110	1	False	2023-04-24 14:41:37.000000	N/A	\Device\HarddiskVolume1\Windows\System32\winlogon.exe
\winlogon.exe
1312	1288	explorer.exe	0x82577380	38	959	1	False	2023-04-24 14:41:39.000000	N/A	\Device\HarddiskVolume1\Windows\explorer.exe	C:\Win
.EXE
* 3704	1312	notepad.exe	0x82558d40	1	62	1	False	2023-04-24 14:58:43.000000	N/A	\Device\HarddiskVolume1\Windows\System32\notepad.exe
:\Users\Hoxed\Desktop\note.txt	C:\Windows\system32\NOTEPAD.EXE
* 2956	1312	notepad.exe	0x825af750	5	247	1	False	2023-04-24 14:48:50.000000	N/A	\Device\HarddiskVolume1\Windows\System32\notepad.exe
:\Windows\system32\notepad.exe
* 1556	1312	vmtoolsd.exe	0x863fdb90	6	218	1	False	2023-04-24 14:41:39.000000	N/A	\Device\HarddiskVolume1\Program Files\VMware\VMware Too
Mware\VMware Tools\vmtoolsd.exe" -n vmusr	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
* 3840	1312	notepad.exe	0x82501030	1	62	1	False	2023-04-24 14:59:24.000000	N/A	\Device\HarddiskVolume1\Windows\System32\notepad.exe
:\Users\Hoxed\Desktop\note.txt	C:\Windows\system32\NOTEPAD.EXE
```

Juicy!! After logon, Notepad is used by the user ***HOXED ← :) I like the name***

\Users\Hoxed\Desktop\note.txt *has been written*
To be noted, VMware Tools is also used

PID is 1312

List process command line args

```
volatility3 -f CompromisedSystemMem.vmem windows.cmdl
```

```
2300    WmiPrvSE.exe    C:\Windows\system32\wbem\wmiprvse.exe
3704    notepad.exe     "C:\Windows\system32\NOTEPAD.EXE" C:\Users\Hoxed\Desktop\note.txt
3840    notepad.exe     "C:\Windows\system32\NOTEPAD.EXE" C:\Users\Hoxed\Desktop\note.txt
3940    cmd.exe Required memory at 0x7ffdf010 is not valid (process exited?)
3980    conhost.exe     Required memory at 0x7ffdf010 is not valid (process exited?)
3960    ipconfig.exe    Required memory at 0x7ffdc010 is not valid (process exited?)
[Aug 22, 2024 - 12:51:13 (CEST)] exegol-thm memory-mystery # volatility3 -f CompromisedSystemMem.vmem windo
```

List sessions

```
volatility3 -f CompromisedSystemMem.vmem windows.sessions.Ses
sions
```

```
1       -       504     winlogon.exe    /SYSTEM 2023-04-24 14:41:37.000000
1       -       1300    dwm.exe WIN-MNF9FL8RCB0/Hoxed   2023-04-24 14:41:39.000000
1       Console 1312    explorer.exe    WIN-MNF9FL8RCB0/Hoxed   2023-04-24 14:41:39.000000
1       -       1408    taskhost.exe    WIN-MNF9FL8RCB0/Hoxed   2023-04-24 14:41:39.000000
1       Console 1556    vmtoolsd.exe    WIN-MNF9FL8RCB0/Hoxed   2023-04-24 14:41:39.000000
1       Console 2956    notepad.exe     WIN-MNF9FL8RCB0/Hoxed   2023-04-24 14:48:50.000000
1       Console 3704    notepad.exe     WIN-MNF9FL8RCB0/Hoxed   2023-04-24 14:58:43.000000
1       Console 3840    notepad.exe     WIN-MNF9FL8RCB0/Hoxed   2023-04-24 14:59:24.000000
```

> *Nothing much, notepad notepad notepad, so let's dig in and* ***dump the note.txt***

Find the offset file to dump

```
volatility3 -f CompromisedSystemMem.vmem windows.filescan|gre
p -i note.txt
# To Dump an specific PID in case of a big memory dump file
# volatility3 -f CompromisedSystemMem.vmem -o . windows.memma
p.Memmap --pid 1312 --dump
```

```
0x3fc77360 100.0\Users\Hoxed\Desktop\note.txt    128
```

Dump the file

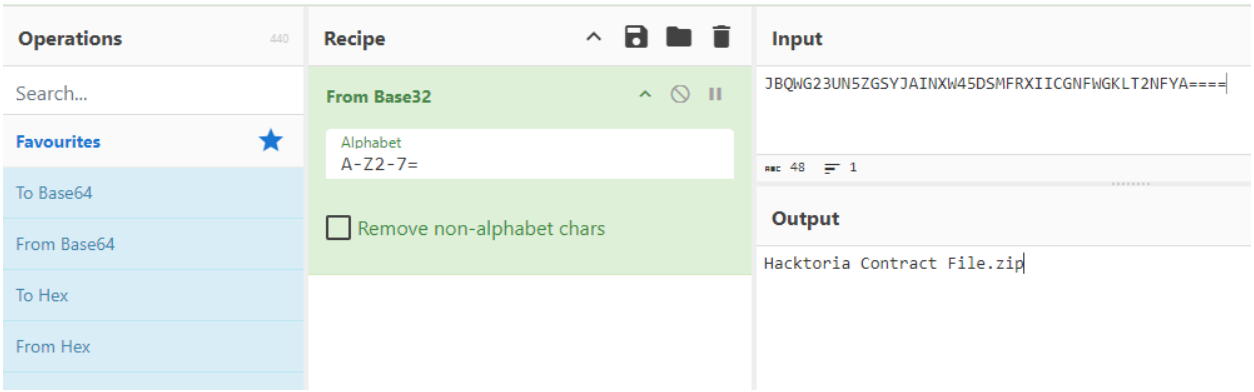
```
volatility3 -f CompromisedSystemMem.vmem -o .  windows.dumpfi
les --physaddr 0x3fc77360
```

```
Cache   FileObject      FileName        Result

DataSectionObject       0x3fc77360      note.txt        file.0x3fc77360.0x8428cf78.DataSectionObject.note.txt.dat
```

```
cat file.0x3fc77360.0x8428cf78.DataSectionObject.note.txt.dat
JBQWG23UN5ZGSYJAINXW45DSMFRXIICGNFWGKLT2NFYA====

JBQWG23UN5ZGSYJAINXW45DSMFRXIICGNFWGKLT2NFYA====

JBQWG23UN5ZGSYJAINXW45DSMFRXIICGNFWGKLT2NFYA====
```

So it is base64 or something similar, you can use **Cyberchef with the magic Recipe**.
cat file.0x3fc77360.0x8428cf78.DataSectionObject.note.txt.dat|base32 -d

Hacktoria Contract File.zip ← Nice, we have to find this file now



Looking for the zip file

Similar as above

```
[Aug 22, 2024 - 14:32:58 (CEST)] exegol-thm memory-mystery # volatility3 -f CompromisedSystemMem.vmem windows.filescan|grep Hacktoria
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM f
he same file name, e.g. CompromisedSystemMem.vmem and CompromisedSystemMem.vmss.
0x3da0fac0 100.0\Hacktoria Contract File.zip    128
0x3f257f80      \Users\Hoxed\AppData\Local\Temp\vmware-Hoxed\VMwareDnD\8d66c36c\Hacktoria Contract File.zip     128
0x3fc9f658      \Users\Hoxed\AppData\Roaming\Microsoft\Windows\Recent\Hacktoria Contract File.lnk       128
[Aug 22, 2024 - 14:33:33 (CEST)] exegol-thm memory-mystery # volatility3 -f CompromisedSystemMem.vmem -o .  windows.dumpfiles --physaddr 0x3da0fac0
Volatility 3 Framework 2.7.0
WARNING  volatility3.framework.layers.vmware: No metadata file found alongside VMEM file. A VMSS or VMSN file may be required to correctly process a VMEM f
he same file name, e.g. CompromisedSystemMem.vmem and CompromisedSystemMem.vmss.
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result

DataSectionObject       0x3da0fac0      Hacktoria Contract File.zip     file.0x3da0fac0.0x85869a90.DataSectionObject.Hacktoria Contract File.zip.dat
[Aug 22, 2024 - 14:33:53 (CEST)] exegol-thm memory-mystery # 7z x file.0x3da0fac0.0x85869a90.DataSectionObject.Hacktoria\ Contract\ File.zip.dat
```

A password is required to decompress the file.

I wasted a lot of time because I tried every dictionary I could find.
After 2 hours, I have to admit that I missed something.

Dumps user hashes from memory

I was wondering if the user creds where the one to find to unlock the zip.

It's not :(.

```
volatility3 -f CompromisedSystemMem.vmem windows.hashdump.Has
hdump
```

```
Progress:  100.00               PDB scanning finished
User    rid     lmhash  nthash

Administrator   500     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Guest   501     aad3b435b51404eeaad3b435b51404ee        31d6cfe0d16ae931b73c59d7e0c089c0
Hoxed   1000    aad3b435b51404eeaad3b435b51404ee        7a21990fcd3d759941e45c490f143d5f
```

Looking into the registry

```
volatility3 -f CompromisedSystemMem.vmem windows.registry.hiv
elist
```

```
0x87c104c8              Disabled
0x87c1a248      \REGISTRY\MACHINE\SYSTEM        Disabled
0x87c44268      \REGISTRY\MACHINE\HARDWARE      Disabled
0x87cd7008      \SystemRoot\System32\Config\DEFAULT     Disabled
0x87ce3008      \Device\HarddiskVolume1\Boot\BCD        Disabled
0x87ce39c8      \SystemRoot\System32\Config\SOFTWARE    Disabled
0x888ca520      \??\C:\System Volume Information\Syscache.hve   Disabled
0x8a6f47c8      \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT        Disabled
0x8a77e5c0      \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT  Disabled
0x8d15d9c8      \??\C:\Users\Hoxed\ntuser.dat   Disabled
0x8d16a008      \??\C:\Users\Hoxed\AppData\Local\Microsoft\Windows\UsrClass.dat Disabled
0x968eb008      \SystemRoot\System32\Config\SECURITY    Disabled
0x969519c8      \SystemRoot\System32\Config\SAM Disabled
```

Juicy SAM is here!!!

The Security Accounts Manager (*SAM*) is a database *file* in the *Microsoft Windows* operating system (OS) that contains usernames and passwords

> **Again I wanted to stick with Volatility3 but could not manage to extract the SAM after few hours.**
> **So I moved on volatility2**

Dump the registry to get SAM

With Volatility2 you need the right Profile

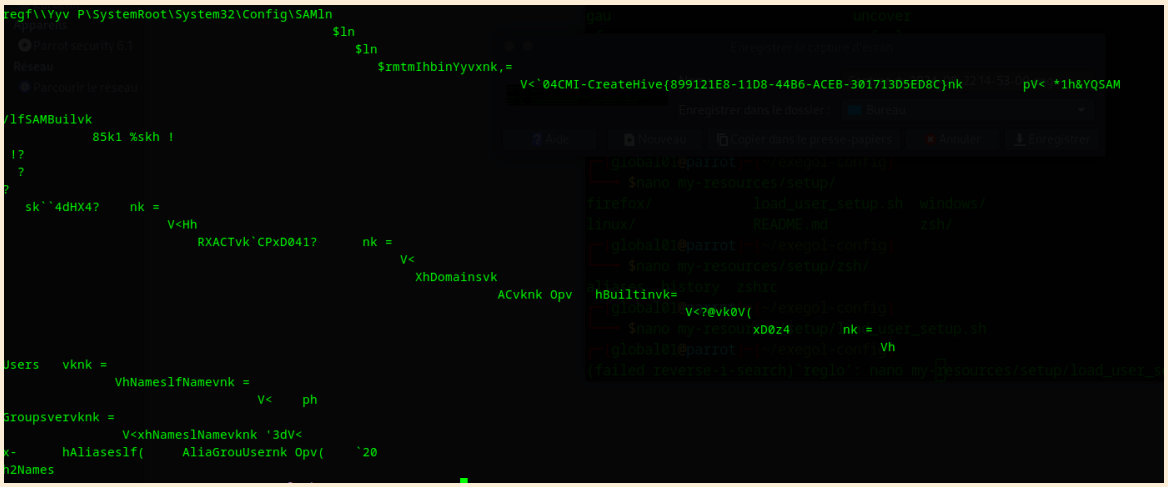
```
volatility2 -f CompromisedSystemMem.vmem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug    : Determining profile based on
KDBG search...
          Suggested Profile(s) : Win7SP1x86_23418, Win7SP0x8
6, Win7SP1x86_24000, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel A
S)
                     AS Layer2 : FileAddressSpace (/workspac
e/memory-mystery/CompromisedSystemMem.vmem)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x8297bc28L
          Number of Processors : 1
     Image Type (Service Pack) : 1
                KPCR for CPU 0 : 0x8297cc00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2023-04-24 14:59:30 UTC+0000
     Image local date and time : 2023-04-24 17:59:30 +0300


 volatility2 -f CompromisedSystemMem.vmem --profile=Win7SP1x8
6 dumpregistry -D output
```

Get the Hint :)

```
strings -n10 output/registry.0x969519c8.SAM.reg
CMI-CreateHive{899121E8-11D8-44B6-ACEB-301713D5ED8C}
Administrators
S-1-5-21-1154659777-2139612456-419014984
Event Log Readers
24F3736544
Performance Monitor Users
UserPasswordHint <-- Looking good
Administrator
Administratoroni
Performance Log Users
LastSkuUpgrade
Distributed COM Users
ServerDomainUpdates
Event Log Readers
```

.reg files are kind of binary

head output/registry.0x969519c8.SAM.reg




```
xxd output/registry.0x969519c8.SAM.reg
```

```
00002ce0: e019 0000 4e61 6d65 e0ff ffff 766b 0100  ....Name....vk..
00002cf0: 7c01 0000 6037 0000 0300 0000 0100 0000  |...`7..........
00002d00: 4300 0000 0000 0000 d8ff ffff 766b 1000  C...........vk..
00002d10: 1a00 0000 301d 0000 0300 0000 0100 0000  ....0...........
00002d20: 5573 6572 5061 7373 776f 7264 4869 6e74  UserPasswordHint
00002d30: e0ff ffff 6500 6e00 6400 2000 6900 7400  ....e.n.d. .i.t.
00002d40: 2000 7700 6900 7400 6800 2000 3500 0000   .w.i.t.h. .5...
00002d50: 4001 0000 9000 0000 a000 0000 1400 0000  @...............
00002d60: 4400 0000 0200 3000 0200 0000 02c0 1400  D.....0.........
00002d70: 0e00 0501 0101 0000 0000 0001 0000 0000  ................
00002d80: 02c0 1400 ffff 1f00 0101 0000 0000 0005  ................
```

THE END - crack the zip with the new hint

Let's add 5 at the end of each line of the most common wordlist

```
sed 's/$/5/' /opt/rockyou.txt > rockyou_modified.txt
head rockyou_modified.txt
1234565
123455
1234567895
password5
iloveyou5
princess5
12345675

zip2john file.0x3da0fac0.0x85869a90.DataSectionObject.Hacktor
ia\ Contract\ File.zip > file.hash
john --wordlist=rockyou_modified.txt file.hash

WE HAVE THE PASS TO UNLOCK THE ZIP AND...
THE FINAL FLAAAAAAAAAAGGGGGGGGGGGGGGG !!!!!!!!!!!!
```

— gl0bal01