MemoryDecompression capabilities

This document will demonstrate an example where the MemoryDecompression tool is used, and show its usefulness in an investigation. As the strings-tool is often utilized in investigations to find traces of malicious activities, it is important that the data we are analysing is available in clear text form. In Windows 10, if the memory pages that contains the malicious activity are compressed, they will obfuscate potentially important information to the examiner. This example will demonstrate how decompression gives the examiner more information from memory.

We have two indicators of compromise:

- **Duriell**
- **Olashamann**

The actual actions done on this target:

- Opened a powershell prompt, and typed **'echo «Hello Duriell!»'**
- Opened a bash prompt (Windows subsystem for Linux), and typed **'echo «Hello Olashamann!»'**

We have a memory sample to work with the suspicious activity. We will run a yarascan to look for the indicators.

```
# volatility -f memory.img --profile=Win10x64_16299 yarascan -Y 'Olashamann' --
wide
Volatility Foundation Volatility Framework 2.6
Rule: r1
Owner: Process MemCompression Pid 1536
0x0379bf04  4f 6c 61 73 68 61 6d 61 6e 6e 21 22 00 45 2f 2e   Olashamann!".E/.
0x0379bf14  6c 6f 63 61 00 00 00 00 6c 2f 62 69 6e 3a 24 50   loca....l/bin:$P
0x0379bf24  41 54 48 22 00 24 7b 73 65 72 76 69 63 65 73 5b   ATH".${services[
0x0379bf34  40 5d 7d 27 20 2d 2d 20 00 08 00 00 09 09 24 63   @]}'.--.......$c
0x0379bf44  75 72 20 29 29 00 74 20 64 65 73 63 72 69 62 65   ur.)).t.describe
0x0379bf54  b8 00 63 6f 6e 74 61 69 6e 73 20 48 45 3c 88 00   ..contains.HE<..
0x0379bf64  01 41 44 20 3b 3b 0a 09 00 00 28 62 72 61 6e 63   .AD.;;....(branc
0x0379bf74  68 29 62 00 09 67 69 8f 01 2d 2d 61 6c 6c bf 01   h)b..gi..--all..
0x0379bf84  a4 c5 02 cf 01 07 03 a3 2a 20 20 00 02 41 7c 28   ........*....A|(
0x0379bf94  04 66 61 75 6c 74 5f 01 2d 2d 74 61 67 73 f0 04   .fault_.--tags..
0x0379bfa4  65 78 61 63 74 2d 6d 61 74 63 68 4f 03 23 65 73   exact-matchO.#es
0x0379bfb4  61 63 20 00 00 00 00 32 3e 2f 64 65 76 2f 6e 75   ac.....2>/dev/nu
0x0379bfc4  6c 6c 29 22 00 7c 49 54 7c 78 6d 7c 58 4d 7c 69   ll)".|IT|xm|XM|i
0x0379bfd4  73 6f 7c 49 53 4f 29 01 00 00 00 7c 2b 28 5b 30   so|ISO)....|+([0
0x0379bfe4  2d 39 5d 29 2e 40 28 76 64 72 7c 56 44 52 29 29   -9]).@(vdr|VDR))
0x0379bff4  3f 28 2e 70 61 72 74 29 27 00 b0 01 00 00 00 50   ?(.part)'......P
```

```
# volatility -f memory.img --profile=Win10x64_16299 yarascan -Y 'Duriell' --wide
Volatility Foundation Volatility Framework 2.6
Rule: r1
Owner: Process MemCompression Pid 1536
0x07755ac4  44 00 75 00 72 00 69 00 65 00 6c 00 6c 00 00 00   D.u.r.i.e.l.l...
0x07755ad4  00 00 00 00 ff ff 00 00 00 00 00 00 00 00 00 00   ................
0x07755ae4  e0 e5 96 3e a0 01 00 00 19 00 9d 06 0f 00 00 10   ...>............
```

```
0x07755af4  d8 0f 00 07 00 0f ff e2 0f 68 a0 ad ca fb 7f 00   .........h......
0x07755b04  00 00 00 00 00 00 00 00 00 90 7f db 41 a0 01 00   ............A...
0x07755b14  00 46 72 18 45 5c 00 50 88 00 6c ea ff ff 0f 40   .Fr.E\.P..l....@
0x07755b24  00 07 00 ff ff fc 03 e0 e5 96 3e a0 01 00 00 d0   ..........>.....
0x07755b34  1b 47 20 ff fc 03 f7 1f 0f ff f4 07 ff ff ff 2f   .G............./
0x07755b44  02 00 07 00 ff 4d 20 37 03 4d 2f 03 ff 70 7f 07   .....M.7.M/..p..
0x07755b54  d7 c7 0b ff 70 47 04 ff 2c 0d 50 7b ff ff ff 4f   ....pG..,.P{...O
0x07755b64  00 07 00 ff ff 5b 01 80 07 ff 0a ff 5b 01 ef 0a   .....[......[...
0x07755b74  0f ff 3e 0d 9d 3a 42 34 06 37 00 00 ff ff ff 40   ..>..:B4.7.....@
0x07755b84  00 07 00 ff ff 55 01 40 00 c0 ff ff 38 ef 0a ff   .....U.@....8...
0x07755b94  55 01 bf 0a 0f ff 46 0d ff 4b 07 04 1f 3f 81 29   U.....F..K...?.)
0x07755ba4  60 00 07 00 cc 3a b7 00 00 58 bf 00 6d b7 00 c0   `....:...X..m...
0x07755bb4  19 7d 5e b1 02 af 00 66 00 00 bd 02 d7 00 3f 04   .}^....f......?.
```

We can see that the IOCs can be found in the address space of the MemCompression process with PID 1536. If the IOCs were resident in their respective processes, powershell and bash, we would expect to see them in a «conhost.exe» process. We will decompress the pages from the MemCompression process by dumping the VADs with Volatility plugin vaddump, to see if we can find some more data related to the IOCs:

```
# volatility -f memory.img --profile=Win10x64_16299 vaddump –p 1536 –D Duriell-Olashamann-vaddump
```

Then we use the MemoryDecompression tool to decompress the VADs. All decompressed data is written to the file “Duriell-Olashamann-all-vads-decompressed.bin”

```
PS> MemoryDecompression.exe Duriell-Olashamann-vaddump/ Duriell-Olashamann-all-vads-decompressed.bin
```

The total size of the vaddump output is **494MB**:

```
# du -h Duriell-Olashamann-vaddump/
494M    Duriell-Olashamann-vaddump/
```

The total size of the decompressed data is **1.1GB**:

```
# ls -lah Duriell-Olashamann-all-vads-decompressed
-rwxrwxrwx 1 root root 1.1G Aug 27 12:45 Duriell-Olashamann-all-vads-decompressed
```

This means that memory compression makes more data available to the examiner than other operating systems without this feature, if the examiner has a decompression tool available.

Now we will run strings on the compressed and decompressed data, and compare the results. Unicode is accounted for with the -el flag.

Strings on **<u>compressed</u>** content:

```
# strings -el Duriell-Olashamann-vaddump/* | grep -E 'Duriell|Olashamann'
```

```
Duriell
```

1 hit

```
# strings Duriell-Olashamann-vaddump/* | grep -E 'Duriell|Olashamann'

"Hello Olashamann!"
echo "Hello Olashamann!"
$ echo "Hello Olashamann!"
/cho "Hello Olashamann!"b
```

4 hits

Strings on **<u>decompressed</u>** content:

```
# strings Duriell-Olashamann-all-vads-decompressed | grep -E 'Duriell|Olashamann'

Hello Olashamann!
Duriell
Duriell
Hello Duriell!
"Hello Duriell!@
"Hello Duriell
"Hello Duriell!:
Hello Duriell!
Hello Duriell!
"Hello Duriell!@
Hello Duriell!
promptDuriell!
echo "Hello Duriell!"
echo "Hello Duriell
Hello Duriell
Hello Duriell
Hello Duriell
Hello Duriell
echo "Hello Duriell!
Hello Duriell!
Hello Duriell!
Hello Duriell!
Hello Duriell!
echo "Hello Duriell!@
Hello Duriell!@
Hello Duriell!@
Hello Duriell!@
Hello Duriell!@
echo "Hello Duriell!
Hello Duriell!
Hello Duriell!
Hello Duriell!
Hello Duriell!
echo "Hello Duriell!:
Hello Duriell!:
Hello Duriell!:
Hello Duriell!:
Hello Duriell!:
echo "Hello Duriell!
Hello Duriell!
Hello Duriell!
```

```
Hello Duriell!
Hello Duriell!
Hello Duriell!
echo "Hello Duriell!"
Hello Duriell!
Hello Duriell!
Hello Duriell!
Hello Duriell!
echo "Hello Duriell!"
Hello Duriell!
Hello Duriell!
Hello Duriell!
Hello Duriell!
echo "Hello Duriell!"
echo "Hello Duriell!"
echo "Hello Duriell!"
promptDuriell!
Hello Duriell!
Hello Duriell!
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
PS C:\Users\User> echo "Hello Duriell!"
Hello Duriell!
PS C:\Users\User>
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
user@WinDev1802Eval:/mnt/c/Windows/System32$
user@WinDev1802Eval:/mnt/c/Windows/System32$
user@WinDev1802Eval:/mnt/c/Windows/System32$ echo "Hello Olashamann!"
Hello Olashamann!
user@WinDev1802Eval:/mnt/c/Windows/System32$
```

72 hits

```
# strings Duriell-Olashamann-all-vads-decompressed | grep -E 'Duriell|Olashamann'

cho "Hello Olashamann"
"Hello Olashamann!"
echo "Hello Olashamann!"
[00m$ echo "Hello Olashamann!"
echo "Hello Duriell!"
echo "Hello Duriell!"
[DHello Olashamann!
Hello Olashamann!
echo "Hello Olashamann!"
echo "Hello Olashamann!"
echo "Hello Olashamann!"
```

11 hits

As shown by the output, the decompressed data gives us way more information than the compressed data. In this case, we could still find the IOCs by searching in the compressed memory. However, other indicators such as IP addresses could become impossible to find in compressed form in its actual form.