MemoryDecompression v0.9 user guide

This guide explains how to use the MemoryDecompression tool. The tool uses a brute-force approach to decompress memory pages that has been compressed by Windows 10. It has been tested successfully on data from memory dumps and page files. For now, the tool can only be run on a Windows 8 or Windows 10 client, as the ntdll.dll function used to decompress is only available on those versions. In a future version, the

Usage

- Open a console on your Windows 8/10 workstation (cmd/powershell)
- `PS> MemoryDecompression.exe <input file or folder> <output-file>`

Input file/folder

The input parameter can be either a file or a folder. If the input parameter is a folder, the tool will attempt to decompress ALL the files it contains. Investigators can use a tool like Volatility to extract the compressed memory from the MemCompression[1] process. Output files from both `vaddump` and `memdump` (Volatility plugins) works. The investigator can also extract page files (pagefile.sys) from a disk image and run the decompressor on the file. Tests have shown that this can take over **4 hours** on a 6GB page file.

Output file

The output parameter specifies the file which the decompressed output data is written to. As of version 0.1, the tool does not check if the file specified already exists, and will overwrite it if it has the correct permissions. So be careful not to overwrite an important file.

Example:

The example demonstrates how the MemoryDecompression tool works.

Page file:

The size of the pagefile.sys used in this example was ~6GB. The "Total compressed data" shows that the MemoryDecompression tool has found over 1GB of compressed data that decompresses to over 3GB of data, shown in "Total decompressed data:". The tool also outputs the amount of time decompressing the files took.

```
PS> MemoryDecompression.exe pagefile.sys pagefile-decompressed.bin

Decompressing    .\pagefile.sys

Total decompressed pages:       803827
Total compressed data:          1111505498 bytes
Total decompressed data:        3292475392 bytes


Decompression completed in:
Total Microseconds:   16731799969
Total Seconds:        16731
```

[1] Compressed memory is stored in the process space of a process in Windows 10 called «MemCompression».

```
Total Minutes:        278
Total Hours:  4
```

Memory dump:

The tool should work directly on a memory dump, but it will take a lot of time, so we want to extract the compressed data from the memory dump using Volatility. Outputs are minimized for readability.

```
# volatility -f memory.dmp --profile=Win10x64_16299 pslist

Name           PID  Start
-------------- ---- ------
MemCompression 1708 2018-08-24 07:38:02 UTC+0000
```

The PID is used to dump the VAD-segments of the process, containing the compressed data.

```
# volatility -f memory.dmp --profile=Win10x64_16299 vaddump -p 1708 -D
vaddump-folder/
```

```
PS> MemoryDecompression.exe vaddump-folder all-vads-decompressed.bin
Decompressing    MemCompression.4afa580.0x00000000000b0000-0x00000000000cffff.dmp
Decompressing    MemCompression.4afa580.0x00000000000d0000-0x00000000000effff.dmp
Decompressing    MemCompression.4afa580.0x00000000000f0000-0x000000000010ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000a10000-0x0000000000a2ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000a30000-0x0000000000a4ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000a50000-0x0000000000a6ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000a70000-0x0000000000a8ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000a90000-0x0000000000aaffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000ab0000-0x0000000000acffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000ad0000-0x0000000000aeffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000af0000-0x0000000000b0ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000b10000-0x0000000000b2ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000b30000-0x0000000000b4ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000b50000-0x0000000000b6ffff.dmp
Decompressing    MemCompression.4afa580.0x0000000000b70000-0x0000000000b8ffff.dmp

Total decompressed pages:       1239
Total compressed data:          1789658 bytes
Total decompressed data:        5074944 bytes


Decompression completed in:
Total Microseconds:     12657726
Total Seconds:  12
Total Minutes:  0
Total Hours:    0
```

The amount of VAD-segments will probably be significantly higher.

Any issues or questions, send me an e-mail on alexoest@gmail.com.