Unpacking Clop

By Sebdraven

Published: 2019-12-02 · Archived: 2026-04-06 01:04:01 UTC

2 min read

Dec 2, 2019

On twitter, a good analysis of the ransomware Clop has done. But nothing on the unpacking.

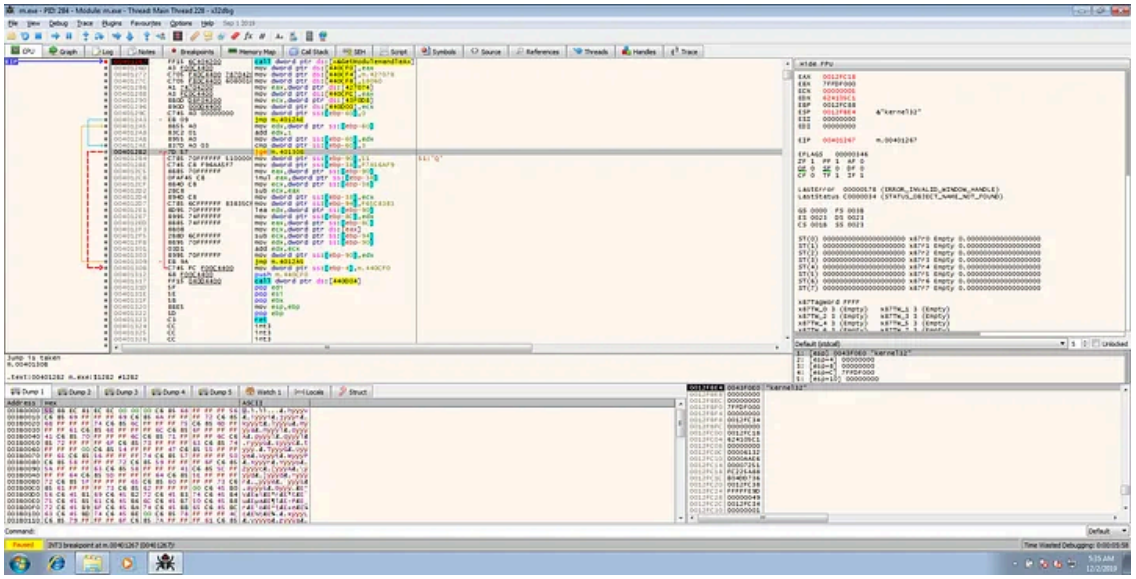
The packer has three stages.

The first stage is an allocation and dexoring of the overlay in the function FUN_00401000

*local_c = (code *)VirtualAllocEx((HANDLE)0xffffffff,(LPVOID)0x0,0x1c20,DAT_0043f0dc,0x40)*

while (local_40 < 900) {
local_80 = DAT_00426260;
*uVar1 = *(int *)(&DAT_00426264 + local_40 * 4) - local_40 ^ DAT_00426260;*
local_24 = local_24 + -0x438;
local_84 = (uVar1 << 7 | uVar1 >> 0x19) ^ DAT_00426260;
*(uint *)(local_c + local_40 * 4) = local_84;*
local_40 = local_40 + 1;
}

Press enter or click to view image in full size



the dropper jump in the shellcode with:

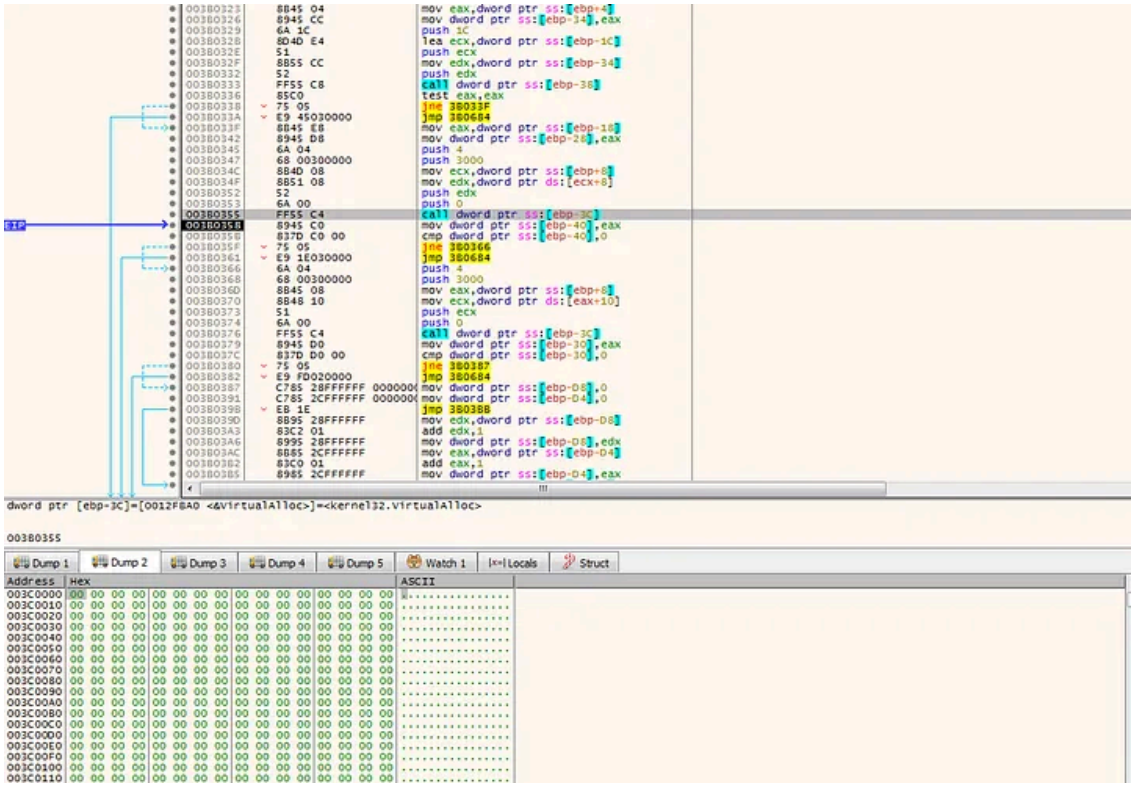
00401317 call dword ptr ds:[440D04]

the second stage is the execution of the shell code in six steps:

Get Sebdraven's stories in your inbox

The first step is to allocate a new page with Virtualloc.

Press enter or click to view image in full size



The second step is decoded an compressed PE.

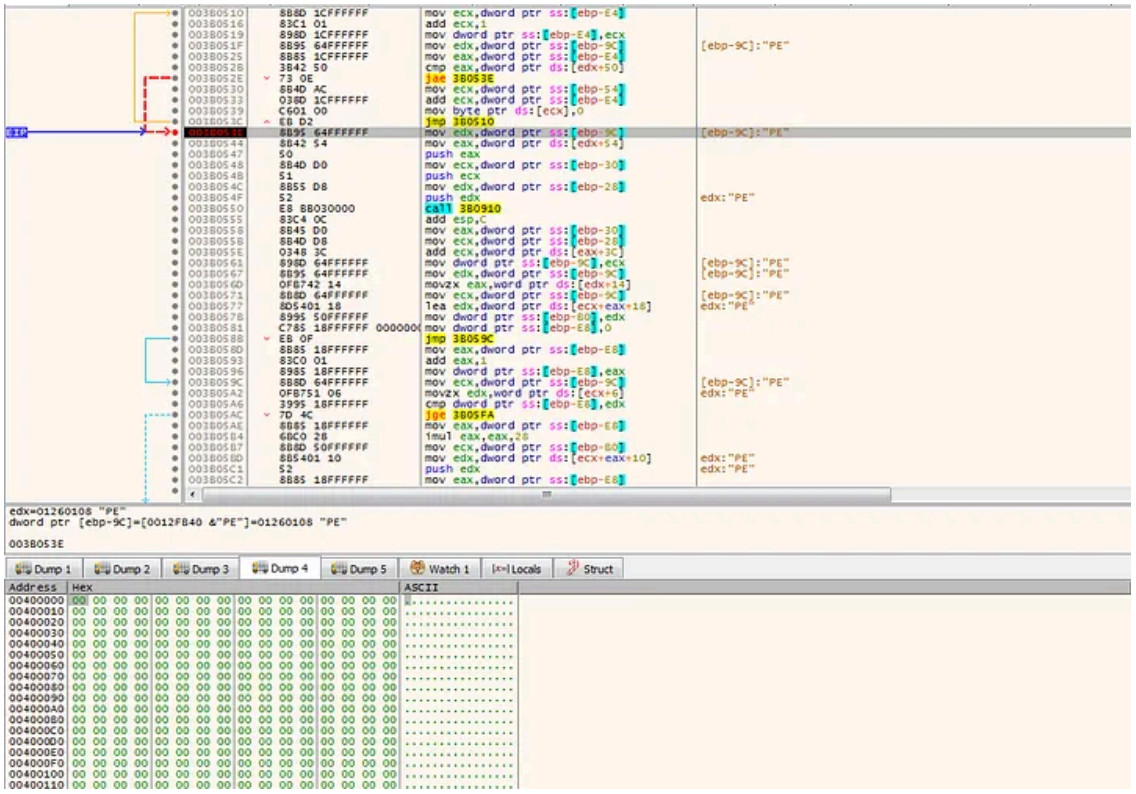
Press enter or click to view image in full size

The third step is a decompression of the payload without import table in 3B010.

The fourth step is reconstruction of the import table in 3B0910.

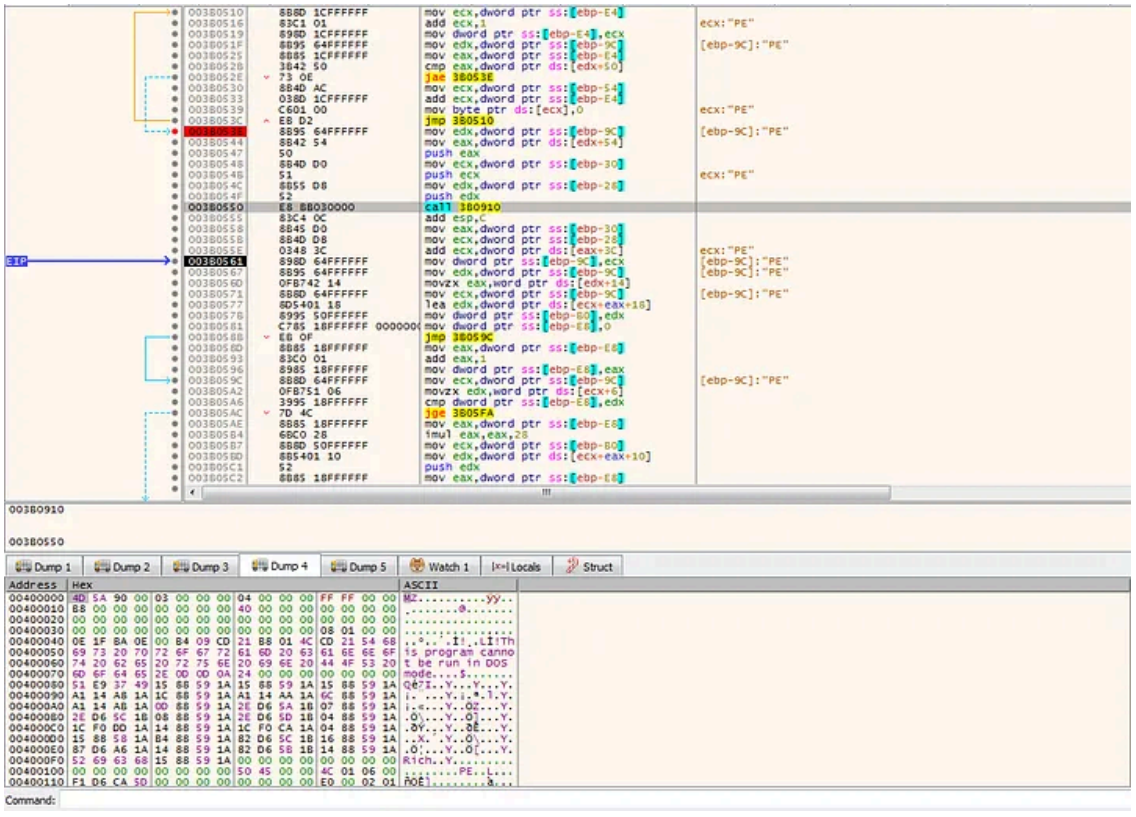
The fifth step is the wipe of the loader in memory.

Press enter or click to view image in full size



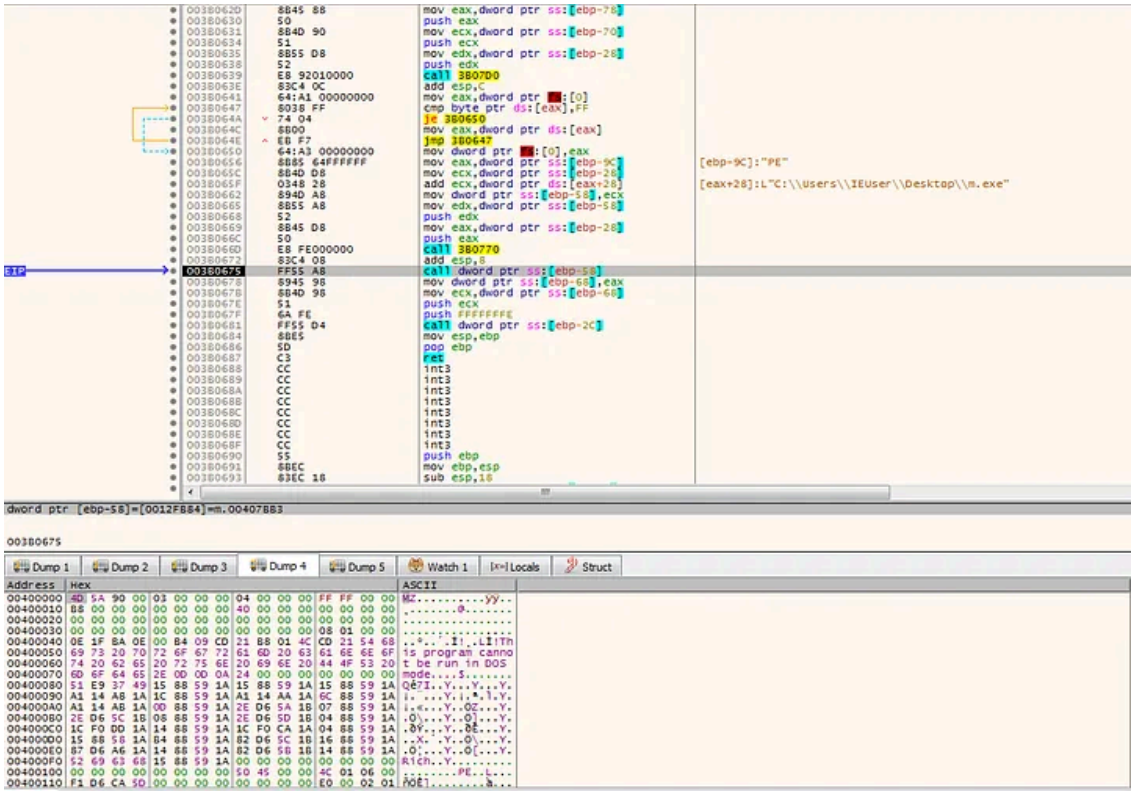
And the last stage is the copy of the real payload with the function 3B0910.

Press enter or click to view image in full size



And jump in the new entrypoint in dword ptr [ebp-58]=[0012FB84]=m.00407BB3

Press enter or click to view image in full size



Now you have the real malware clop for following the analysis of [Minhee Lee]

Source: https://medium.com/@Sebdraven/unpacking-clop-416b83718e0f