Emotet Unpacking:

By Ilan Duhin

Published: 2023-01-26 · Archived: 2026-04-05 17:23:09 UTC

Writer: Ilan Duhin

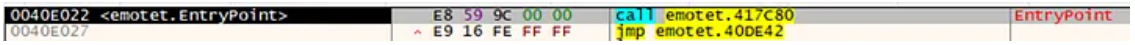
Executive Summary:

Emotet is an advanced, self-propagating and modular Trojan. Emotet was once a banking Trojan, but recently has been used as a downloader for other malware or malicious campaigns. It uses multiple methods for maintaining persistence and Evasion techniques **like packing**. In addition, it can be spread through phishing spam emails containing malicious attachments or links.

Emotet uses a number of malicious techniques when he locates on the victim's computer such as: **allocating memory for process injection, and creating new processes/threads to make persistence.**

Starting with **x32dbg & Running our sample** until the Entry point.

Press enter or click to view image in full size

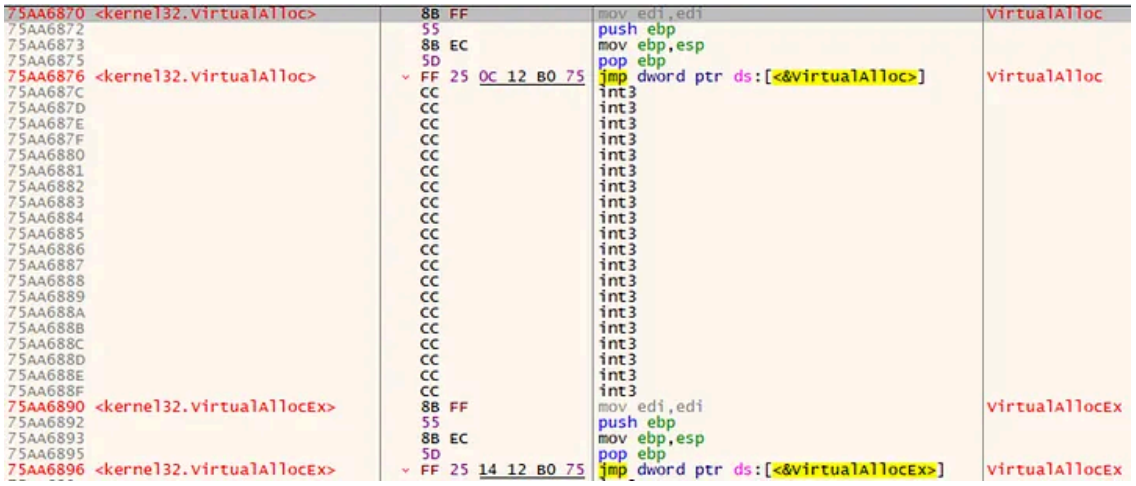


We should now search for API call of VirtualAlloc (we saw earlier the allocation memory on process hacker in the dynamic investigation).

So we need to search in the debugger (**Ctrl + G)=VirtualAlloc** and press OK so we can put **BP** on her and see which arguments contain the original code.

When we get to the beginning of the function, our goal is to see the "**ret"** that describe the end of the function so we can put **BP.**

Press enter or click to view image in full size

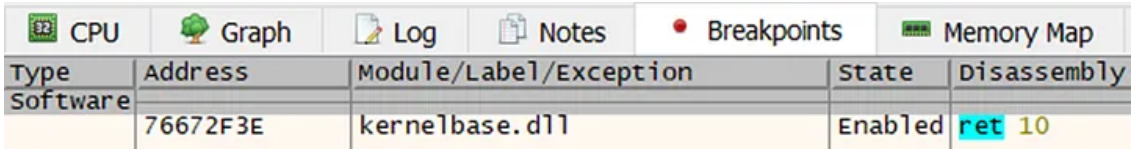


To see the end we need to press **Enter.**

Press enter or click to view image in full size

Now we put **BP.** To make sure that the BP is set we can look at Breakpoint tab.

Press enter or click to view image in full size



Press enter or click to view image in full size

Now Debug & Run + **Step over** (F8) the function (the debugger take now us to the original code).

When we press **step over** we jump to the next function below. **But if we scroll up one function** we see that the register **edi** store the VirtualAlloc function.

Press enter or click to view image in full size

In situations like this when we found the call that contains our function we need to check the arguments that it pushes into it for searching our **MZ Header.**

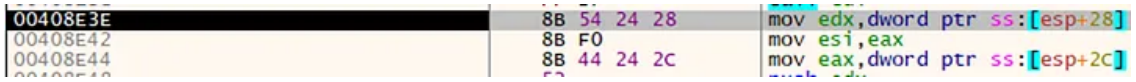
Get Ilan Duhin's stories in your inbox

Join Medium for free to get updates from this writer.

Remember me for faster sign in

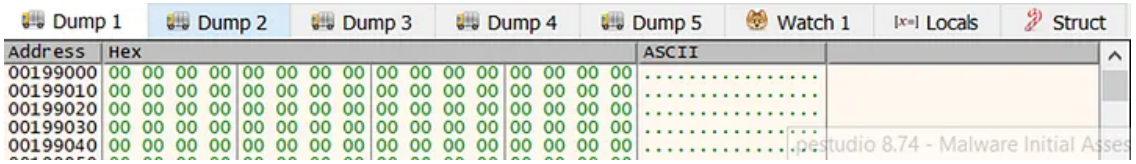
The two arguments we see between the “calls” that used by the function to push them into her are: **[esp+28]** & **[esp+2C].**

Press enter or click to view image in full size



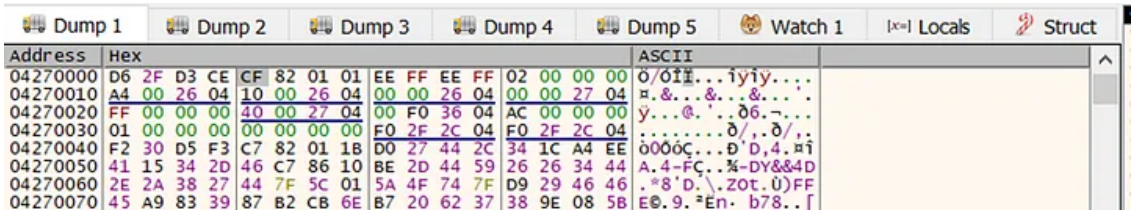
Now we need to check there hex values **of unpacked code** by clicking “follow in dump”. **The first check is empty** (we don’t see any clue about **MZ Header**).

Press enter or click to view image in full size



Also the second one.

Press enter or click to view image in full size



In this situation when we **don’t** find any hex values of unpacked code we need to **Run + Step over** one more time to search for more functions call of VirtualAlloc so we can search there if they have arguments that contain the original unpacked code.

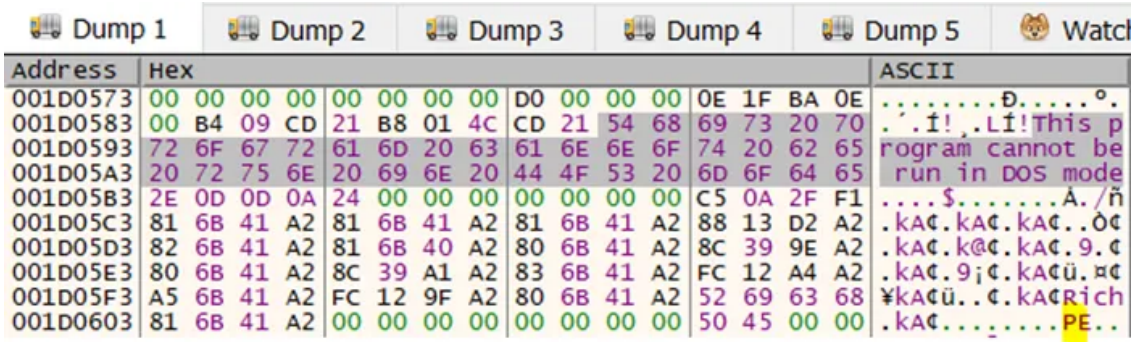
So when we Run again we jumped to the **ret 10** instruction again.

When we press (F8) — step over we jump into the function that calls **ebp** register that contains VirtualAlloc function and a number of arguments we need to explore.

Press enter or click to view image in full size

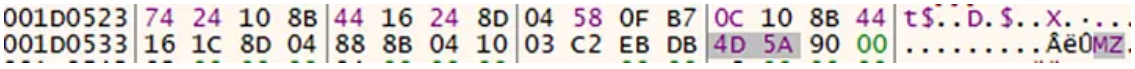
Similar to the first arguments, here we have another one: **[edi+54]**.

Click “follow in dump” and let’s see the results. When we scroll up we see that the hex strings looks like **executable** with description of **“This program cannot run in DOS mode”,** it is perfect for us because every PE header starts like this. **Now what is left to find out is where the MZ.**



Little bit scrolling up and we see the **MZ Header** that is probably the **unpacked code!**

Press enter or click to view image in full size



In this stage of analysis (after finding the unpacked code) we should go to **Memory map** TAB to locate the specific address that contains **Execute permissions** and dump her into **new file**.

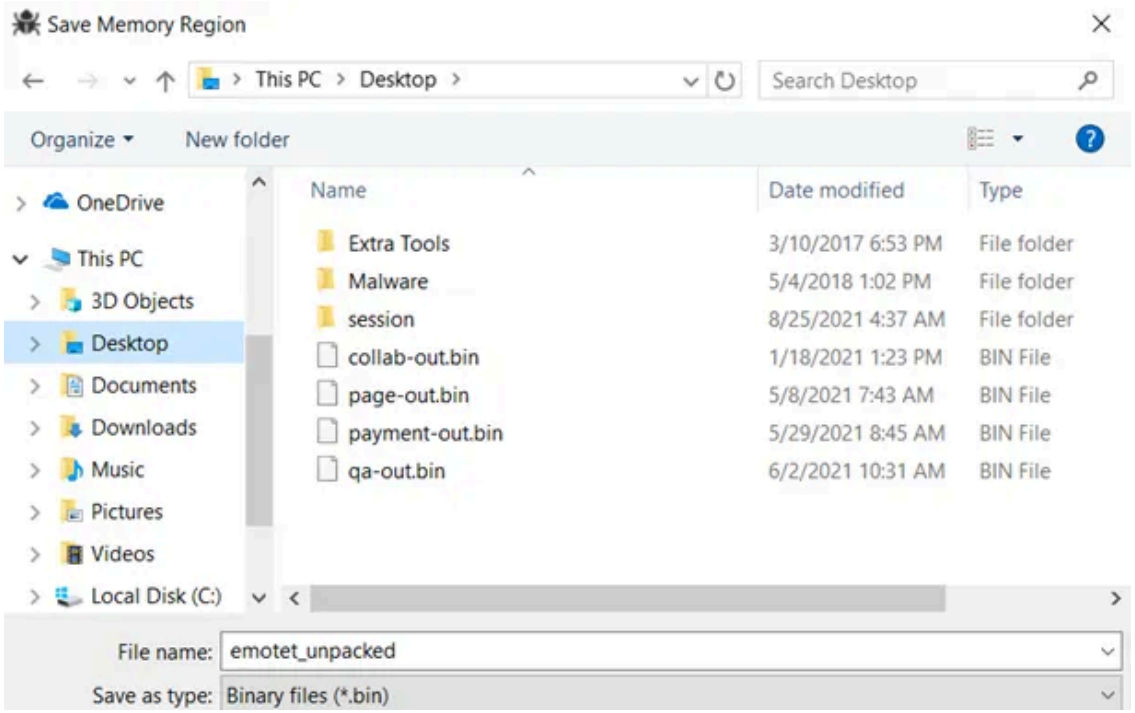
To do this, **right click** on the hex values table **& “follow in memory map”.**

Press enter or click to view image in full size

Its automatically points us to the address that the malware doing it executable capabilities.

All we have left to do is dump the address of unpacked code into new file like I said earlier.

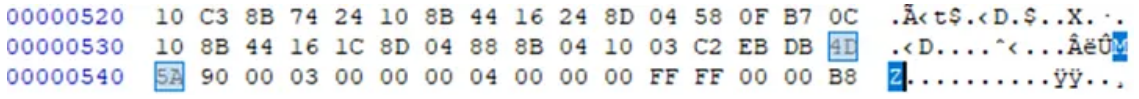
To do this, **right click** on memory address **& “Dump memory to file”.**



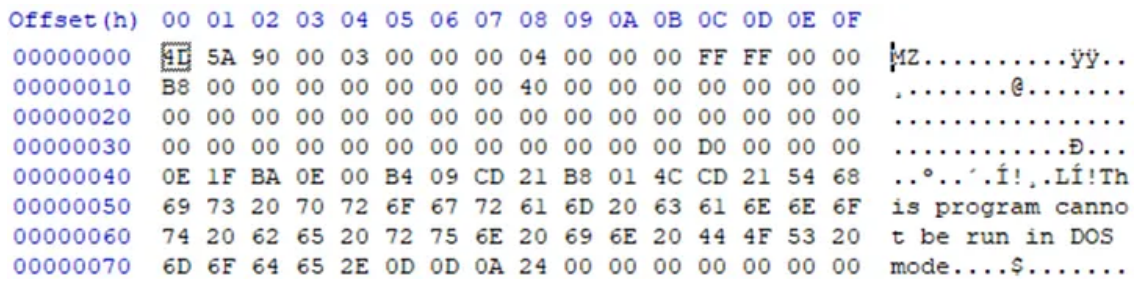
The most fun part for me in unpacking is when you drag the **unpacked file** into **HxD** and clean all the beginning before the **MZ.**

First, we search the MZ string with **Ctrl+F**, when we locate him, we **erase** all strings before him so we can save it into a cleaned **PE File.**

Press enter or click to view image in full size



Press enter or click to view image in full size



Source: https://medium.com/@Ilandu/emotet-unpacking-35bbe2980cfb