Unpacking Remcos malware

muha2xmad.github.io/unpacking/remcos/

January 13, 2022

Muhammad Hasan Ali

Malware Analysis learner

1 minute read

As-salamu Alaykum

Introducton

Remcos is a RAT type malware that attackers use to perform actions on infected machines remotely. This malware is extremely actively caped up to date with updates coming out almost every single month. 1

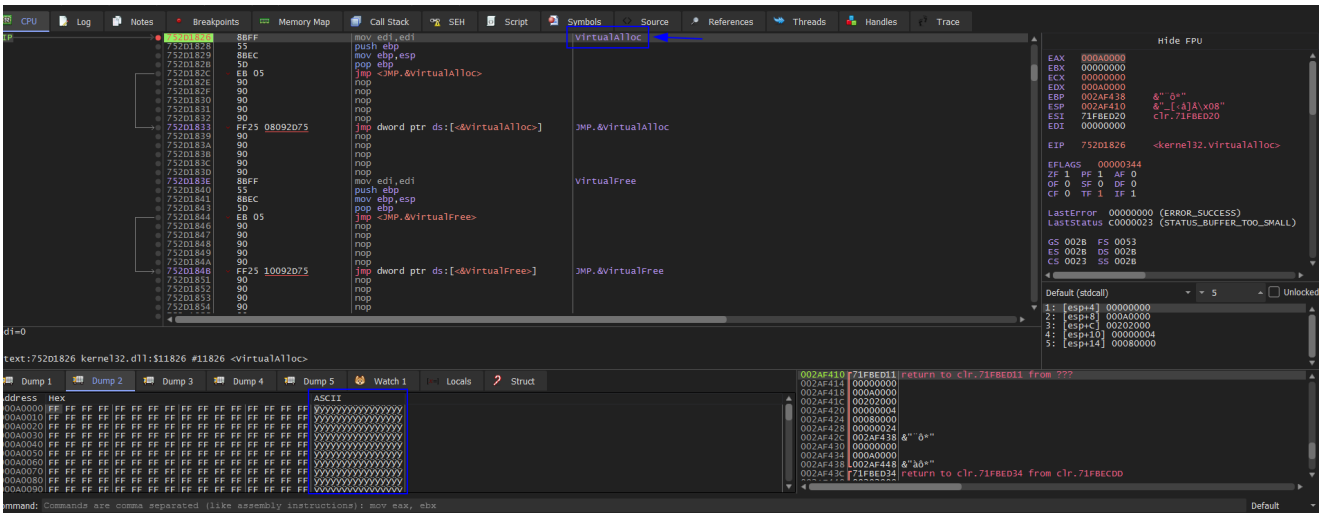
MD5: 5E9770C2B22B03E5726285900AFAB954

Static

Open the sample in `DiE` we see that's a `.NET` executable. It's high `Entropy` then it's packed.

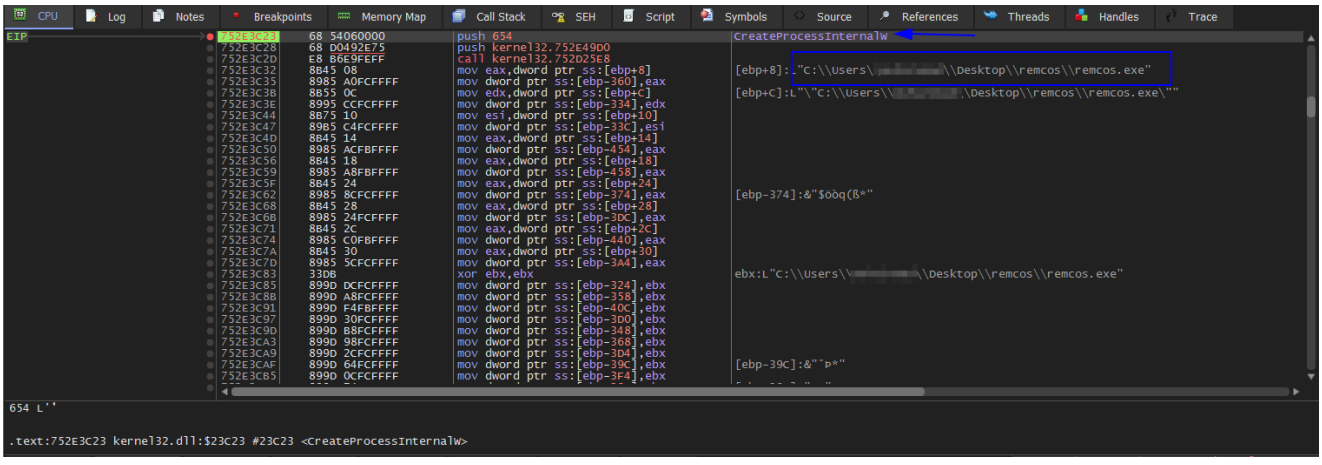
Unpacking process

Drag the sample into `x32dbg` and set BPs at `VirtualAlloc`, `VirtualProtect`, `CreateProcessInternalW`, `IsDebuggerPresent`. Then press `F9` we to hit the first BP which is `IsDebuggerPresent` then `Execute till return` and change `EAX` to `0`. Then run `F9` we hit `VirtualAlloc` and `Execute tille return` and dump `EAX` then check the dump. After many times hitting `VirtualAlloc` BP we notice that it's useless so **disable this BP**.



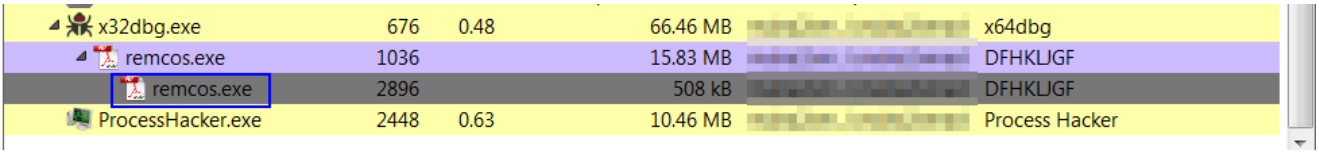
Figure(1):

Then run `F9` to hit `VirtualProtect` BP Which is the same as `VirtualAlloc` **Disable it too**. Then press `F9` to run and hit `IsDebuggerPresent` then `Execute till return` and change `EAX` to `0`. Then press `F9` we get `exception error` ignore it and press `F9` to keep going. We hit `CreateProcessInternalW` BP. Because it's injecting code into an existed or new process. In this case, it will inject a new child process.



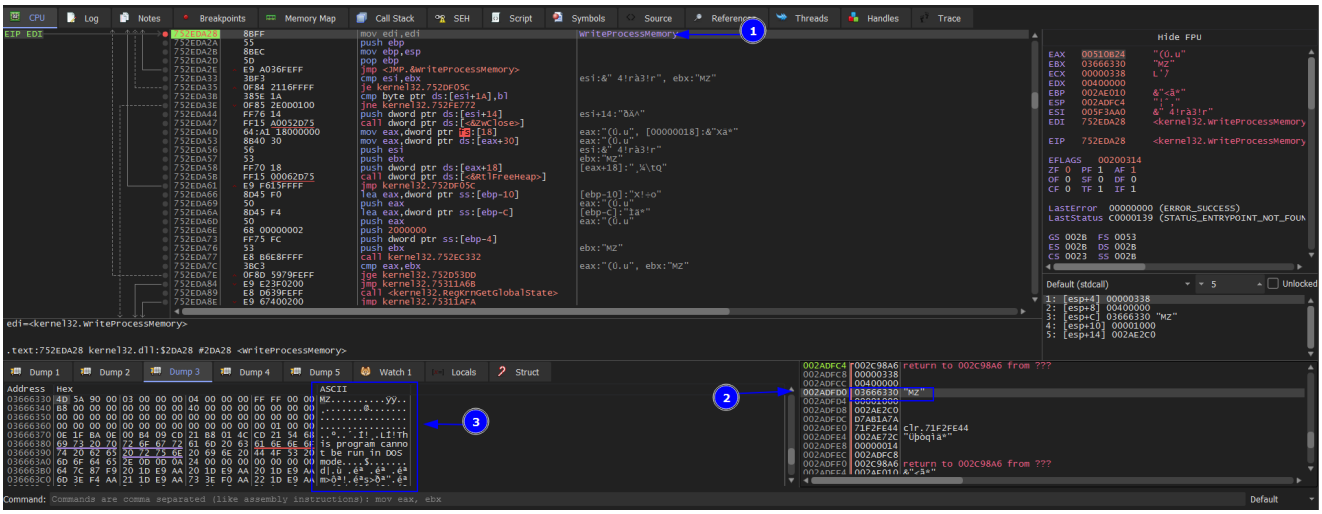
Figure(2):

Then we set `WriteProcessMemory` , and `NtResumeThread` BPs. Beacuase after injecting the process then resume the process from the suspended state. We will unpack it before resuming the process So we don't need the last BP. Press `F9` to hit `WriteProcessMemory` BP. We see the suspended process from `Process Hacker` tool.



Figure(3):

From the documantation of `WriteProcessMemory` the 3rd parameter is `buffer` which holds our unpacked file.



Figure(4):

Then we select from `MZ` to the end of the dump section then `right click` => `Binary` => `Save to a File` . This our unpacked file.

Article quote

> أضئ مصباحك لرُبما دلَّ على الطريق

REF

1- https://any.run/malware-trends/remcos

2- https://www.youtube.com/watch?v=DIH4SvKuktM&t=2s&ab_channel=OALabs

3- WriteProcessMemory