Unpacking Ramnit malware

muha2xmad.github.io/unpacking/ramnit/

January 12, 2022

Muhammad Hasan Ali

Malware Analysis learner

3 minute read

As-salamu Alaykum

Introducton

The Ramnit Trojan is a type of malware able to exfiltrate sensitive data. This kind of data can include anything ranging from banking credentials, FTP passwords, session cookies, and personal data. Leaking this information can easily destroy user trust in a business, and in the process lose customers and ruin reputations. 1

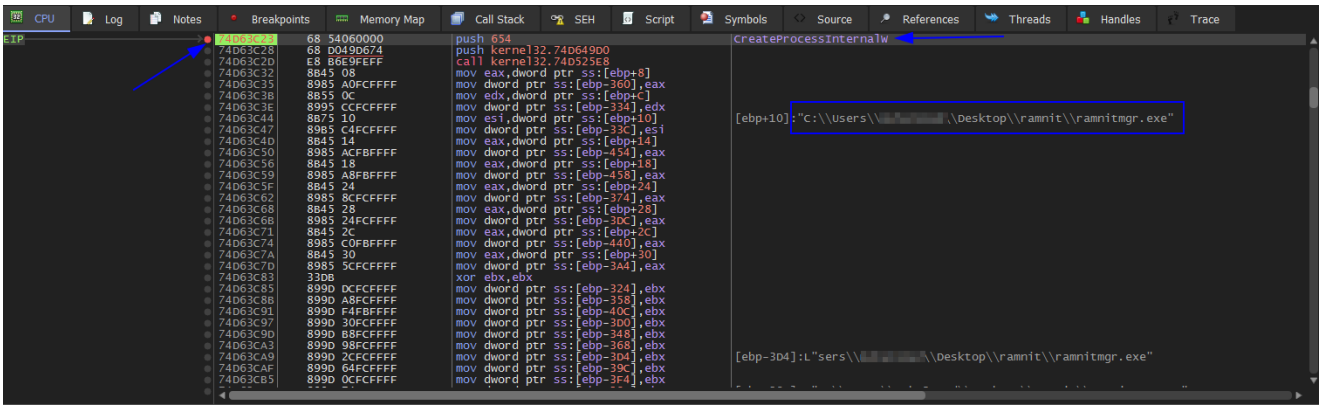
MD5: 6B71498D63E05F83648E6D9A9CEDBF0A

Static

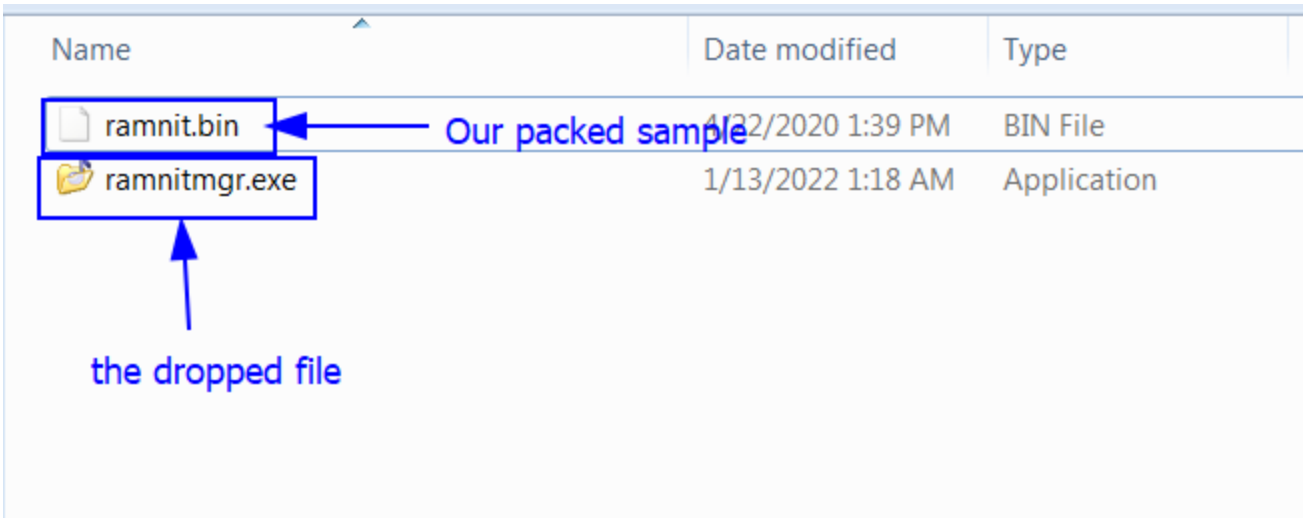
Open the sample in `DiE` we see that it's high `Entropy` and it's packed.

Unpacking process

Drag the sample into `x32dbg` and set BPs at `VirtualAlloc`, `VirtualProtect`, `CreateProcessInternalW`, `IsDebuggerPresent`, `WriteProcessMemory`, and `NtResumeThread`. Then press `F9` we to hit the first BP. As we know that `Ramnit` malware is a dropper, we see that it's dropping a file in the same directory where the sample is being debugged.

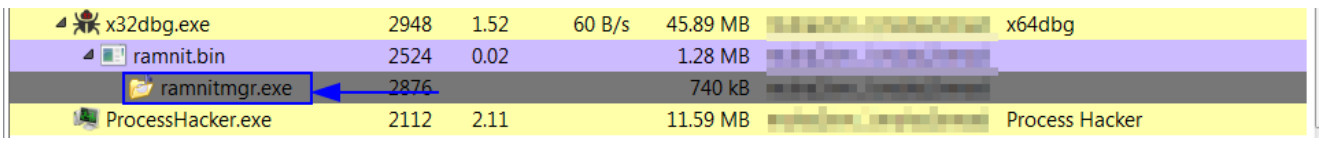


Figure(1):



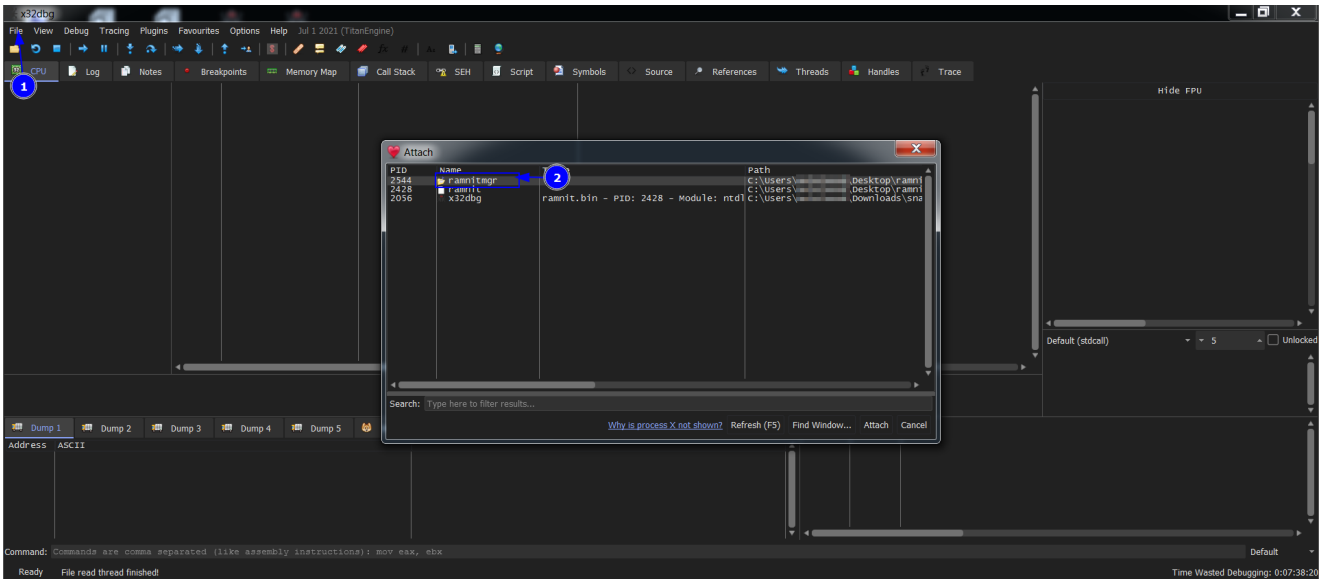
Figure(2):

Then press `F9` now we hit `NtResumeThread` BP now we know that it's injecting unpacking code. If we open `Process Hacker` we see under the `ramnit` process there's a `ramnitmgr.exe` child process which is suspended. The parent process is `ramnit.bin` and the child process is `ramnitmgr.exe`.



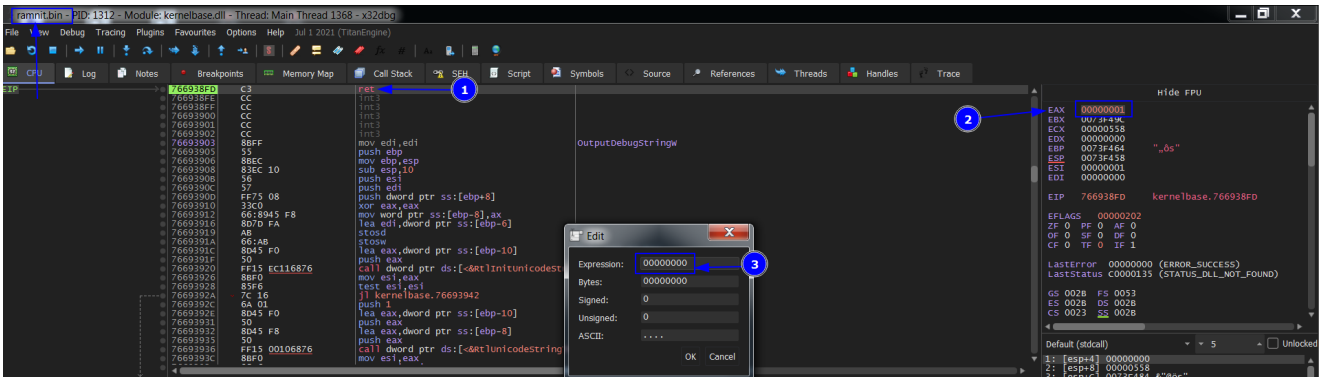
Figure(3):

Now **Don't close the debugger**. Open a new `x32dbg` window the press `file` in the menu then `attach` the child process. Now we have two `x32dbg` windows are opened. Now if we try to set BPs in the debugger of the `child` process it says it's `invalid add` because the process still suspended. To activate go to the debugger of the `parent` process and `run to user code`. Now go to the `child` debugger and set the first 5 BPs as we did above.



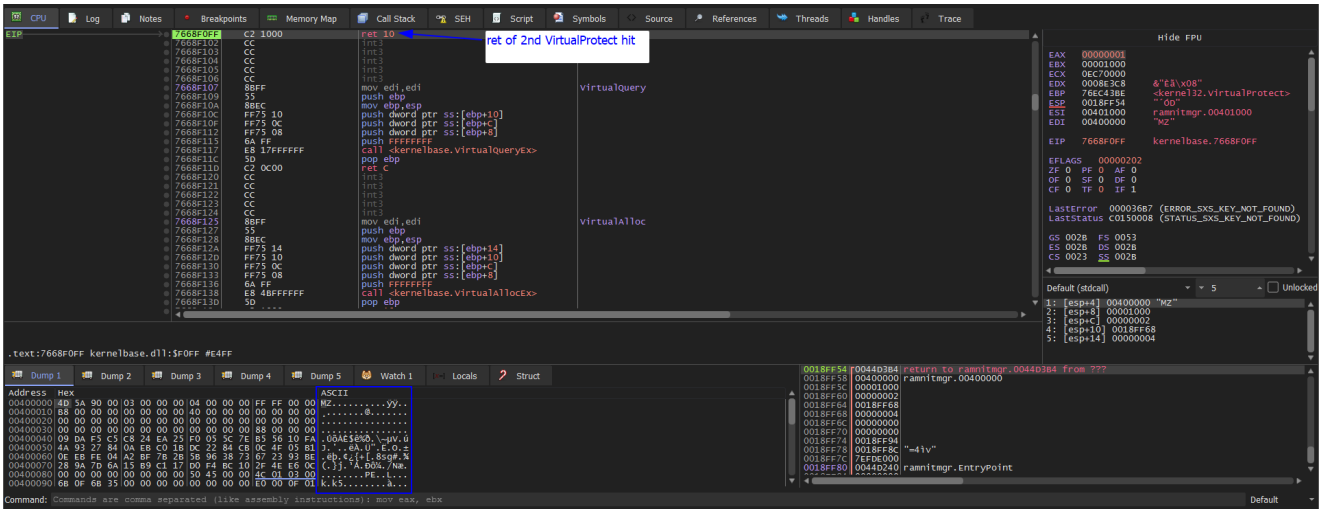
Figure(4):

Return to `Parent` debugger, press `F9` to hit `IsDebuggerPresent` BP, beacause the debugger is present so `EAX` is set to `1` if we continue the debugger will exit and pops up `this is a compiled autoit script`. So we need to change it to `0`. Now `Execute till return` and `double click` on `EAX` and change it to `0`. After that run `F9` again and `IsDebuggerPresent` BP hits do the same and change it to `0` and then run `F9`.



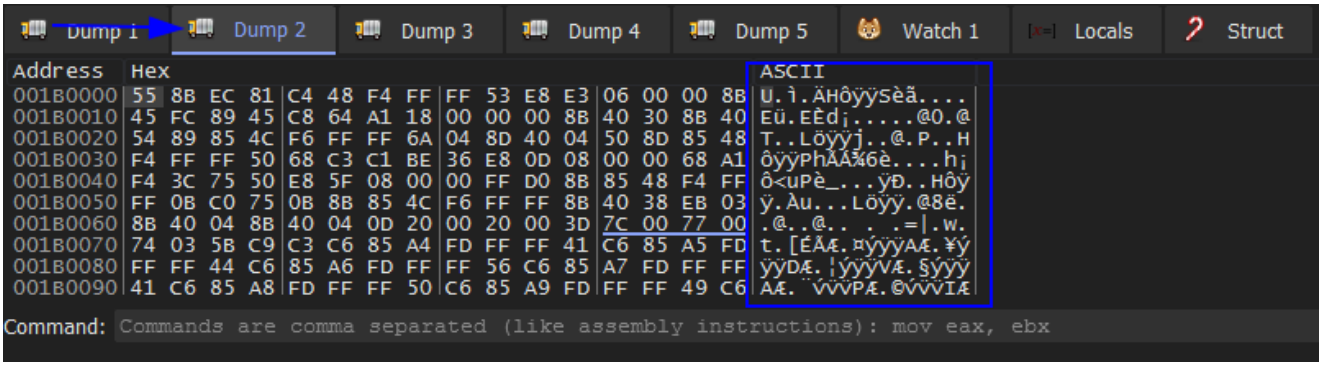
Figure(5):

Now we go back to the `child` process debugger to get the unpacked file. Then run `F9` hits `VirtualProtect` BP then `Execute till return` we see the 2nd parameter points to a location `400000` and change the permission to `RWC` which an indicator of unpacking. Then we dump it we see `MZ` magic byte. Run F9 again we see the same location but changes the permission to `R` which an indicator to finish unpacking. We go and `Follow in Memory map` and save it. **Analyze it then come back it's not our goal.**



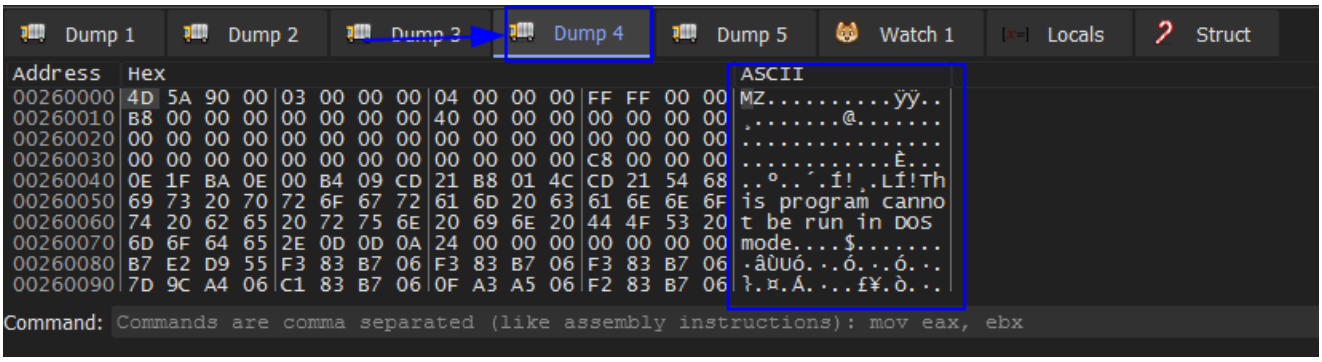
Figure(6):

Now we are back and press `F9` hits `VirtualAlloc` BP and `Execute till return` we see it's allocating memory then dump `EAX` in `dump 2` then press `F9` we see it's unpacking some strange strings in the `dump 2` . Then `Execute till return` and dump `EAX` in `dump 3` then press `F9` we see `dump 3` is empty. Then `Execute till return` and dump `EAX` to `dump 4` . Then run `F9` and chech `dump 4` we see our unpacked file.



Figure(7):

Now we open `Process Hacker` to save our unpacked file which is packed with `UPX` . The OEP might be different to yours. Then unpack `UPX` using `CFF Explorer` tool.



Figure(8):

Article quote

> لن يدومَ الهمُّ يا حلوَ المُحيّا، لن يظلّ الحزنُ في عينيكَ يحيا

REF

1- https://www.cybereason.com/blog/banking-trojan-delivered-by-lolbins-ramnit-trojan

2- https://www.youtube.com/watch?v=l6ZunH6YG0A&ab_channel=GuidedHacking