By: Sachin Verma
contact.vermma7@gmail.com Linkedin:sachin-verma-48715a9a/

# How Emotet Infects a PC

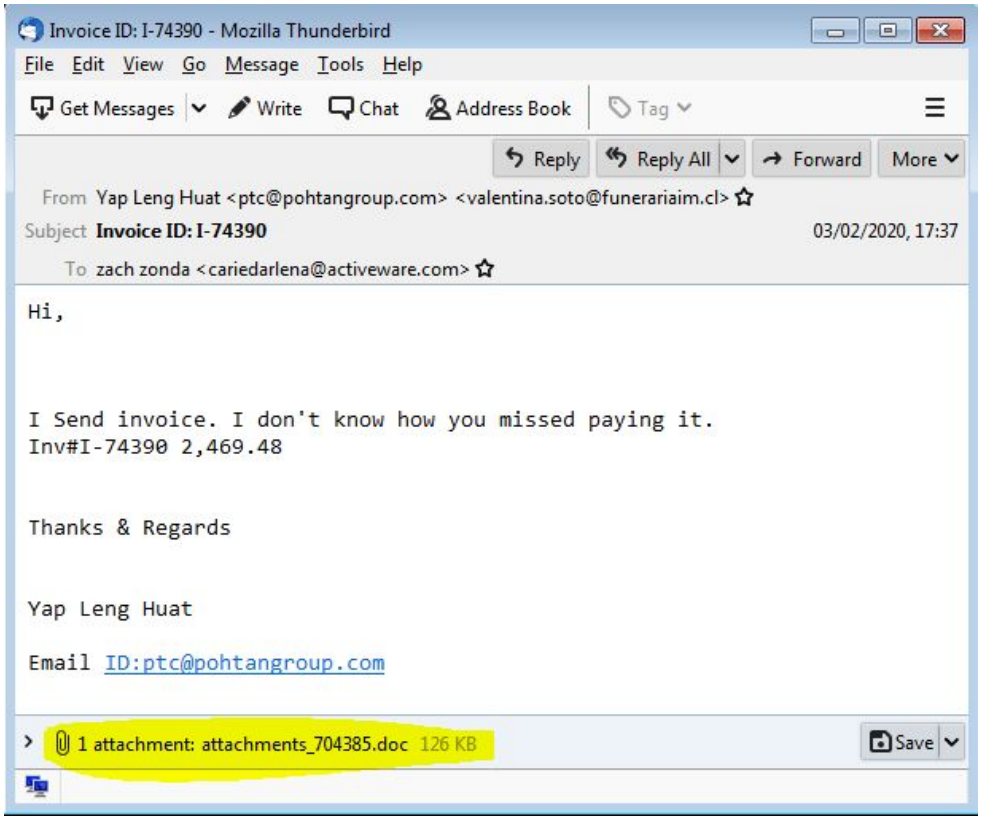
In This Document, we are going to discuss **How Emotet Infects** a PC and a detailed analysis of it.

**What is Emotet?**

Emotet is a banking malware, I think you have heard this quote before, but from where the “banking” term came?
This malware sneaks into your PC and steals your personal information like username, passwords, in the very beginning of its era it is focused on stealing internet banking related information.
Emotet was first encountered in 2014. As it got aged it evolved from just a **banking** trojan to perform many more things.
Now it has the ability to infect the host to send spam email, self upgrading modules, backdoor activity, etc..

**How does it spread?**

It usually got spread by the spam emails, just like in the screenshot below.



By: Sachin Verma
contact.vermma7@gmail.com Linkedin:sachin-verma-48715a9a/

Would you open this invoice, if it comes to your inbox? Maybe you don't, but there are still a huge number of people who are not aware of malicious emails and they download the attachment and open it and that's enough to infect your PC.

**What is in the Attachment?**

Attachment is just a doc file. Do you think it can do any harm to your PC?
Let's figure out what it can do


SHA-1 of the doc file: 0dc994ee4c96f4fcd8f8d4a5b3fadba14f15355e

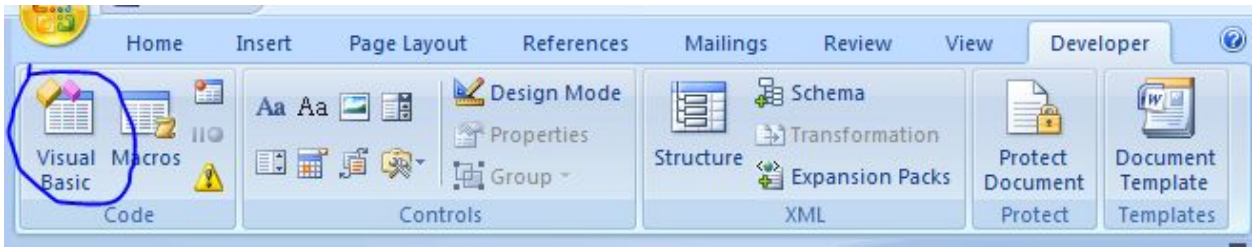

Ah, it is just asking you to enable editing... By enabling the editing you will give it permissions to enable the macros as well.

By: Sachin Verma
contact.vermma7@gmail.com Linkedin:sachin-verma-48715a9a/

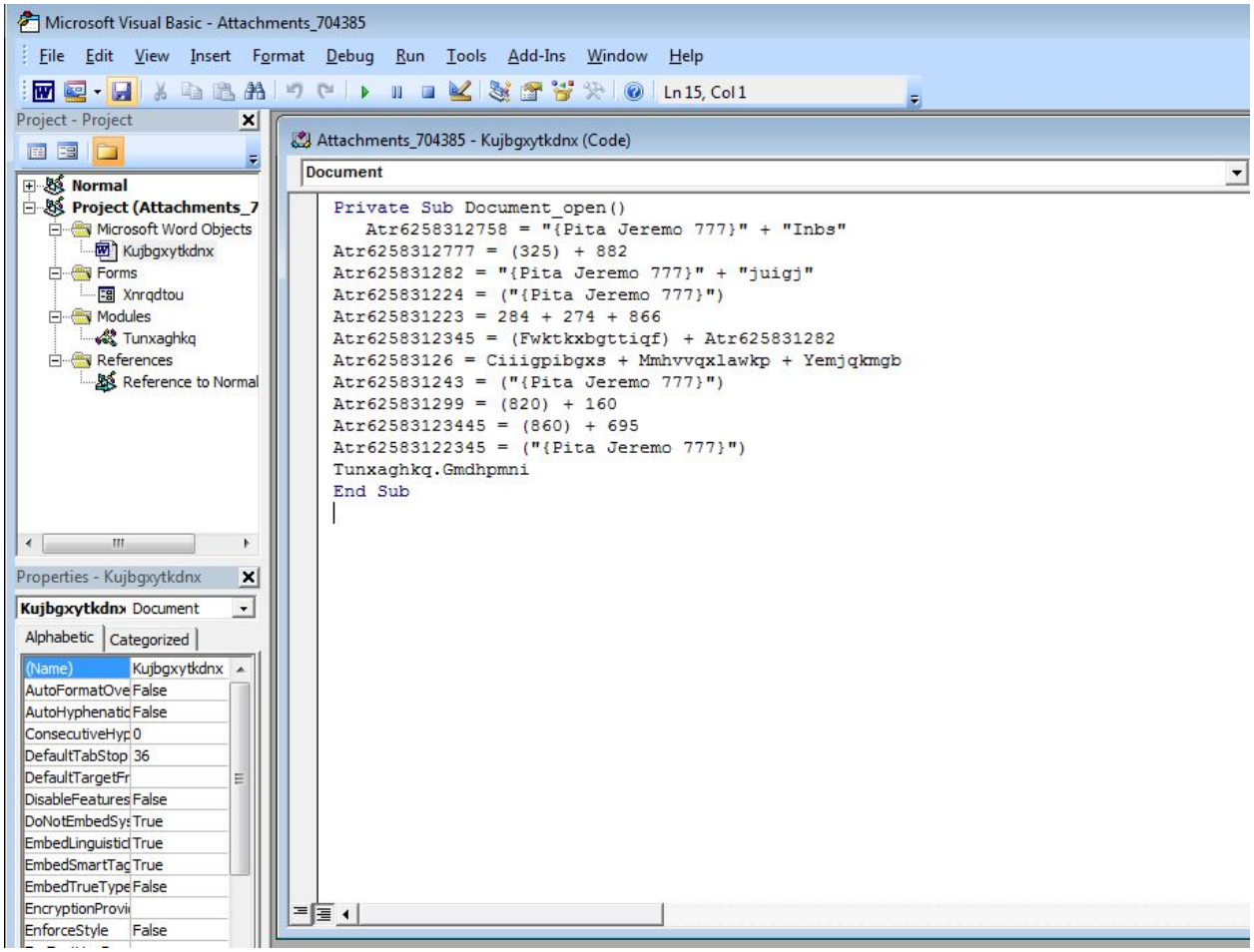
Now, what are macros? : Macros are the piece of program code that enables us to make some daily tasks automate, which can also be used for bad purposes as well… I'll demonstrate it in a minute. ;)

**Let's see what macro looks like.**

Just follow the below screenshot to reach macros
Click on the Developer Tab > Visual Basic.




After clicking the Visual Basic, You will see a screen like below




This is what macro looks like…
But you must be thinking this looks nothing malicious... What is wrong with this??

By: Sachin Verma
contact.vermma7@gmail.com Linkedin:sachin-verma-48715a9a/

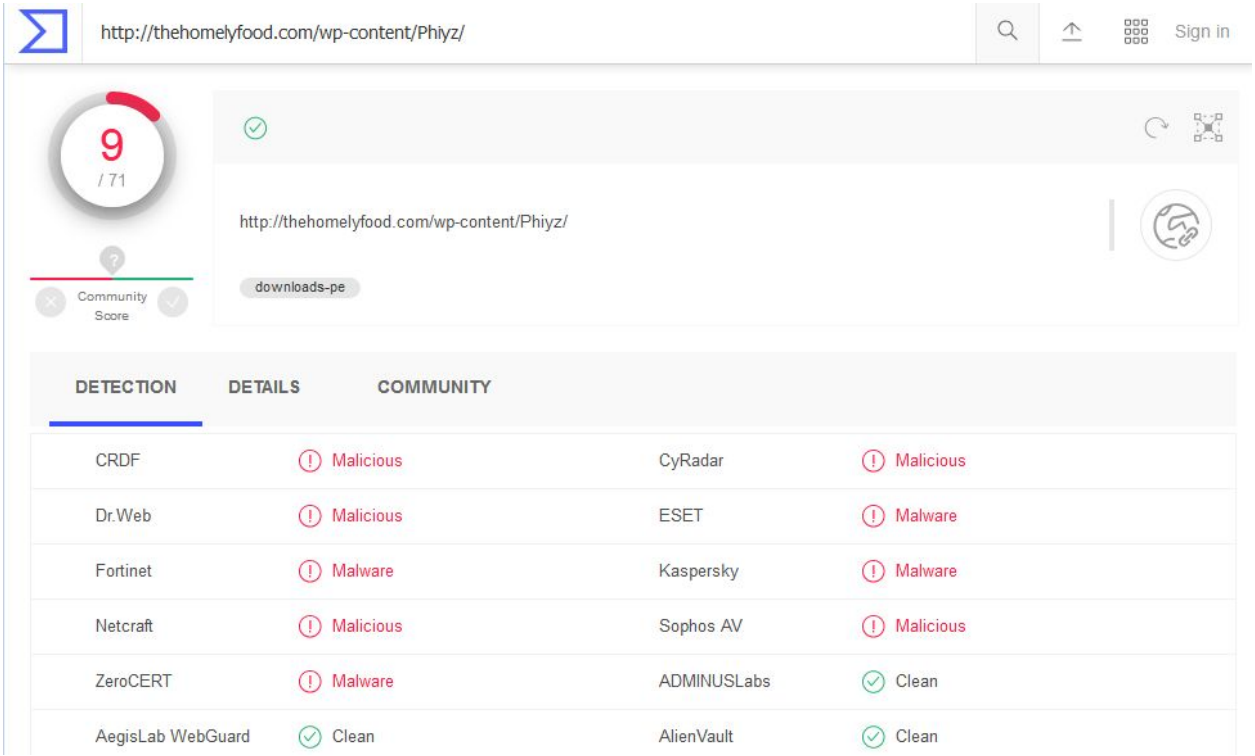
Let me run this doc file. And will show you what it does...
**Note: Just keep up your network monitoring tool if you are trying with me. (i am using fiddler)**

Ah, after executing the document in the safe environment and monitoring its activity, what I saw it is making a connection with 5 URL's
**Note: I just kept my network disabled so nothing malicious can be download**

| | | | | |
|---|---|---|---|---|
| 20 | 502 | HTTP | thehomelyfood.com | /wp-content/Phiyz/ |
| 21 | 502 | HTTP | Tunnel to | cfped-duca.com:443 |
| 22 | 502 | HTTP | Tunnel to | bookdigger.azurewebsites... |
| 23 | 502 | HTTP | wasap.lse.org.ro | /wp-admin/1Dz89/ |
| 24 | 502 | HTTP | furiousfox.in | /wp-content/aR/ |

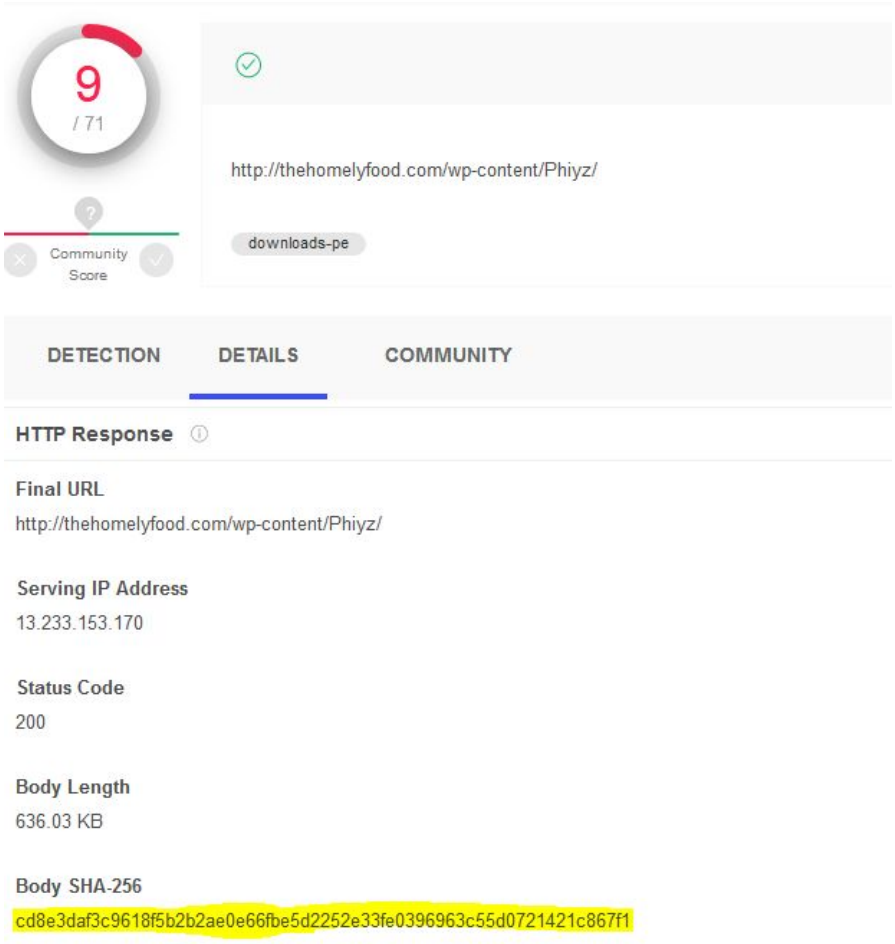
And it is trying to drop its payload in the "c:\user\PCName" folder

But why make connections? Let's check these URLs in the virustotal.com



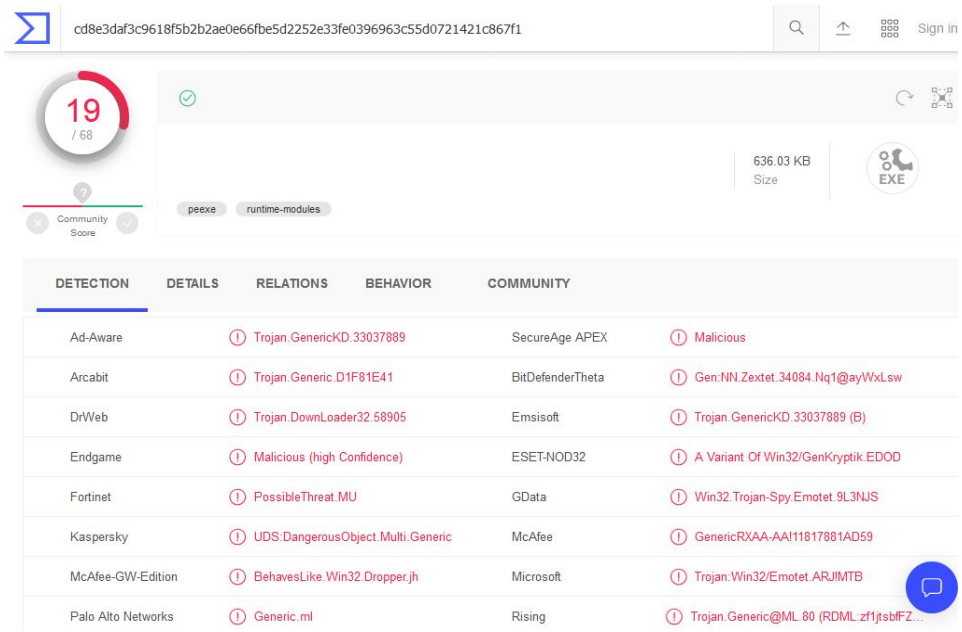

VirusTotal says the URI is malicious, but why? What is it trying to do? Let's check...

By: Sachin Verma
contact.vermma7@gmail.com Linkedin:sachin-verma-48715a9a/




.

By going to its details, I got the SHA-256 of the file which this URL is trying to download, Let's click on this SHA and see what it is.



https://www.virustotal.com/gui/file/cd8e3daf3c9618f5b2b2ae0e66fbe5d2252e33fe0396963c55d0721421c867f1/detection

Oh look, It is getting detected by 19 AV vendors.

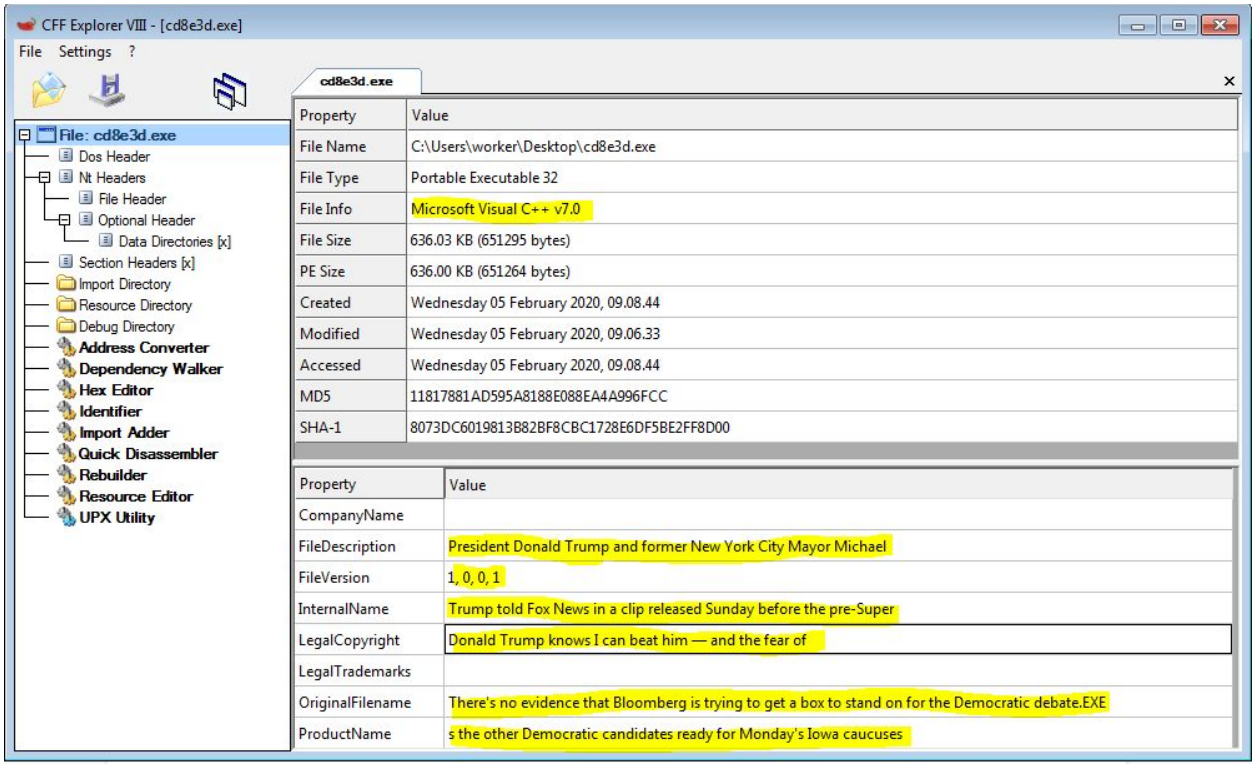
Now it is confirmed that Email which came to us pretending to be an invoice attached is actually a Malware Spam.

Now let's Dig more deeper into the File Downloaded by the Doc file :
SHA-256 : cd8e3daf3c9618f5b2b2ae0e66fbe5d2252e33fe0396963c55d0721421c867f1

**Payload Analysis:**

cd8e3daf3c9618f5b2b2ae0e66fbe5d2252e33fe0396963c55d0721421c867f1

Let's open the file in CFF explorer and see what details we can gather…

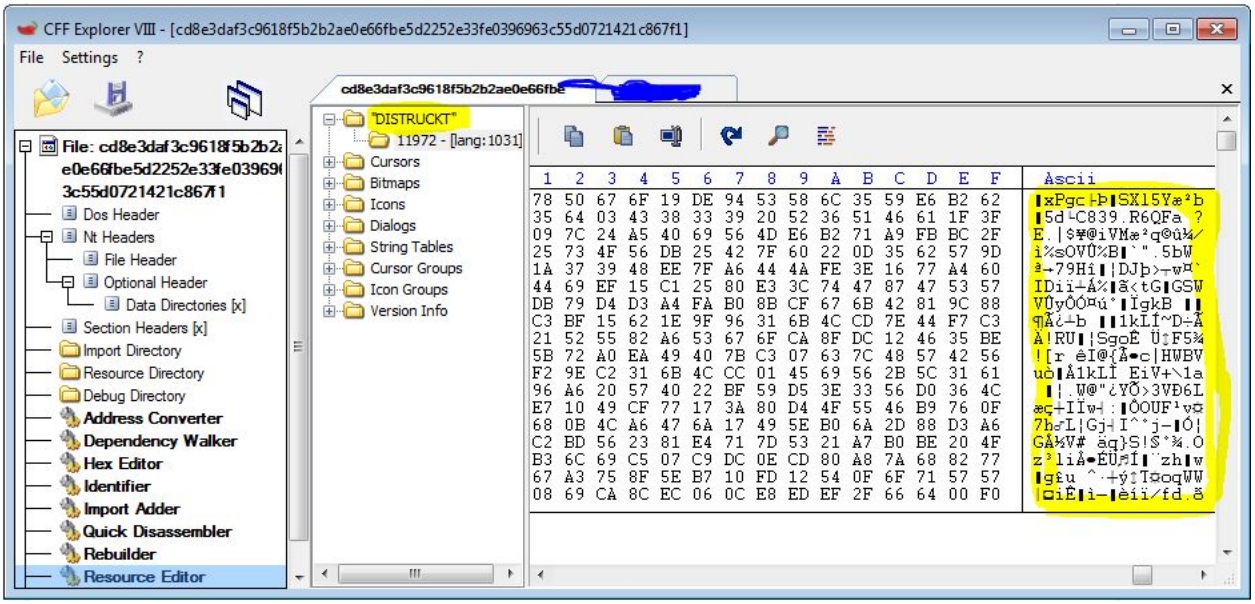



Look at all the highlighted areas in the above screen-shot.

- From file info, we can say it's not packed.
- Doesn't even look like legit file description, some bogus values are entered in there related to Trump.. duh...

By: Sachin Verma
contact.vermma7@gmail.com Linkedin:sachin-verma-48715a9a/

I found something unusual in the Resource editor as well. Check the Screenshot below.




Looking at the highlighted areas, weird “DISTRUKT” Folder in the resource section, and having too much data, the data it looks encrypted as it is so dense.

Maybe this data creates some meaningful stuff after decryption.. Will check this later. (Keep this point in mind)

Let’s check strings, why? Because string analysis can tell us a lot about what the program is capable of, and see what I got… :P

```
87  DISTRUCKT
88  KERNEL32.DLL
89  Fuck Sophos
90  Invalid DateTimeSpan
91  AfxOldWndProc423
```

LOL, it looks like a targeted attack to the SOPHOS, Lets see what else we have..

```
501  GetEnvironmentVariableA
502  GetEnvironmentVariableW
503  GetStringTypeExA
504  GetStringTypeExW
505  GetProcAddress
506  GetModuleHandleA

597  VirtualProtect
598  VirtualAlloc
599  GetSystemInfo

677  SetCursor
678  GetKeyState

730  GetWindowTextA

742  SetWindowsHookExA
```

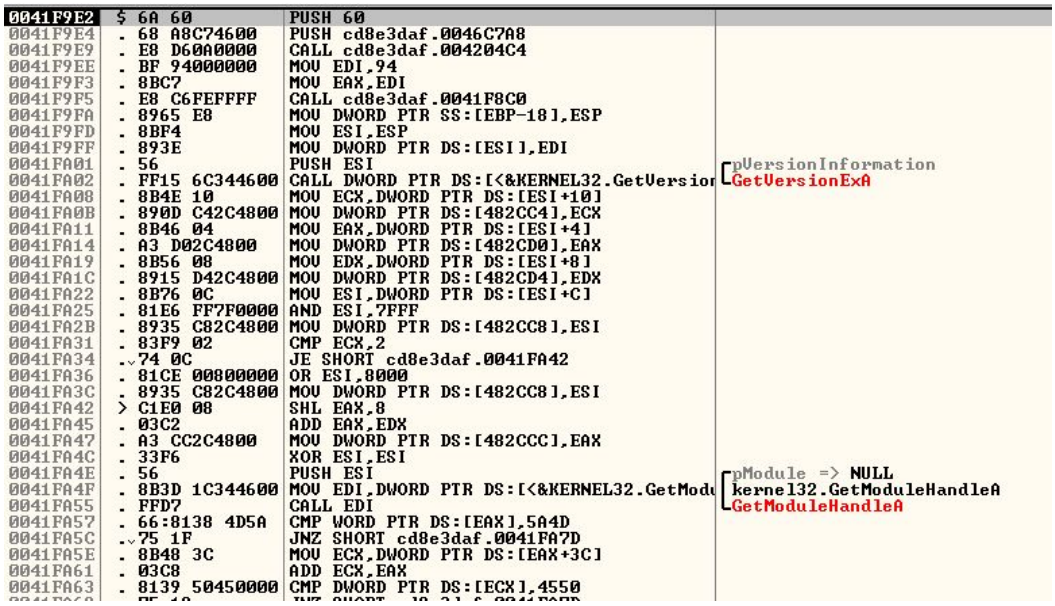
It does have many more suspicious API calls.

*Maybe if you're thinking how to extract strings from this file then follow below process:*
***Download Strings v2.53 from here:*** *https://docs.microsoft.com/en-us/sysinternals/downloads/strings*

***Use this Command:*** *strings -n 8 YourFileName.exe*

**Let's start debugging in the OLLyDbg**

I have loaded the File in OLLyDbg. I am on the Entry point of the file.




Before stepping over, Let's collaborate what information we have gathered above.

- We found a weird-looking encrypted file in the Resource section "DISTRUKT".
- It is using VirtualAlloc and VirtualProtect.
- Having some spy related modules like SetWindowHook ,GetWindowText, GetKeyState, GetSystemInfo.

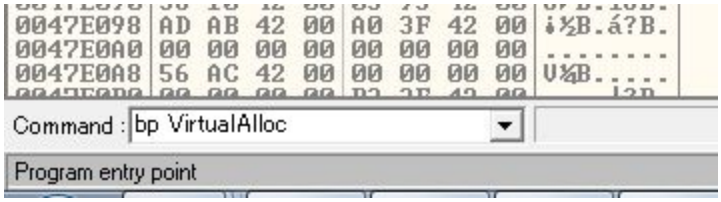
let's set some precautionary **breakpoints**, These breakpoints are totally dependent on our above analysis.

**The BreakPoint on VirtualAlloc:**

- VirtualAlloc is helpful because it returns newly created regions in memory in register EAX.
- And I think that our malware is trying to allocate memory regions to encrypted files inside .rsrc "DISTRUKT" and then it will decrypt the file.
- If we use a breakpoint on that, it will stop while allocating the memory and we can further analyze that allocated memory.
  Note * VirtualAlloc simply allocates memory not populate it.

By: Sachin Verma
contact.vermma7@gmail.com Linkedin:sachin-verma-48715a9a/

Setting breakpoint on VirtualAlloc:

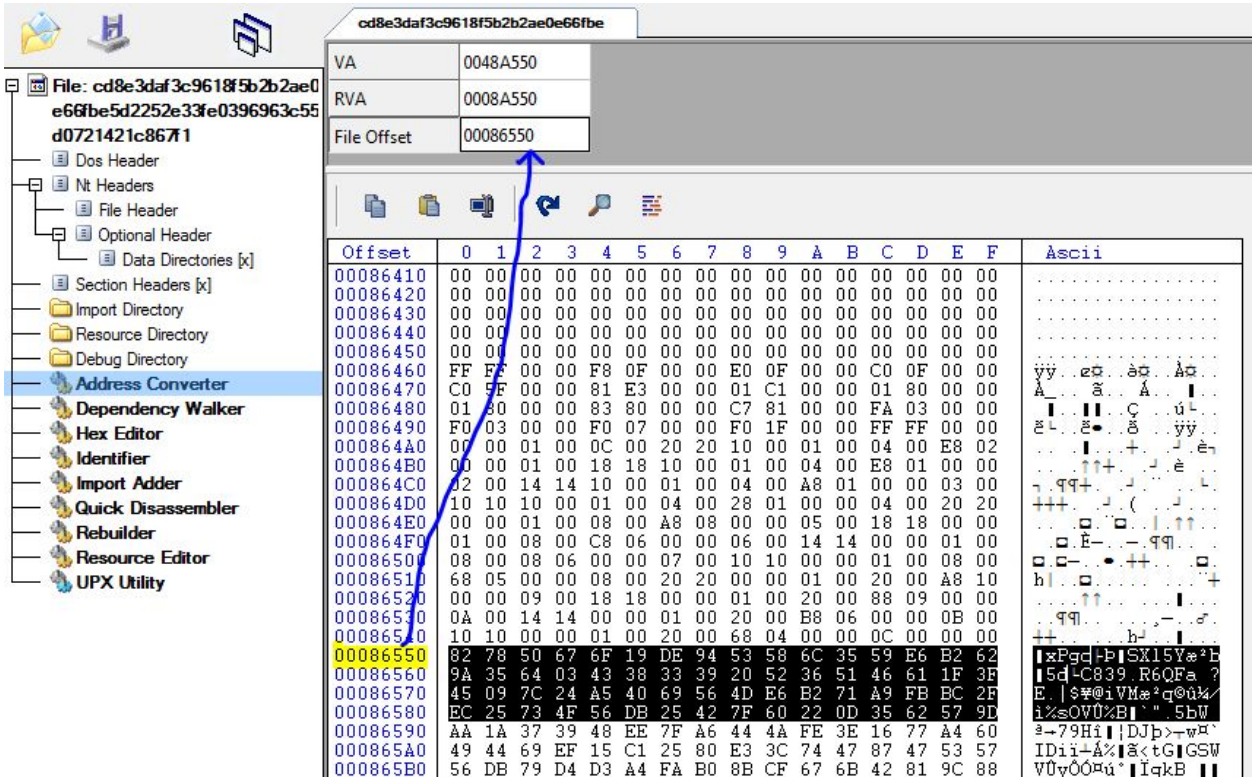



Press Enter after typing “Bp VirtualAlloc” into the command box.

**The breakpoint on .rsrc memory region:**

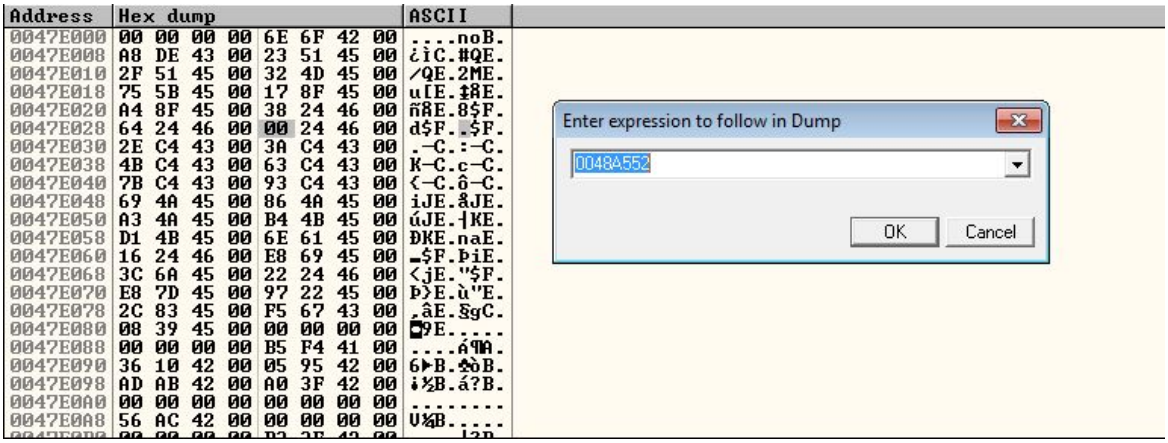
- We are going to set Hardware on access breakpoint on the memory location which I told you to Keep point in mind
- Because if it is going to allocate new memory for data in .rsrc, then it will surely access the .rsrc section to copy on the new location, at that point our Hardware on Access will give a pause to the program for analysis.

For setting the hardware breakpoint we have to first find the memory location address of .rsrc, Follow the Screenshot for that.

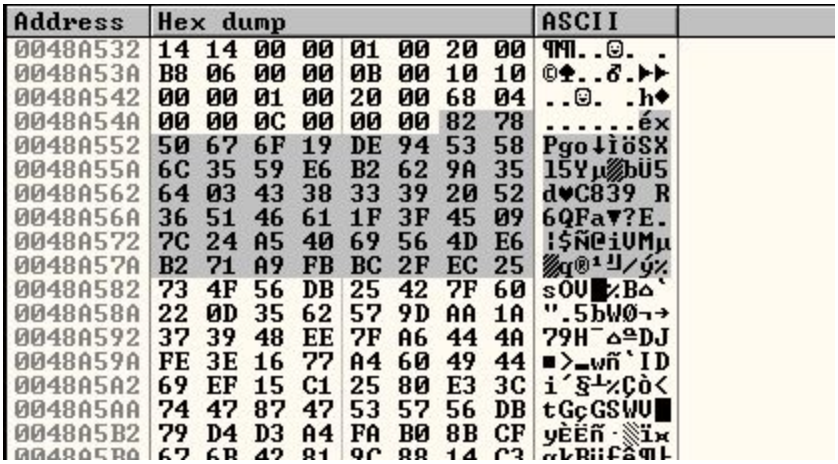



- Just take the offset of the the memory location which we looks like encrypted data in.rsrc and put it into the above converter, it will give us the VA and RVA of the file.

- Now we have VA(virtual address) of the address “0048A550” no. we have to go back to Olly in which our program already loaded.
- Press the shortcut CTRL+G and pop will appear like below, enter the memory location “0048A550” in that, and press OK

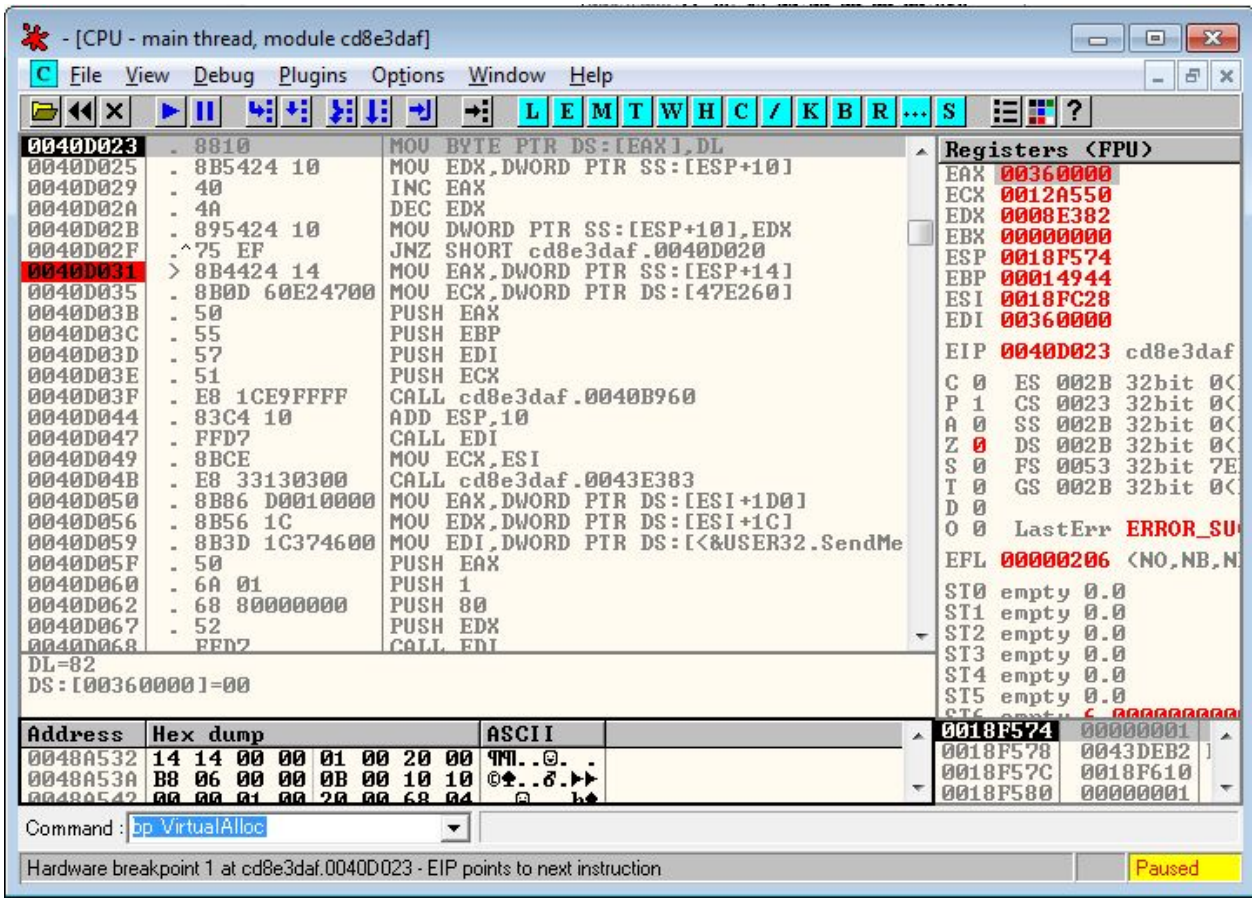



- Now you reached to the memory address ”0048A550” and select some area, and now set a Hardware On-access Breakpoint by Right click > Breakpoint > Hardware, On Access > Dword

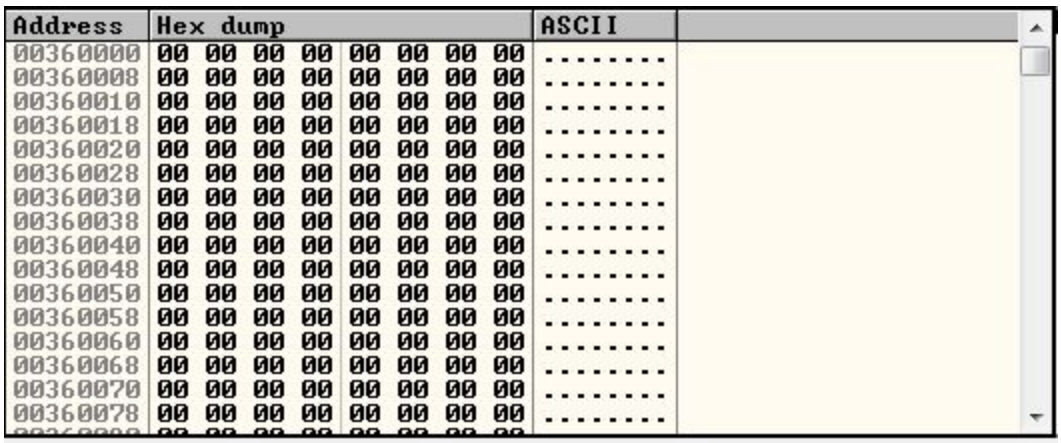



Now we set the both of the breakpoints, now we will cross our fingers and press F9.

Ah, small success, we reach the hardware breakpoint:



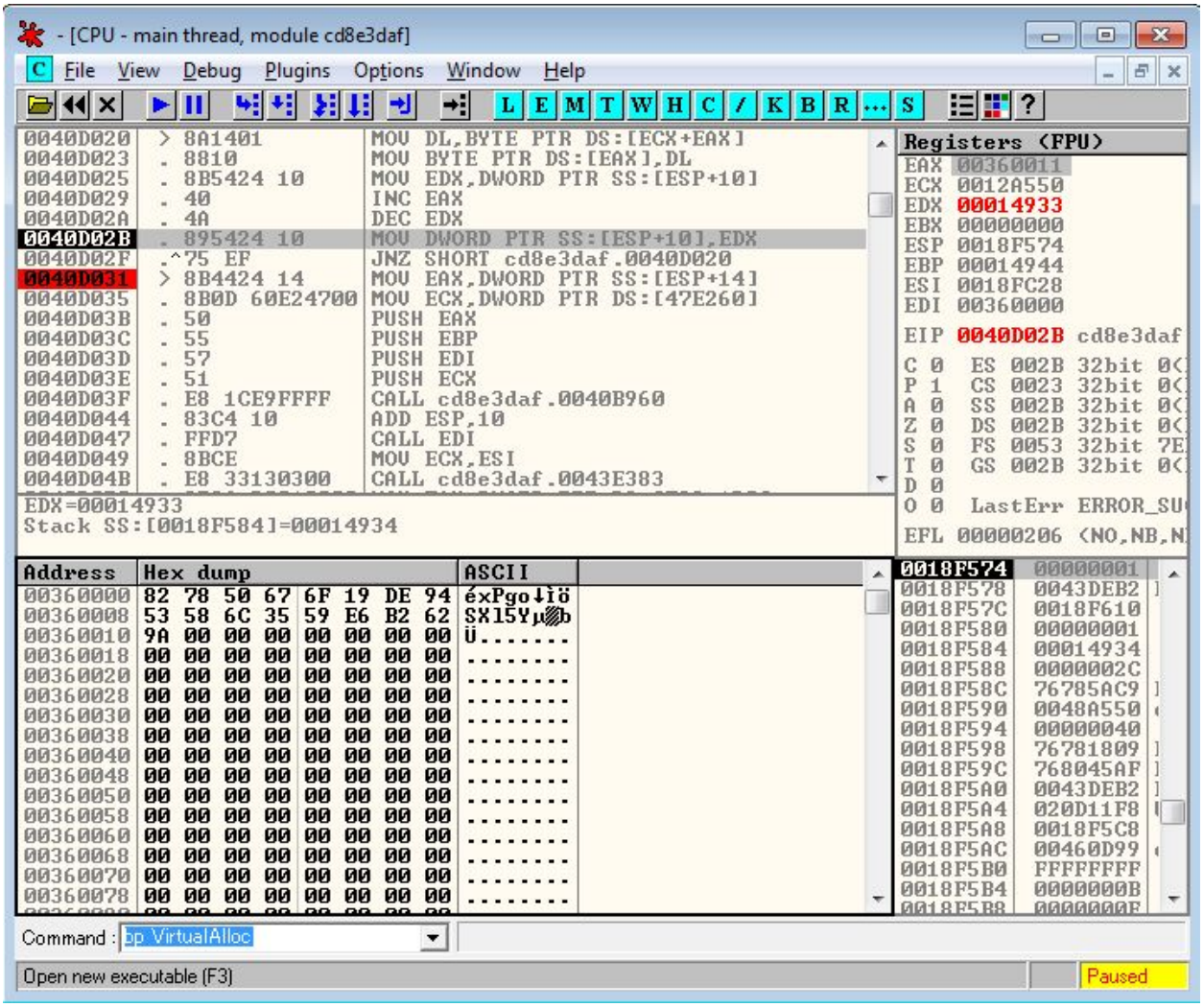

We got the allocated memory location in EAX “00360000”, let’s follow that location in the dump.




See the allocated memory is empty. Because encrypted data in .rsrc did not start copying yet. Keep Pressing F8 you’ll see data getting copied to the allocated memory.

After pressing F8 a couple of times, we see data getting copied, let’s set breakpoint outside the loop and press F9 to get the full dump.

By: Sachin Verma
contact.vermma7@gmail.com Linkedin:sachin-verma-48715a9a/



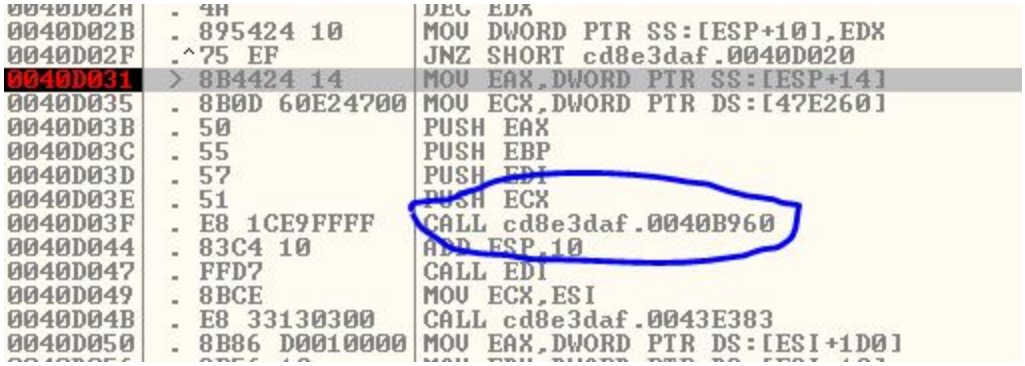

After pressing F9 it gave me whole data transferred.

Please mind the Address changes in next screenshot because I have restarted the program:

00360000 >to> 002F0000

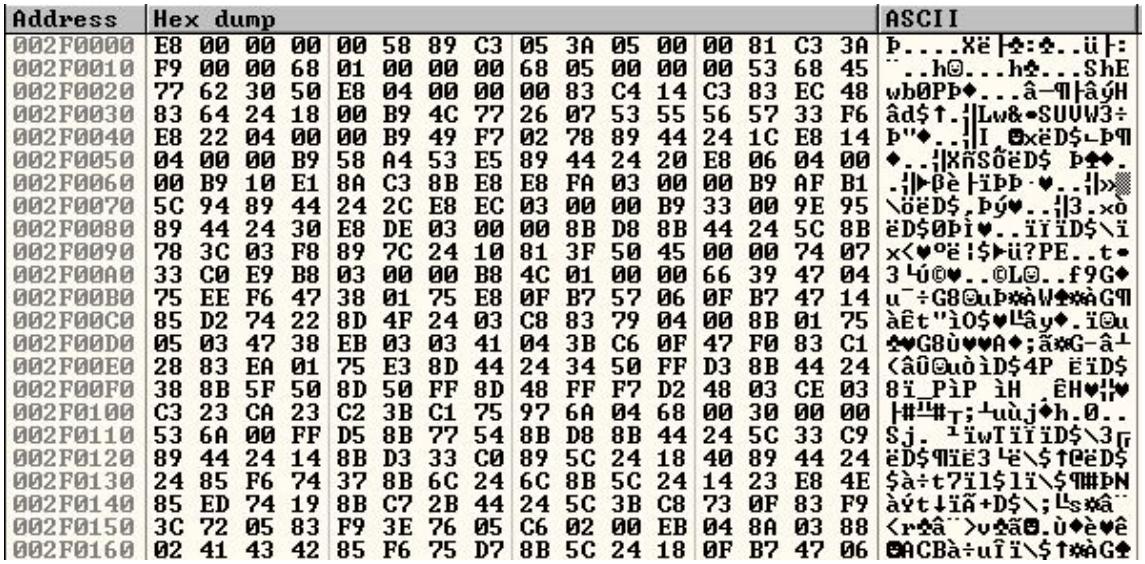
| Address | Hex dump | | | | | | | | | | | | | | | | ASCII |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 002F0000 | 82 | 78 | 50 | 67 | 6F | 19 | DE | 94 | 53 | 58 | 6C | 35 | 59 | E6 | B2 | 62 | éxPgo↓ÌöSX15Yµb |
| 002F0010 | 9A | 35 | 64 | 03 | 43 | 38 | 33 | 39 | 20 | 52 | 36 | 51 | 46 | 61 | 1F | 3F | Ü5d♥C839 R6QFa▼? |
| 002F0020 | 45 | 09 | 7C | 24 | A5 | 40 | 69 | 56 | 4D | E6 | B2 | 71 | A9 | FB | BC | 2F | E.¦$Ñ@iVMµ▒q®¹¼/ |
| 002F0030 | EC | 25 | 73 | 4F | 56 | DB | 25 | 42 | 7F | 60 | 22 | 0D | 35 | 62 | 57 | 9D | ý%sOV▒%Bà`".5bW¥ |
| 002F0040 | AA | 1A | 37 | 39 | 48 | EE | 7F | A6 | 44 | 4A | FE | 3E | 16 | 77 | A4 | 60 | ¬→79H¯▵ºDJ■>▂wñ` |
| 002F0050 | 49 | 44 | 69 | EF | 15 | C1 | 25 | 80 | E3 | 3C | 74 | 47 | 87 | 47 | 53 | 57 | IDi´§½Çù<tGçGSW |
| 002F0060 | 56 | DB | 79 | D4 | D3 | A4 | FA | B0 | 8B | CF | 67 | 6B | 42 | 81 | 9C | 88 | V▒yÈÉñ·▒ıxgkBüÉê |
| 002F0070 | 14 | C3 | BF | 15 | 62 | 1E | 9F | 96 | 31 | 6B | 4C | CD | 7E | 44 | F7 | C3 | ¶├┐§b▲fû1kL=^D ├ |
| 002F0080 | C4 | 21 | 52 | 55 | 82 | A6 | 53 | 67 | 6F | CA | 8F | DC | 12 | 46 | 35 | BE | −‼RUéªSgo╩Ñ▄↕F5¼ |
| 002F0090 | 21 | 5B | 72 | A0 | EA | 49 | 40 | 7B | C3 | 07 | 63 | 7C | 48 | 57 | 42 | 56 | ![ráûI@{├•c¦HWBV |
| 002F00A0 | 75 | F2 | 9E | C2 | 31 | 6B | 4C | CC | 01 | 45 | 69 | 56 | 2B | 5C | 31 | 61 | u=x┬1kL╠☺EiV+\1a |
| 002F00B0 | 1F | 96 | A6 | 20 | 57 | 40 | 22 | BF | 59 | D5 | 3E | 33 | 56 | D0 | 36 | 4C | ▼û ª W@"¸Y¹>3VÐ6L |
| 002F00C0 | E6 | E7 | 10 | 49 | CF | 77 | 17 | 3A | 80 | D4 | 4F | 55 | 46 | B9 | 76 | 0F | µÞ►Ixw‡:ÇÈOUF╣v☼ |
| 002F00D0 | 37 | 68 | 0B | 4C | A6 | 47 | 6A | 17 | 49 | 5E | B0 | 6A | 2D | 88 | D3 | A6 | 7h♂Lª Gj‡I^▒j-êÉª |
| 002F00E0 | 47 | C2 | BD | 56 | 23 | 81 | E4 | 71 | 7D | 53 | 21 | A7 | B0 | BE | 20 | 4F | G┬½V#üäq}S!°▒¥ O |
| 002F00F0 | 7A | B3 | 6C | 69 | C5 | 07 | C9 | DC | 0E | CD | 80 | A8 | 7A | 68 | 82 | 77 | z│li┼•┌▄Ð╞Ç¿zhéw |
| 002F0100 | 8E | 67 | A3 | 75 | 8F | 5E | B7 | 10 | FD | 12 | 54 | 0F | 6F | 71 | 57 | 57 | ägúuÅ^·▲►²‡Ï¤oqWW |
| 002F0110 | 05 | 08 | 69 | CA | 8C | EC | 06 | 0C | E8 | ED | EF | 2F | 66 | 64 | 00 | F0 | ♣◘iʲ¼îý♦.bý´/fd.- |
| 002F0120 | C1 | 13 | 12 | 45 | CD | E1 | 44 | BA | BB | 37 | 68 | 6C | 0D | CD | 2D | 72 | ┴‼‡E=ÐD╢╗7hl.=-r |
| 002F0130 | 69 | E0 | 80 | 11 | 5D | F3 | 3C | 43 | 03 | CA | 0B | 73 | 42 | 41 | 81 | 7B | ióÇ◄]¾<C♥╩ßsBAü{ |
| 002F0140 | DC | 8A | 05 | 41 | E8 | F2 | 4F | 2F | 66 | 64 | 08 | F1 | 3B | 58 | B5 | A8 | ▄è♣AÞ=O/fd◘±;X¿¿ |
| 002F0150 | 7A | 40 | 72 | F9 | CB | 55 | 3A | 71 | 8B | 46 | 69 | BD | 49 | EF | 75 | ED | z@rˉ╦U:qïFi¢Iˊuý |
| 002F0160 | 68 | 39 | 13 | 25 | EA | B7 | 22 | 80 | DD | 3E | 4D | 2D | 56 | D0 | 36 | 5E | h9‼%Uà"Ç!>M-VÐ6^ |
| 002F0170 | 6C | 82 | 2B | 7F | C7 | F8 | 47 | 01 | CB | 90 | 1A | 52 | 89 | B9 | 0B | 5E | lé+⌂Å°GÇ╕Ê→R빂♂^ |
| 002F0180 | 6E | E0 | 1D | 8C | 05 | CF | 58 | 55 | 9E | EE | 1F | 99 | 69 | 8F | D9 | 23 | nó↔î♣×XU× ▼Öiß┘# |
| 002F0190 | 4B | 1D | D2 | BA | 22 | 6D | E3 | 33 | D1 | 65 | 33 | 1E | E0 | D8 | 65 | 1E | K↔Ê‖"mô3Ðe3▲óÏe▲ |
| 002F01A0 | B7 | B3 | 77 | 1D | 14 | D4 | F7 | 79 | C3 | F2 | 02 | AF | B9 | 17 | 68 | 64 | à|w↔¶Ê.y╞=☻»╣‡hd |
| 002F01B0 | C6 | F3 | E9 | 56 | 4D | 65 | 75 | 96 | E3 | 0C | 74 | 73 | E4 | 07 | 5B | D2 | ã▒ÚVMeuûô.tsõ•[Ê |
| 002F01C0 | 96 | 16 | 14 | 36 | 9A | 37 | 8E | 0C | 47 | 15 | EF | 05 | 52 | B3 | CB | B2 | û▂¶6Ü7ä.G§´ªR|╦▒ |
| 002F01D0 | 4E | 54 | DD | 52 | 85 | BB | 33 | 5E | 6E | E8 | 31 | 74 | 4D | 30 | 26 | DD | NT¦Rà╗3^nÞ1tM0&¦ |
| 002F01E0 | 39 | 41 | 56 | EE | 62 | FD | 99 | 13 | 71 | 38 | 4B | DC | 11 | 5E | 66 | 82 | 9AV¯b²ö‼q8K▄◄^fé |

Now Press F8 until you reach the call.



```
0040D02B   . 895424 10      MOV DWORD PTR SS:[ESP+10],EDX
0040D02F   .^75 EF          JNZ SHORT cd8e3daf.0040D020
0040D031   > 8B4424 14      MOV EAX,DWORD PTR SS:[ESP+14]
0040D035   . 8B0D 60E24700  MOV ECX,DWORD PTR DS:[47E260]
0040D03B   . 50             PUSH EAX
0040D03C   . 55             PUSH EBP
0040D03D   . 57             PUSH EDI
0040D03E   . 51             PUSH ECX
0040D03F   . E8 1CE9FFFF    CALL cd8e3daf.0040B960
0040D044   . 83C4 10        ADD ESP,10
0040D047   . FFD7           CALL EDI
0040D049   . 8BCE           MOV ECX,ESI
0040D04B   . E8 33130300    CALL cd8e3daf.0043E383
0040D050   . 8B86 D0010000  MOV EAX,DWORD PTR DS:[ESI+1D0]
```

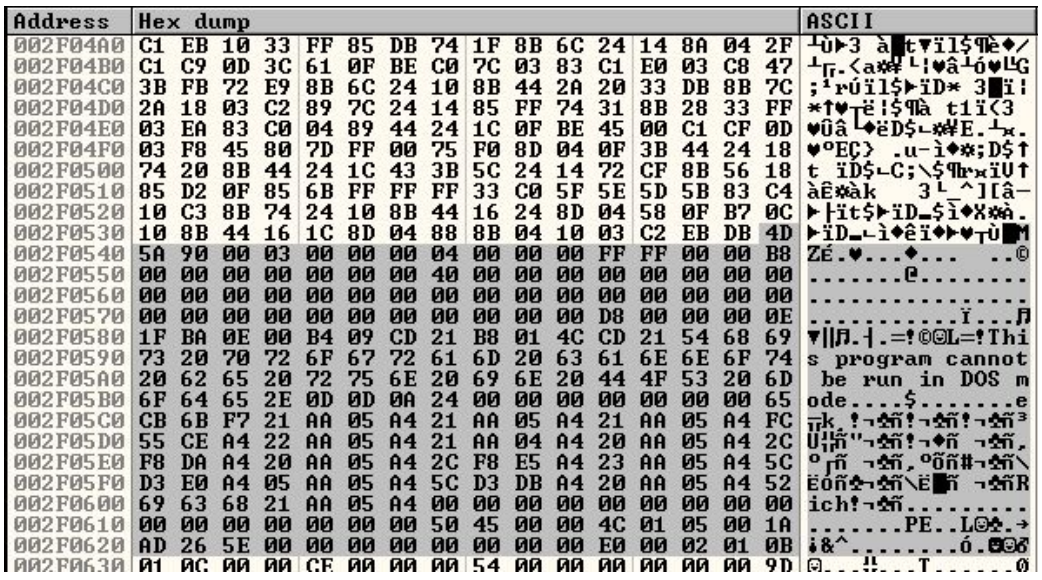
And press F8 on this call too. Just keep eye on HEX dump, to see data getting decrypted.



| Address | Hex dump | ASCII |
|---|---|---|
| 002F0000 | E8 00 00 00 00 58 89 C3 05 3A 05 00 00 81 C3 3A | Þ....Xë├♣:♣..ü├: |
| 002F0010 | F9 00 00 68 01 00 00 00 68 05 00 00 00 53 68 45 | ¨..h☺...h♣...ShE |
| 002F0020 | 77 62 30 50 E8 04 00 00 00 83 C4 14 C3 83 EC 48 | wb0PÞ♦...â—¶├âýH |
| 002F0030 | 83 64 24 18 00 B9 4C 77 26 07 53 55 56 57 33 F6 | âd$↑.╢Lw&•SUVW3÷ |
| 002F0040 | E8 22 04 00 00 B9 49 F7 02 78 89 44 24 1C E8 14 | Þ"♦..╢I ☻xëD$∟Þ¶ |
| 002F0050 | 04 00 00 B9 58 A4 53 E5 89 44 24 20 E8 06 04 00 | ♦..╢Xñ§σëD$ Þ♣♦. |
| 002F0060 | 00 B9 10 E1 8A C3 8B E8 E8 FA 03 00 00 B9 AF B1 | .╢►ßè├ïÞÞ·♥..╢»▒ |
| 002F0070 | 5C 94 89 44 24 2C E8 EC 03 00 00 B9 33 00 9E 95 | \öëD$,Þý♥..╢3.x○ |
| 002F0080 | 89 44 24 30 E8 DE 03 00 00 8B D8 8B 44 24 5C 8B | ëD$0Þ♥..ïÏïD$\ï |
| 002F0090 | 78 3C 03 F8 89 7C 24 10 81 3F 50 45 00 00 74 07 | x<♥°ë¦$►ü?PE..t• |
| 002F00A0 | 33 C0 E9 B8 03 00 00 B8 4C 01 00 00 66 39 47 04 | 3└ú©♥..©L☺..f9G♦ |
| 002F00B0 | 75 EE F6 47 38 01 75 E8 0F B7 57 06 0F B7 47 14 | u¯÷G8☺uÞ*♣W♣*♣G¶ |
| 002F00C0 | 85 D2 74 22 8D 4F 24 03 C8 83 79 04 00 8B 01 75 | àÊt"ìO$♥╙ây♦.ï☺u |
| 002F00D0 | 05 03 47 38 EB 03 03 41 04 3B C6 0F 47 F0 83 C1 | ♣♥G8ù♥♥A♦;ã*G-â┴ |
| 002F00E0 | 28 83 EA 01 75 E3 8D 44 24 34 50 FF D3 8B 44 24 | (âÛ☺uòìD$4P ËïD$ |
| 002F00F0 | 38 8B 5F 50 8D 50 FF 8D 48 FF F7 D2 48 03 CE 03 | 8ï_PìP ìH ¸ÊH♥╬♥ |
| 002F0100 | C3 23 CA 23 C2 3B C1 75 97 6A 04 68 00 30 00 00 | ├#╩#┬;┴uùj♦h.0.. |
| 002F0110 | 53 6A 00 FF D5 8B 77 54 8B D8 8B 44 24 5C 33 C9 | Sj. ╘ïwTïÏïD$\3╔ |
| 002F0120 | 89 44 24 14 8B D3 33 C0 89 5C 24 18 40 89 44 24 | ëD$¶ïË3└ë\$↑@ëD$ |
| 002F0130 | 24 85 F6 74 37 8B 6C 24 6C 8B 5C 24 14 23 E8 4E | $à÷t7ïl$lï\$¶#ÞN |
| 002F0140 | 85 ED 74 19 8B C7 2B 44 24 5C 3B C8 73 0F 83 F9 | àýt↓ïã+D$\;╚s*â¨ |
| 002F0150 | 3C 72 05 83 F9 3E 76 05 C6 02 00 EB 04 8A 03 88 | <r♣â¨>v♣ã☻.ù♦è♥ê |
| 002F0160 | 02 41 43 42 85 F6 75 D7 8B 5C 24 18 0F B7 47 06 | ☻ACBà÷uÎï\$↑*♠G♠ |

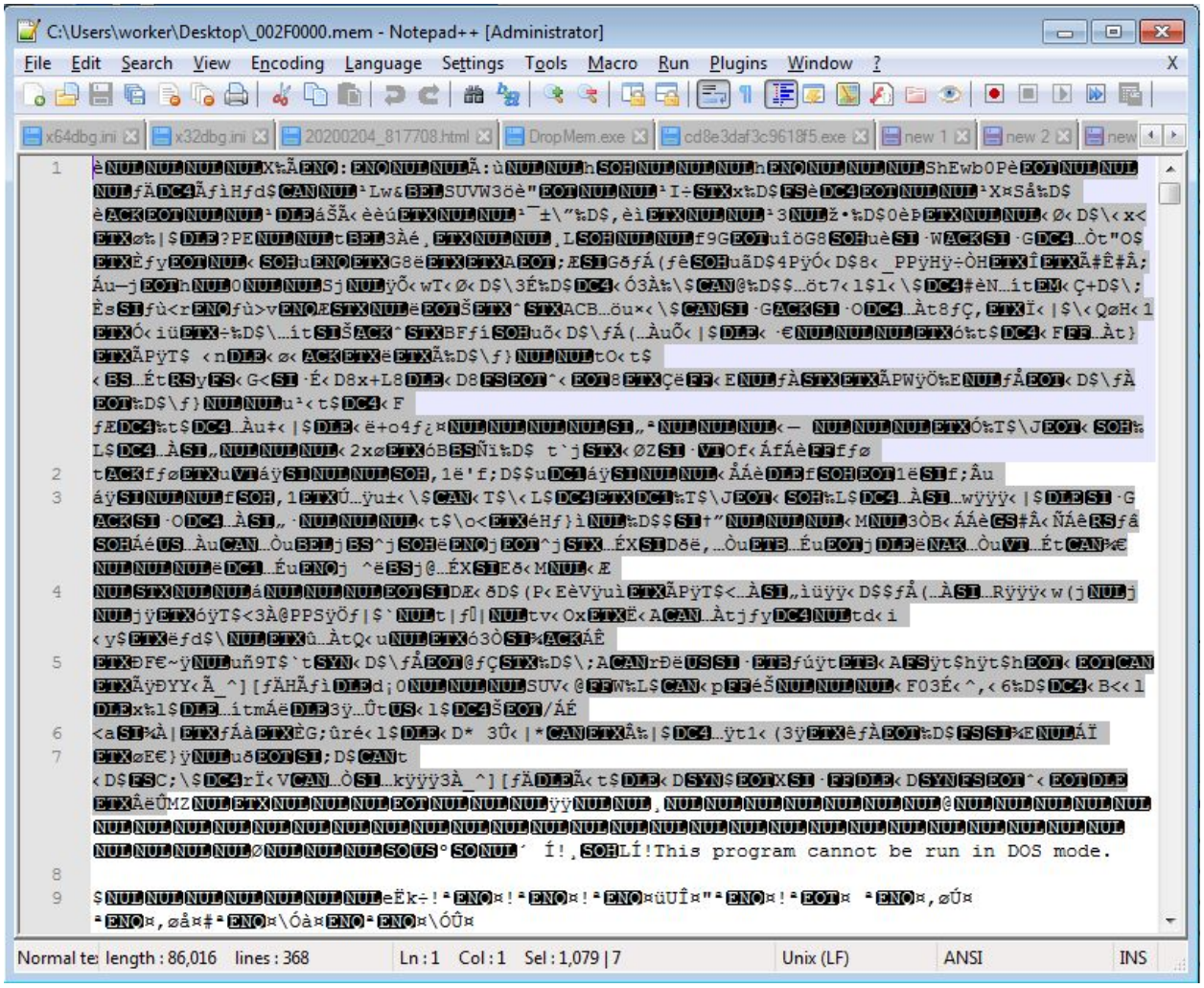
But this decrypted data still looks of no use. :(

Don’t worry, scroll a little down and you’ll find a hidden MZ header.



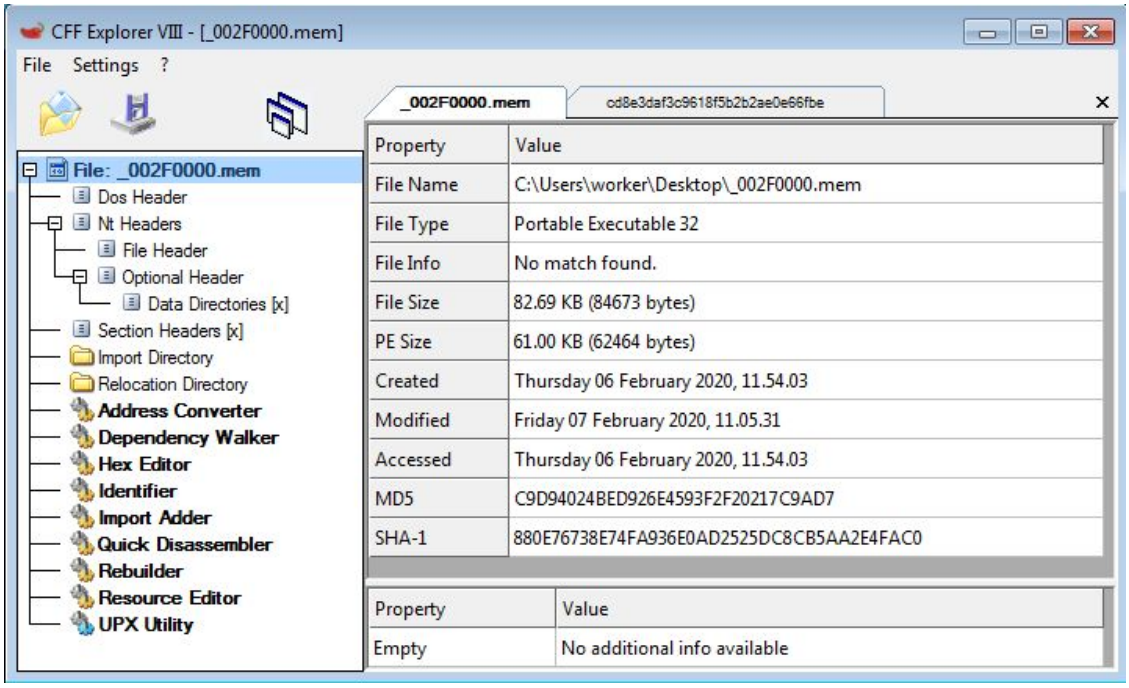
| Address | Hex dump | ASCII |
|---|---|---|
| 002F04A0 | C1 EB 10 33 FF 85 DB 74 1F 8B 6C 24 14 8A 04 2F | ┴ü►3 à▀t▼ïl$¶è♦/ |
| 002F04B0 | C1 C9 0D 3C 61 0F BE C0 7C 03 83 C1 E0 03 C8 47 | ┴╔.<a*╛└¦♥â┴ó♥╙G |
| 002F04C0 | 3B FB 72 E9 8B 6C 24 10 8B 44 2A 20 33 DB 8B 7C | ;¹rúïl$►ïD* 3▀ï! |
| 002F04D0 | 2A 18 03 C2 89 7C 24 14 85 FF 74 31 8B 28 33 FF | *↑♥┬ë¦$¶à t1ï(3 |
| 002F04E0 | 03 EA 83 C0 04 89 44 24 1C 0F BE 45 00 C1 CF 0D | ♥Ûâ└♦ëD$∟*╛E.┴╪. |
| 002F04F0 | 03 F8 45 80 7D FF 00 75 F0 8D 04 0F 3B 44 24 18 | ♥°EÇ} .u-ì♦*;D$↑ |
| 002F0500 | 74 20 8B 44 24 1C 43 3B 5C 24 14 72 CF 8B 56 18 | t ïD$∟C;\$¶r╪ïV↑ |
| 002F0510 | 85 D2 0F 85 6B FF FF FF 33 C0 5F 5E 5D 5B 83 C4 | àÊ*àk   3└_^]ât |
| 002F0520 | 10 C3 8B 74 24 10 8B 44 16 24 8D 04 58 0F B7 0C | ►├ït$►ïD▬$ì♦X*♣. |
| 002F0530 | 10 8B 44 16 1C 8D 04 88 8B 04 10 03 C2 EB DB 4D | ►ïD▬∟ì♦êï♦►♥┬ü▀M |
| 002F0540 | 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 | Zé.♥...♦...  ..© |
| 002F0550 | 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00 | .......@........ |
| 002F0560 | 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 | ................ |
| 002F0570 | 00 00 00 00 00 00 00 00 00 00 00 00 D8 00 00 00 0E | ............Ï...♬ |
| 002F0580 | 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69 | ▼‖♬.┤.=¦©☺L=¦Thi |
| 002F0590 | 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74 | s program cannot |
| 002F05A0 | 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D | be run in DOS m |
| 002F05B0 | 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 65 | ode....$.......e |
| 002F05C0 | CB 6B F7 21 AA 05 A4 21 AA 05 A4 21 AA 05 A4 FC | ╦k╖!¬♣ñ!¬♣ñ!¬♣ñ³ |
| 002F05D0 | 55 CE A4 22 AA 05 A4 21 AA 04 A4 20 AA 05 A4 2C | U╬ñ"¬♣ñ!¬♦ñ ¬♣ñ, |
| 002F05E0 | F8 DA A4 20 AA 05 A4 2C F8 E5 A4 23 AA 05 A4 5C | °┌ñ ¬♣ñ,°σñ#¬♣ñ\ |
| 002F05F0 | D3 E0 A4 05 AA 05 A4 5C D3 DB A4 20 AA 05 A4 52 | Ëσñ♣¬♣ñ\Ë▀ñ ¬♣ñR |
| 002F0600 | 69 63 68 21 AA 05 A4 00 00 00 00 00 00 00 00 00 | ich!¬♣ñ......... |
| 002F0610 | 00 00 00 00 00 00 00 50 45 00 00 4C 01 05 00 1A | .......PE..L☺♣.→ |
| 002F0620 | AD 26 5E 00 00 00 00 00 00 00 00 E0 00 02 01 0B | ¡&^.........ó.☺◙ |
| 002F0630 | 01 0C 00 00 CE 00 00 00 54 00 00 00 00 00 00 9D | ☺...╬...T......Ø |

Let's save this dump to the disk and open it to Notepad++ and remove the unwanted content from the file. I have selected the unwanted content till MZ and will remove it.




Now save the file after removing it. And load the file inside CFF explorer

Aha, See we got the perfect PE file ;)




SHA - 1: 880E76738E74FA936E0AD2525DC8CB5AA2E4FAC0

**Checking the behavior of an Extracted file.**

Now let's dive deep into the extracted PE file…… Will continue in some days.