malware analysis report NoMoreRansom.exe

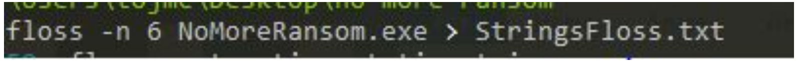
malware explanation

NoMoreRansom is a type of ransomware that encrypts files on the victim's computer and demands a ransom payment, typically in cryptocurrency, to provide the decryption key. It spreads through phishing emails, exploit kits, and other malicious means. Once a system is infected, NoMoreRansom will scan for and encrypt various file types like documents, images, videos etc. It then displays a ransom note with instructions on how to pay the ransom to allegedly get the decryption key. However, there is no guarantee the attackers will actually provide the key after payment.

malware Composition

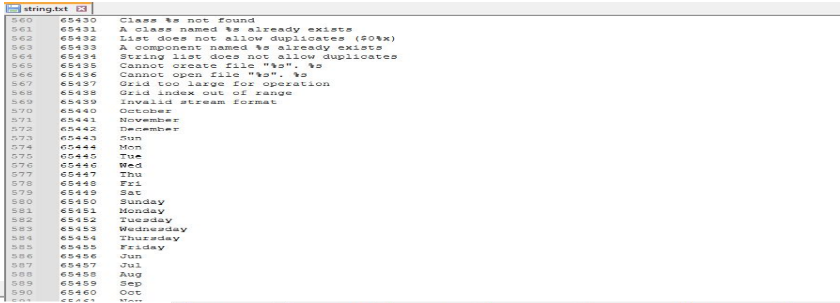
file name	sha-256
NoMoreRansom.exe	2aab13d49b60001de3aa47fb8f7251a973faa7f3c53a3840cdf5fd0b26e9a09f
csrss.exe	2aab13d49b60001de3aa47fb8f7251a973faa7f3c53a3840cdf5fd0b26e9a09f
vssadmin.exe	8c1fabcc2196e4d096b7d155837c5f699ad7f55edbf84571e4f8e03500b7a8b0

static analysis

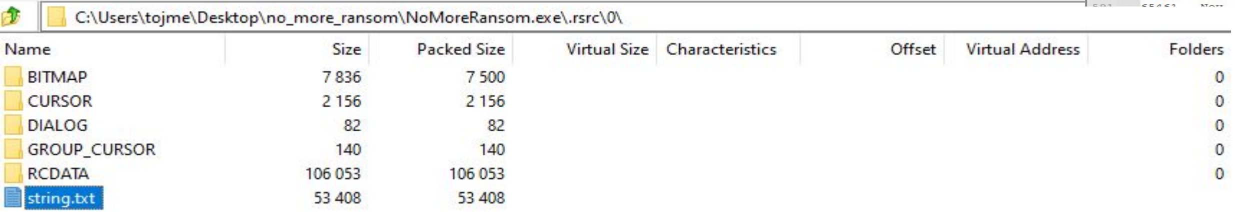


```
floss -n 6 NoMoreRansom.exe > StringsFloss.txt
```

When I extracted the strings using the floss command. I found that the author used strings injection method to make it difficult for analysis I’ve found the strings file when I opened the malware in cff explorer and saw his resources.

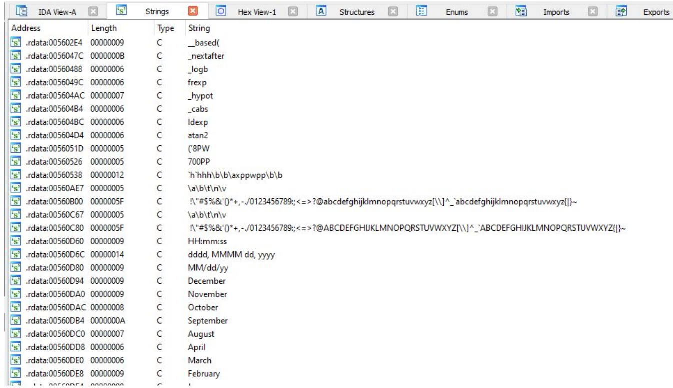


```
65430   Class %s not found
65431   A class named %s already exists
65432   List does not allow duplicates ($0%x)
65433   A component named %s already exists
65434   String list does not allow duplicates
65435   Cannot create file "%s". %s
65436   Cannot open file "%s". %s
65437   Grid too large for operation
65438   Grid index out of range
65439   Invalid stream format
65440   October
65441   November
65442   December
65443   Sun
65444   Mon
65445   Tue
65446   Wed
65447   Thu
65448   Fri
65449   Sat
65450   Sunday
65451   Monday
65452   Tuesday
65453   Wednesday
65454   Thursday
65455   Friday
65456   Jun
65457   Jul
65458   Aug
65459   Sep
65460   Oct
```



C:\Users\tojme\Desktop\no_more_ransom\NoMoreRansom.exe\.rsrc\0\

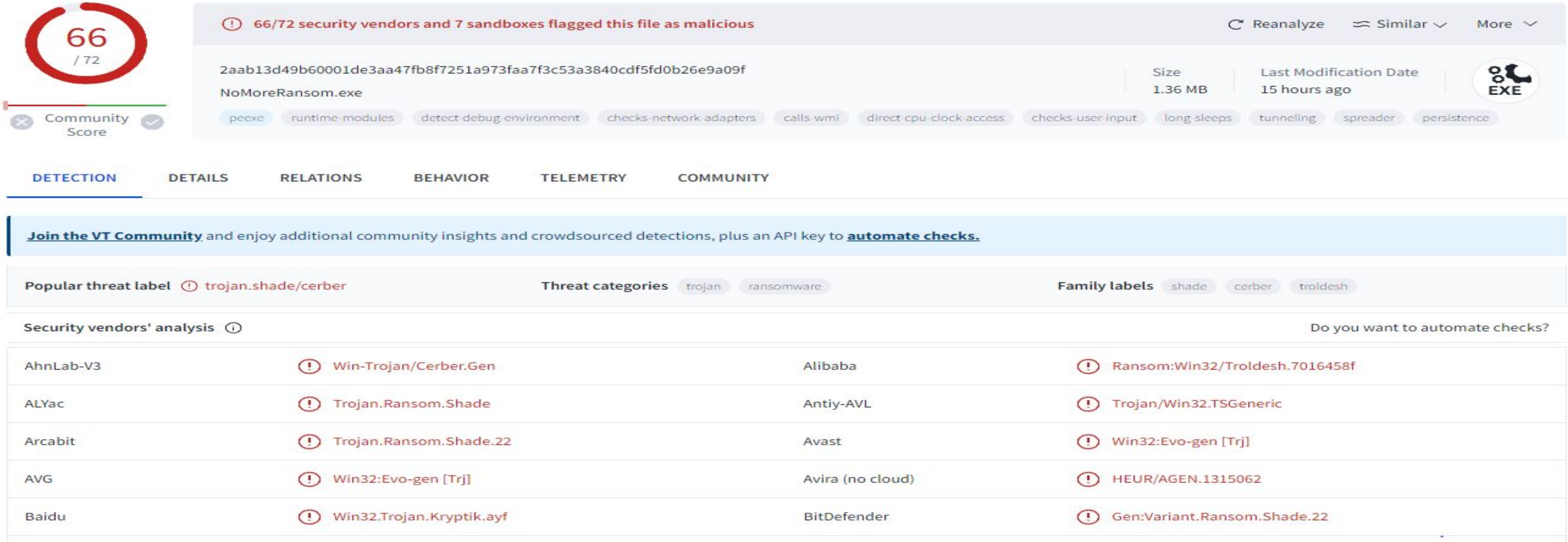
Name	Size	Packed Size	Virtual Size	Characteristics	Offset	Virtual Address	Folders
BITMAP	7 836	7 500					0
CURSOR	2 156	2 156					0
DIALOG	82	82					0
GROUP_CURSOR	140	140					0
RCDATA	106 053	106 053					0
string.txt	53 408	53 408					



Address	Length	Type	String
.rdata:005602E4	00000009	C	__based(
.rdata:0056047C	0000000B	C	_nextafter
.rdata:00560488	00000006	C	_logb
.rdata:0056049C	00000006	C	frexp
.rdata:005604AC	00000007	C	_hypot
.rdata:005604B4	00000006	C	_cabs
.rdata:005604BC	00000006	C	ldexp
.rdata:005604D4	00000006	C	atan2
.rdata:0056051D	00000005	C	('8PW
.rdata:00560526	00000005	C	700PP
.rdata:00560538	00000012	C	\`h\`hhh\b\b\axppwpp\b\b
.rdata:00560AE7	00000005	C	\a\b\t\n\v
.rdata:00560B00	0000005F	C	!\"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\\]^_\`abcdefghijklmnopqrstuvwxyz{|}~
.rdata:00560C67	00000005	C	\a\b\t\n\v
.rdata:00560C80	0000005F	C	!\"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\\]^_\`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~
.rdata:00560D60	00000009	C	HH:mm:ss
.rdata:00560D6C	00000014	C	dddd, MMMM dd, yyyy
.rdata:00560D80	00000009	C	MM/dd/yy
.rdata:00560D94	00000009	C	December
.rdata:00560DA0	00000009	C	November
.rdata:00560DAC	00000008	C	October
.rdata:00560DB4	0000000A	C	September
.rdata:00560DC0	00000007	C	August
.rdata:00560DD8	00000006	C	April
.rdata:00560DE0	00000006	C	March
.rdata:00560DE8	00000009	C	February

virus total

From VirusTotal we can see that this malware is very malicious and got the score 66 of 72!!!



66
/ 72

Community Score

66/72 security vendors and 7 sandboxes flagged this file as malicious

2aab13d49b60001de3aa47fb8f7251a973faa7f3c53a3840cdf5fd0b26e9a09f

NoMoreRansom.exe

Size
1.36 MB

Last Modification Date
15 hours ago

peexe · runtime-modules · detect-debug-environment · checks-network-adapters · calls-wmi · direct-cpu-clock-access · checks-user-input · long-sleeps · tunneling · spreader · persistence

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

Popular threat label trojan.shade/cerber **Threat categories** trojan ransomware **Family labels** shade cerber troldesh

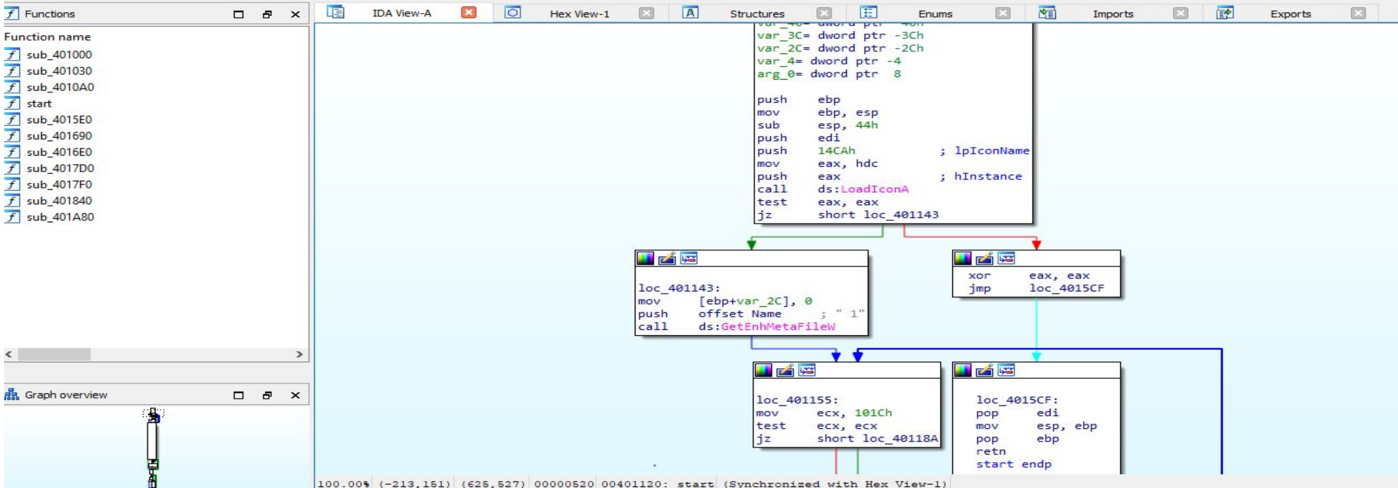
Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Win-Trojan/Cerber.Gen	Alibaba	Ransom:Win32/Troldesh.7016458f
ALYac	Trojan.Ransom.Shade	Antiy-AVL	Trojan/Win32.TSGeneric
Arcabit	Trojan.Ransom.Shade.22	Avast	Win32:Evo-gen [Trj]
AVG	Win32:Evo-gen [Trj]	Avira (no cloud)	HEUR/AGEN.1315062
Baidu	Win32.Trojan.Kryptik.ayf	BitDefender	Gen:Variant.Ransom.Shade.22

Identification

When I first opened the executable file in IDA Pro, I could see that it had a few functions, but most of them were filled with junk code. This made it difficult to analyze the malware's functionality. When I ran the ransomware file, I observed that it was doing a lot of things, such as importing a ransom wallpaper. However, I couldn't see these actions in the code itself. This suggests that the malware is using some kind of packer or code obfuscation technique to hide its true functionality.



```
Function name
sub_401000
sub_401030
sub_4010A0
start
sub_4015E0
sub_401690
sub_4016E0
sub_4017D0
sub_4017F0
sub_401840
sub_401A80
```

```
var_3C= dword ptr -3Ch
var_2C= dword ptr -2Ch
var_4= dword ptr -4
arg_0= dword ptr  8

push    ebp
mov     ebp, esp
sub     esp, 44h
push    edi
push    14CAh           ; lpIconName
mov     eax, hdc
push    eax             ; hInstance
call    ds:LoadIconA
test    eax, eax
jz      short loc_401143
```

```
loc_401143:
mov     [ebp+var_2C], 0
push    offset Name     ; " 1"
call    ds:GetEnhMetaFileW
```

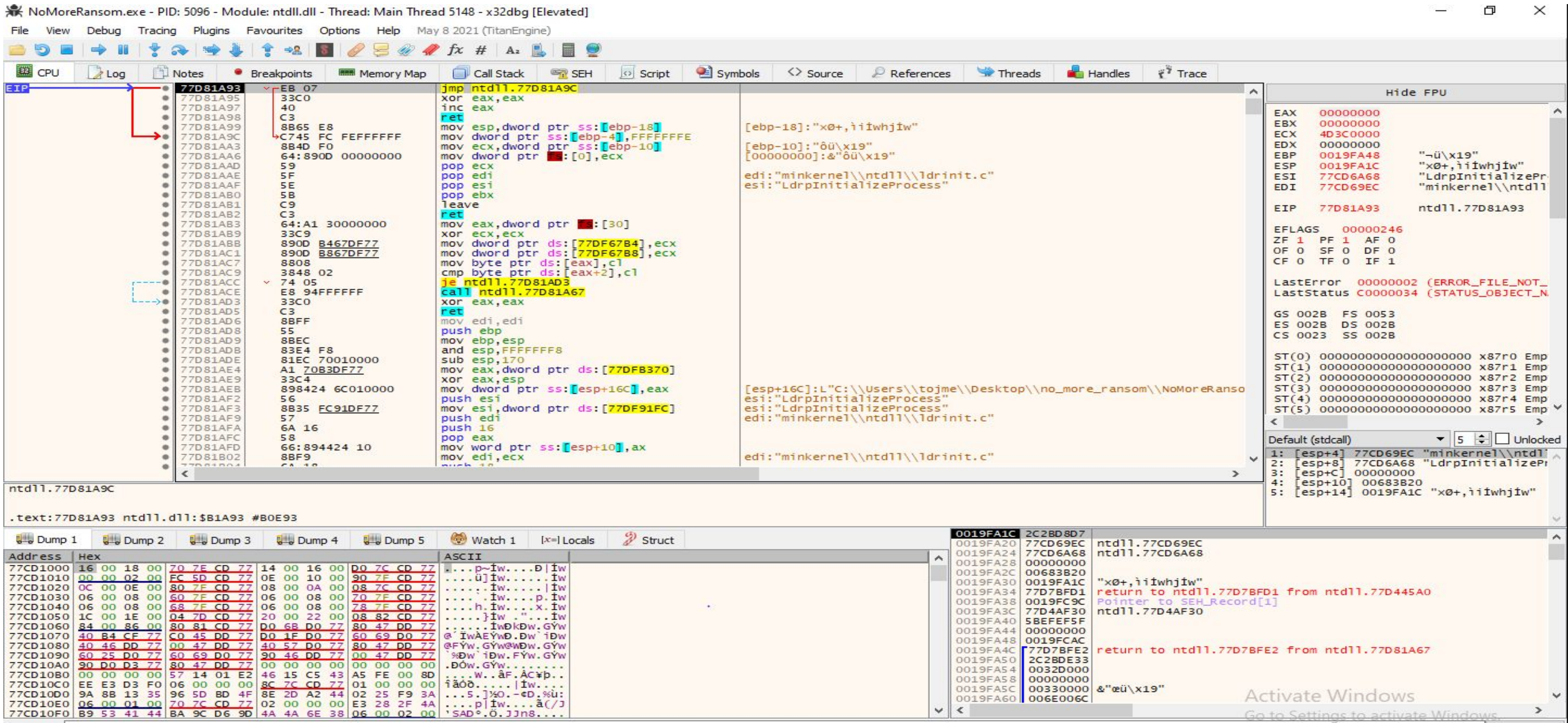
```
xor     eax, eax
jmp     loc_4015CF
```

```
loc_401155:
mov     ecx, 101Ch
test    ecx, ecx
jz      short loc_40118A
```

```
loc_4015CF:
pop     edi
mov     esp, ebp
pop     ebp
retn
start endp
```

```
100.00% (-213,151) (625,527) 00000520 00401120: start (Synchronized with Hex View-1)
```

Manually Unpacking through debugging



NoMoreRansom.exe - PID: 5096 - Module: ntdll.dll - Thread: Main Thread 5148 - x32dbg [Elevated]

```
77D81A93  EB 07              jmp ntdll.77D81A9C
77D81A95  33C0               xor eax,eax
77D81A97  40                 inc eax
77D81A98  C3                 ret
77D81A99  8B65 E8            mov esp,dword ptr ss:[ebp-18]             [ebp-18]:"x0+,ìiÍwhjÍw"
77D81A9C  C745 FC FEFFFFFF   mov dword ptr ss:[ebp-4],FFFFFFFE
77D81AA3  8B4D F0            mov ecx,dword ptr ss:[ebp-10]             [ebp-10]:"ôü\x19"
77D81AA6  64:890D 00000000   mov dword ptr fs:[0],ecx                  [00000000]:&"ôü\x19"
77D81AAD  59                 pop ecx
77D81AAE  5F                 pop edi                                   edi:"minkernel\\ntdll\\ldrinit.c"
77D81AAF  5E                 pop esi                                   esi:"LdrpInitializeProcess"
77D81AB0  5B                 pop ebx
77D81AB1  C9                 leave
77D81AB2  C3                 ret
77D81AB3  64:A1 30000000     mov eax,dword ptr fs:[30]
77D81AB9  33C9               xor ecx,ecx
77D81ABB  890D B467DF77      mov dword ptr ds:[77DF67B4],ecx
77D81AC1  890D B867DF77      mov dword ptr ds:[77DF67B8],ecx
77D81AC7  8808               mov byte ptr ds:[eax],cl
77D81AC9  3848 02            cmp byte ptr ds:[eax+2],cl
77D81ACC  74 05              je ntdll.77D81AD3
77D81ACE  E8 94FFFFFF        call ntdll.77D81A67
77D81AD3  33C0               xor eax,eax
77D81AD5  C3                 ret
77D81AD6  8BFF               mov edi,edi
77D81AD8  55                 push ebp
77D81AD9  8BEC               mov ebp,esp
77D81ADB  83E4 F8            and esp,FFFFFFF8
77D81ADE  81EC 70010000      sub esp,170
77D81AE4  A1 70B3DF77        mov eax,dword ptr ds:[77DFB370]
77D81AE9  33C4               xor eax,esp
77D81AEB  898424 6C010000    mov dword ptr ss:[esp+16C],eax            [esp+16C]:L"C:\\Users\\tojme\\Desktop\\no_more_ransom\\NoMoreRanso
77D81AF2  56                 push esi                                  esi:"LdrpInitializeProcess"
77D81AF3  8B35 FC91DF77      mov esi,dword ptr ds:[77DF91FC]           esi:"LdrpInitializeProcess"
77D81AF9  57                 push edi                                  edi:"minkernel\\ntdll\\ldrinit.c"
77D81AFA  6A 16              push 16
77D81AFC  58                 pop eax
77D81AFD  66:894424 10       mov word ptr ss:[esp+10],ax
77D81B02  8BF9               mov edi,ecx                               edi:"minkernel\\ntdll\\ldrinit.c"
```

```
EAX   00000000
EBX   00000000
ECX   4D3C0000
EDX   00000000
EBP   0019FA48     "¬ü\x19"
ESP   0019FA1C     "x0+,ìiÍwhjÍw"
ESI   77CD6A68     "LdrpInitializePr
EDI   77CD69EC     "minkernel\\ntdll

EIP   77D81A93     ntdll.77D81A93

EFLAGS   00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  00000002 (ERROR_FILE_NOT_
LastStatus C0000034 (STATUS_OBJECT_N

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000 x87r0 Emp
ST(1) 00000000000000000000 x87r1 Emp
ST(2) 00000000000000000000 x87r2 Emp
ST(3) 00000000000000000000 x87r3 Emp
ST(4) 00000000000000000000 x87r4 Emp
ST(5) 00000000000000000000 x87r5 Emp
```

Default (stdcall) 5 □ Unlocked

```
1: [esp+4] 77CD69EC "minkernel\\ntdl
2: [esp+8] 77CD6A68 "LdrpInitializePr
3: [esp+C] 00000000
4: [esp+10] 00683B20
5: [esp+14] 0019FA1C "x0+,ìiÍwhjÍw"
```

```
ntdll.77D81A9C

.text:77D81A93 ntdll.dll:$B1A93 #B0E93
```

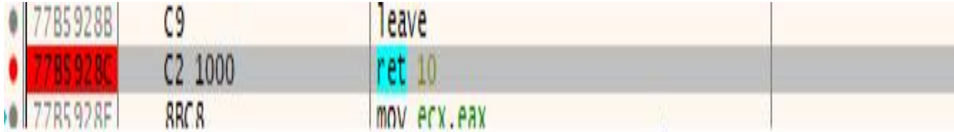
```
Address   Hex                                                ASCII
77CD1000  16 00 18 00 70 7E CD 77 14 00 16 00 D0 7C CD 77  ....p~Íw....Ð|Íw
77CD1010  00 00 02 00 FC 5D CD 77 0E 00 10 00 90 7F CD 77  ....ü]Íw......Íw
77CD1020  0C 00 0E 00 80 7F CD 77 08 00 0A 00 08 7C CD 77  ......Íw.....|Íw
77CD1030  06 00 08 00 60 7F CD 77 06 00 08 00 70 7F CD 77  ....`.Íw....p.Íw
77CD1040  06 00 08 00 68 7F CD 77 06 00 08 00 78 7F CD 77  ....h.Íw....x.Íw
77CD1050  1C 00 1E 00 04 7D CD 77 20 00 22 00 08 82 CD 77  .....}Íw .".. Íw
77CD1060  84 00 86 00 80 81 CD 77 D0 6B D0 77 80 47 DD 77  ......ÍwÐkÐw.GÝw
77CD1070  40 B4 CF 77 C0 45 DD 77 D0 1F D0 77 60 69 D0 77  @´ÏwÀEÝwÐ.Ðw`iÐw
77CD1080  40 46 DD 77 00 47 DD 77 40 57 D0 77 80 47 DD 77  @FÝw.GÝw@WÐw.GÝw
77CD1090  60 25 D0 77 60 69 D0 77 90 46 DD 77 00 47 DD 77  `%Ðw`iÐw.FÝw.GÝw
77CD10A0  90 D0 D3 77 80 47 DD 77 00 00 00 00 00 00 00 00  .ÐÓw.GÝw........
77CD10B0  00 00 00 00 57 14 01 E2 46 15 C5 43 A5 FE 00 8D  ....W..âF.ÅC¥þ..
77CD10C0  EE E3 D3 F0 06 00 00 00 8C 7C CD 77 01 00 00 00  îãÓð.....|Íw....
77CD10D0  9A 8B 13 35 96 5D BD 4F 8E 2D A2 44 02 25 F9 3A  ...5.]½O.-¢D.%ù:
77CD10E0  06 00 01 00 70 7C CD 77 02 00 00 00 E3 28 2F 4A  ....p|Íw....ã(/J
77CD10F0  B9 53 41 44 BA 9C D6 9D 4A 4A 6E 38 06 00 02 00  ¹SAD°.Ö.JJn8....
```

```
0019FA1C  2C2BD8D7
0019FA20  77CD69EC  ntdll.77CD69EC
0019FA24  77CD6A68  ntdll.77CD6A68
0019FA28  00000000
0019FA2C  00683B20
0019FA30  0019FA1C  "x0+,ìiÍwhjÍw"
0019FA34  77D7BFD1  return to ntdll.77D7BFD1 from ntdll.77D445A0
0019FA38  0019FC9C  Pointer to SEH_Record[1]
0019FA3C  77D4AF30  ntdll.77D4AF30
0019FA40  5BEFEF5F
0019FA44  00000000
0019FA48  0019FCAC
0019FA4C  77D7BFE2  return to ntdll.77D7BFE2 from ntdll.77D81A67
0019FA50  2C2BDE33
0019FA54  0032D000
0019FA58  00000000
0019FA5C  00330000  &"œü\x19"
0019FA60  006E006C
```

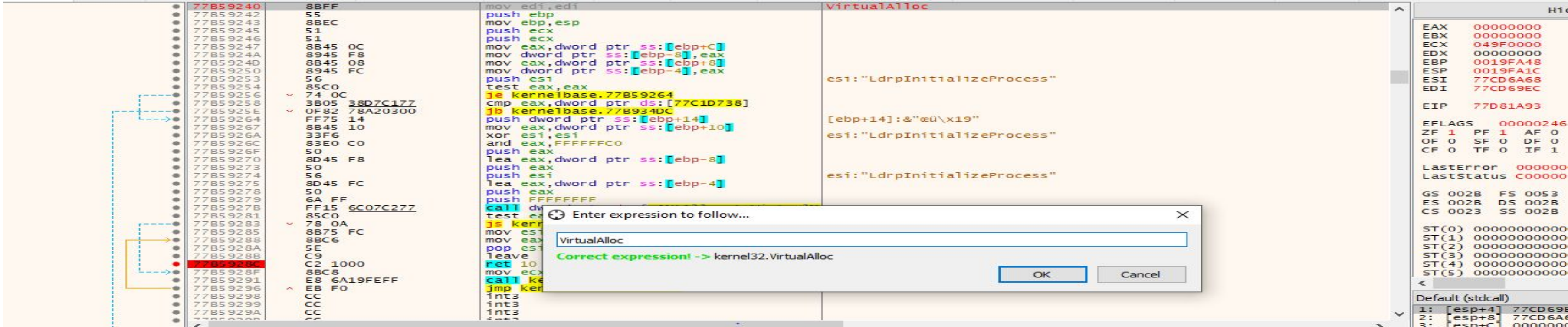
To manually debug this, first I put a breakpoint on the VirtualAlloc API. This API indicates that the malware is allocating memory for the OPE file.

1.then set a breakpoint on the return from VirtualAlloc.

2.run the debugger until the OPE file was loaded into the EAX register.



```
77B5928B    C9        leave
77B5928C    C2 1000   ret 10
77B5928F    8BC8      mov ecx,eax
```



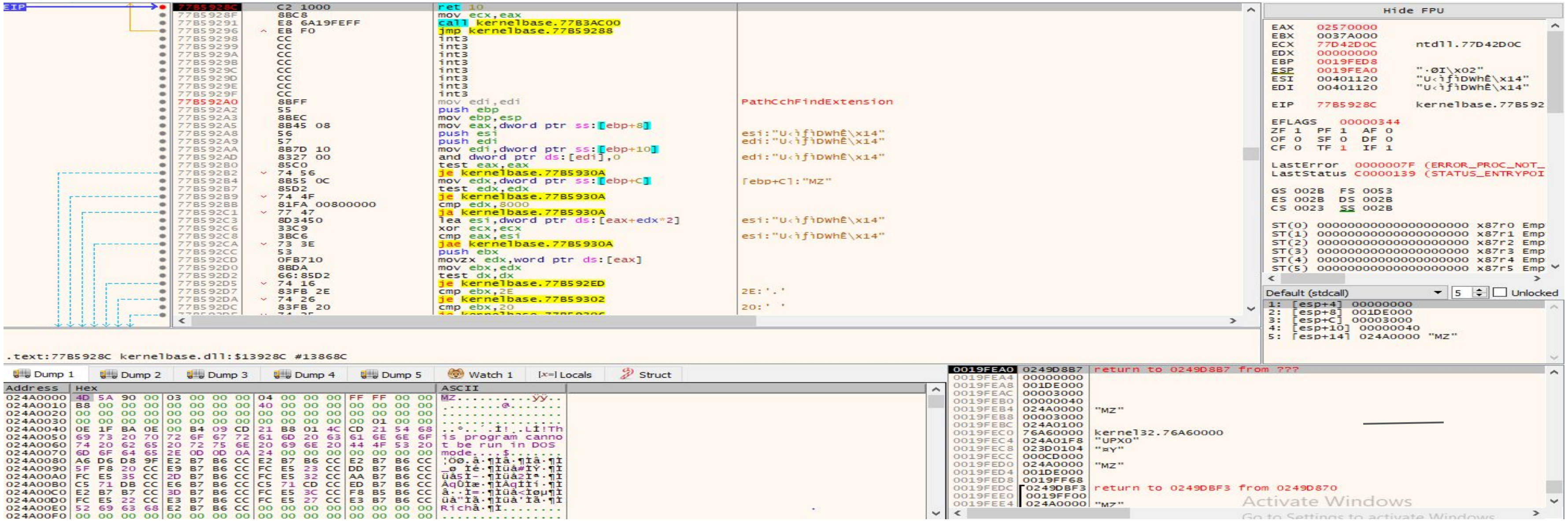
```
77B59240   8BFF          mov edi,edi                            VirtualAlloc
77B59242   55            push ebp
77B59243   8BEC          mov ebp,esp
77B59245   51            push ecx
77B59246   51            push ecx
77B59247   8B45 0C       mov eax,dword ptr ss:[ebp+C]
77B5924A   8945 F8       mov dword ptr ss:[ebp-8],eax
77B5924D   8B45 08       mov eax,dword ptr ss:[ebp+8]
77B59250   8945 FC       mov dword ptr ss:[ebp-4],eax
77B59253   56            push esi                               esi:"LdrpInitializeProcess"
77B59254   85C0          test eax,eax
77B59256   74 0C         je kernelbase.77B59264
77B59258   3B05 38D7C177 cmp eax,dword ptr ds:[77C1D738]
77B5925E   0F82 78A20300 jb kernelbase.77B934DC
77B59264   FF75 14       push dword ptr ss:[ebp+14]             [ebp+14]:&"œü\x19"
77B59267   8B45 10       mov eax,dword ptr ss:[ebp+10]
77B5926A   33F6          xor esi,esi                            esi:"LdrpInitializeProcess"
77B5926C   83E0 C0       and eax,FFFFFFC0
77B5926F   50            push eax
77B59270   8D45 F8       lea eax,dword ptr ss:[ebp-8]
77B59273   50            push eax
77B59274   56            push esi                               esi:"LdrpInitializeProcess"
77B59275   8D45 FC       lea eax,dword ptr ss:[ebp-4]
77B59278   50            push eax
77B59279   6A FF         push FFFFFFFF
77B5927B   FF15 6C07C277 call dw
77B59281   85C0          test ea
77B59283   78 0A         js kerr
77B59285   8B75 FC       mov esi
77B59288   8BC6          mov eax
77B5928A   5E            pop esi
77B5928B   C9            leave
77B5928C   C2 1000       ret 10
77B5928F   8BC8          mov ecx
77B59291   E8 6A19FEFF   call ke
77B59296   EB F0         jmp ker
77B59298   CC            int3
77B59299   CC            int3
77B5929A   CC            int3
```

```
EAX      00000000
EBX      00000000
ECX      049F0000
EDX      00000000
EBP      0019FA48
ESP      0019FA1C
ESI      77CD6A68
EDI      77CD69EC

EIP      77D81A93

EFLAGS     00000246
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 0  IF 1

LastError  000000
LastStatus C00000

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000
ST(1) 00000000000
ST(2) 00000000000
ST(3) 00000000000
ST(4) 00000000000
ST(5) 00000000000

Default (stdcall)
1: [esp+4] 77CD69E
2: [esp+8] 77CD6A6
```

Enter expression to follow...

VirtualAlloc

Correct expression! -> kernel32.VirtualAlloc



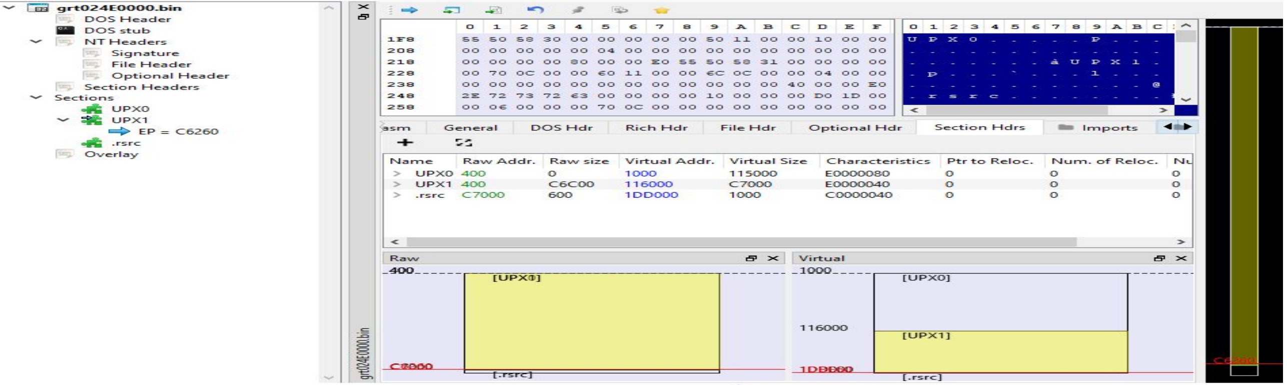
```
77B5928C   C2 1000              ret 10
77B5928F   8BC8                 mov ecx,eax
77B59291   E8 6A19FEFF          call kernelbase.77B3AC00
77B59296 ^ EB F0                jmp kernelbase.77B59288
77B59298   CC                   int3
77B59299   CC                   int3
77B5929A   CC                   int3
77B5929B   CC                   int3
77B5929C   CC                   int3
77B5929D   CC                   int3
77B5929E   CC                   int3
77B5929F   CC                   int3
77B592A0   8BFF                 mov edi,edi                        PathCchFindExtension
77B592A2   55                   push ebp
77B592A3   8BEC                 mov ebp,esp
77B592A5   8B45 08              mov eax,dword ptr ss:[ebp+8]
77B592A8   56                   push esi                           esi:"U<ìƒìDWhÊ\x14"
77B592A9   57                   push edi                           edi:"U<ìƒìDWhÊ\x14"
77B592AA   8B7D 10              mov edi,dword ptr ss:[ebp+10]
77B592AD   8327 00              and dword ptr ds:[edi],0           edi:"U<ìƒìDWhÊ\x14"
77B592B0   85C0                 test eax,eax
77B592B2 v 74 56                je kernelbase.77B5930A
77B592B4   8B55 0C              mov edx,dword ptr ss:[ebp+C]       [ebp+C]:"MZ"
77B592B7   85D2                 test edx,edx
77B592B9 v 74 4F                je kernelbase.77B5930A
77B592BB   81FA 00800000        cmp edx,8000
77B592C1 v 77 47                ja kernelbase.77B5930A
77B592C3   8D3450               lea esi,dword ptr ds:[eax+edx*2]   esi:"U<ìƒìDWhÊ\x14"
77B592C6   33C9                 xor ecx,ecx
77B592C8   3BC6                 cmp eax,esi                        esi:"U<ìƒìDWhÊ\x14"
77B592CA v 73 3E                jae kernelbase.77B5930A
77B592CC   53                   push ebx
77B592CD   0FB710               movzx edx,word ptr ds:[eax]
77B592D0   8BDA                 mov ebx,edx
77B592D2   66:85D2              test dx,dx
77B592D5 v 74 16                je kernelbase.77B592ED
77B592D7   83FB 2E              cmp ebx,2E                         2E:'.'
77B592DA v 74 26                je kernelbase.77B59302
77B592DC   83FB 20              cmp ebx,20                         20:' '

.text:77B5928C kernelbase.dll:$13928C #13868C
```

```
Hide FPU

EAX    02570000
EBX    0037A000
ECX    77D42D0C       ntdll.77D42D0C
EDX    00000000
EBP    0019FED8
ESP    0019FEA0       "·ØI\x02"
ESI    00401120       "U<ìƒìDWhÊ\x14"
EDI    00401120       "U<ìƒìDWhÊ\x14"

EIP    77B5928C       kernelbase.77B592

EFLAGS    00000344
ZF 1  PF 1  AF 0
OF 0  SF 0  DF 0
CF 0  TF 1  IF 1

LastError  0000007F (ERROR_PROC_NOT_
LastStatus C0000139 (STATUS_ENTRYPOI

GS 002B  FS 0053
ES 002B  DS 002B
CS 0023  SS 002B

ST(0) 00000000000000000000 x87r0 Emp
ST(1) 00000000000000000000 x87r1 Emp
ST(2) 00000000000000000000 x87r2 Emp
ST(3) 00000000000000000000 x87r3 Emp
ST(4) 00000000000000000000 x87r4 Emp
ST(5) 00000000000000000000 x87r5 Emp

Default (stdcall)   5   □ Unlocked
1: [esp+4] 00000000
2: [esp+8] 001DE000
3: [esp+C] 00003000
4: [esp+10] 00000040
5: [esp+14] 024A0000 "MZ"
```

```
Address   Hex                                              ASCII
024A0000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
024A0010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ........@.......
024A0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
024A0030  00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00  ................
024A0040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
024A0050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
024A0060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
024A0070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
024A0080  A6 D6 D8 9F E2 B7 B6 CC E2 B7 B6 CC E2 B7 B6 CC  ¦ÖØ.â·¶Ìâ·¶Ìâ·¶Ì
024A0090  5F F8 20 CC E9 B7 B6 CC FC E5 23 CC DD B7 B6 CC  _ø Ìé·¶Ìüå#ÌÝ·¶Ì
024A00A0  FC E5 35 CC 2D B7 B6 CC FC E5 32 CC AA B7 B6 CC  üå5Ì-·¶Ìüå2Ìª·¶Ì
024A00B0  C5 71 DB CC E6 B7 B6 CC C5 71 CD CC ED B7 B6 CC  ÅqÛÌæ·¶ÌÅqÍÌí·¶Ì
024A00C0  E2 B7 B7 CC 3D B7 B6 CC FC E5 3C CC F8 B5 B6 CC  â··Ì=·¶Ìüå<Ìøµ¶Ì
024A00D0  FC E5 22 CC E3 B7 B6 CC FC E5 27 CC E3 B7 B6 CC  üå"Ìã·¶Ìüå'Ìã·¶Ì
024A00E0  52 69 63 68 E2 B7 B6 CC 00 00 00 00 00 00 00 00  Richâ·¶Ì........
024A00F0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

```
0019FEA0  0249D8B7  return to 0249D8B7 from ???
0019FEA4  00000000
0019FEA8  001DE000
0019FEAC  00003000
0019FEB0  00000040
0019FEB4  024A0000  "MZ"
0019FEB8  00003000
0019FEBC  024A0100
0019FEC0  76A60000  kernel32.76A60000
0019FEC4  024A01F8  "UPX0"
0019FEC8  023D0104  "¤Y"
0019FECC  000CD000
0019FED0  024A0000  "MZ"
0019FED4  001DE000
0019FED8  0019FF68
0019FEDC  0249DBF3  return to 0249DBF3 from 0249D870
0019FEE0  0019FF00
0019FEE4  024A0000  "MZ"
```

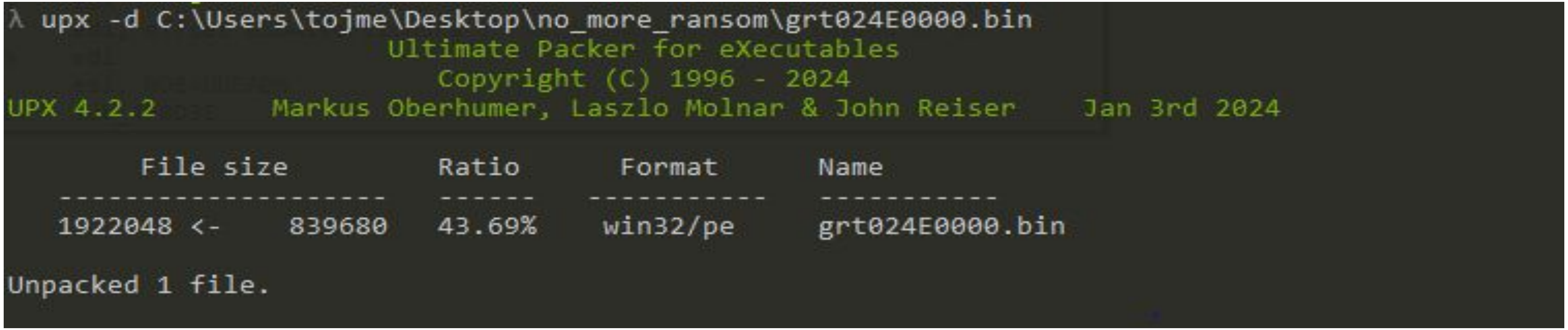
After the malware stopped at the breakpoint, we can see the address that was allocated in the EAX register. In the memory dump, we can see the OEP (Original Entry Point) of the file. Scrolling down a bit, we can see that the file is packed with UPX (Ultimate Packer for eXecutables). So, the next step is to dump this file and unpack it.



```
     0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F
1F8  55 50 58 30 00 00 00 00 00 50 11 00 00 10 00 00
208  00 00 00 00 00 04 00 00 00 00 00 00 00 00 00 00
218  00 00 00 00 80 00 00 E0 55 50 58 31 00 00 00 00
228  00 70 0C 00 00 60 11 00 00 6C 0C 00 00 04 00 00
238  00 00 00 00 00 00 00 00 00 00 00 00 40 00 00 E0
248  2E 72 73 72 63 00 00 00 00 10 00 00 00 D0 1D 00
258  00 06 00 00 00 70 0C 00 00 00 00 00 00 00 00 00
```

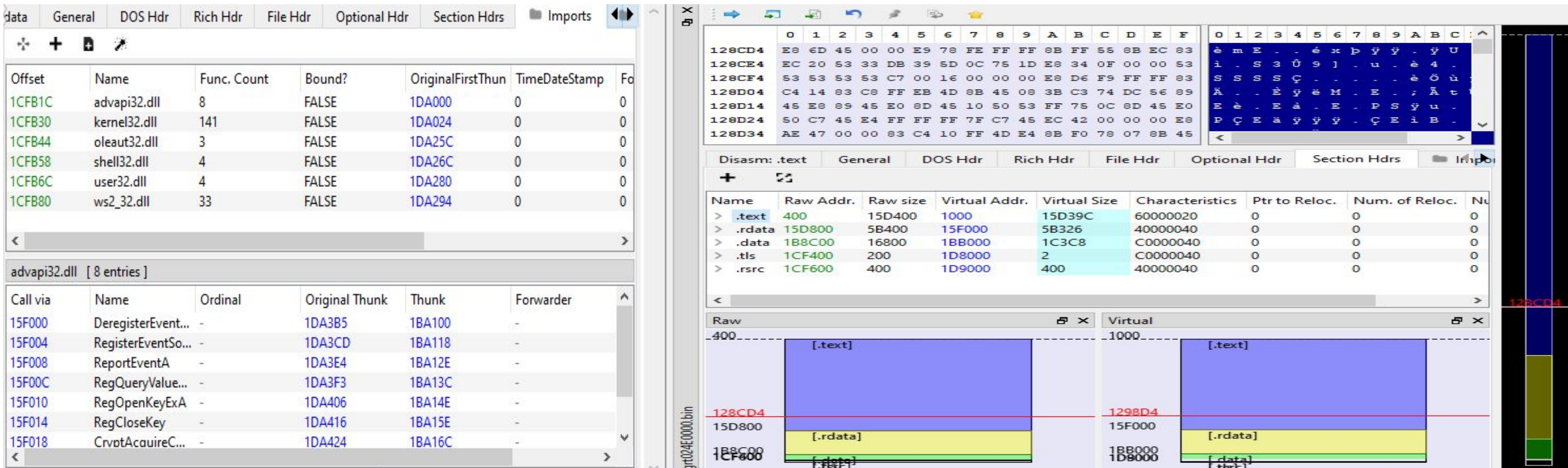
Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Nu
> UPX0	400	0	1000	115000	E0000080	0	0	0
> UPX1	400	C6C00	116000	C7000	E0000040	0	0	0
> .rsrc	C7000	600	1DD000	1000	C0000040	0	0	0

after I dumped the file and opened it in PE-bear we can see that it is packed with upx I unpacked the file using the command upx -d {file_name} and we can see the file size going 800kb -> 1.9mb and lets see the sections now



```
λ upx -d C:\Users\tojme\Desktop\no_more_ransom\grt024E0000.bin
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2024
UPX 4.2.2       Markus Oberhumer, Laszlo Molnar & John Reiser    Jan 3rd 2024

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
   1922048 <-    839680   43.69%    win32/pe     grt024E0000.bin

Unpacked 1 file.
```

Now that the file is unpacked, we can clearly see the sections and the imports of the unpacked file. However, the way I did this was a bit of a 'cheeky hack', as dumping the file in that manner can corrupt the PE file and inject a lot of unnecessary code. I'm still learning the clean and correct way to do this, and it will take me some time to master that approach. Since we have the unpacked file now, let's open it in IDA Pro and start analyzing it.



Offset	Name	Func. Count	Bound?	OriginalFirstThun	TimeDateStamp	Fo
1CFB1C	advapi32.dll	8	FALSE	1DA000	0	0
1CFB30	kernel32.dll	141	FALSE	1DA024	0	0
1CFB44	oleaut32.dll	3	FALSE	1DA25C	0	0
1CFB58	shell32.dll	4	FALSE	1DA26C	0	0
1CFB6C	user32.dll	4	FALSE	1DA280	0	0
1CFB80	ws2_32.dll	33	FALSE	1DA294	0	0

advapi32.dll [8 entries]

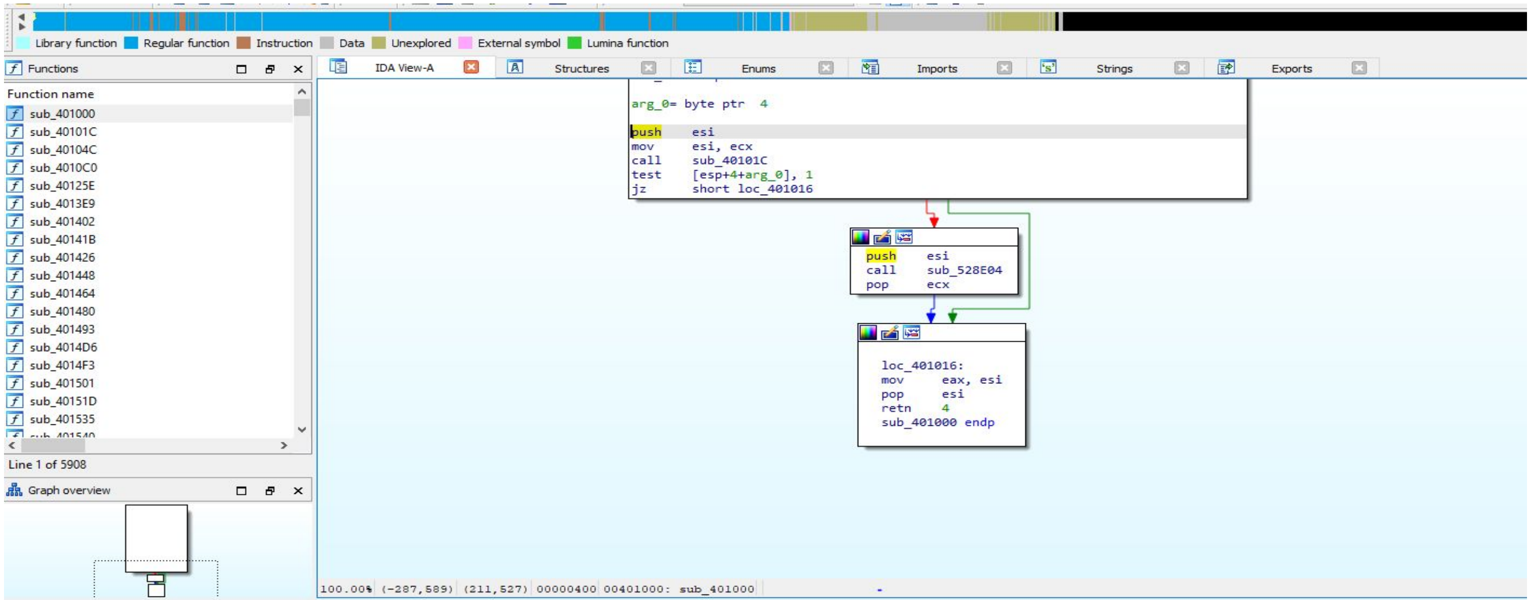
Call via	Name	Ordinal	Original Thunk	Thunk	Forwarder
15F000	DeregisterEvent...	-	1DA3B5	1BA100	-
15F004	RegisterEventSo...	-	1DA3CD	1BA118	-
15F008	ReportEventA	-	1DA3E4	1BA12E	-
15F00C	RegQueryValue...	-	1DA3F3	1BA13C	-
15F010	RegOpenKeyExA	-	1DA406	1BA14E	-
15F014	RegCloseKey	-	1DA416	1BA15E	-
15F018	CryptAcquireC...	-	1DA424	1BA16C	-

```
         0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F    0 1 2 3 4 5 6 7 8 9 A B C
128CD4  E8 6D 45 00 00 E9 78 FE FF FF 8B FF 55 8B EC 83    è m E . . é x þ ÿ ÿ . ÿ U
128CE4  EC 20 53 33 DB 39 5D 0C 75 1D E8 34 0F 00 00 53    ì . S 3 Û 9 ] . u . è 4 .
128CF4  53 53 53 53 C7 00 16 00 00 00 E8 D6 F9 FF FF 83    S S S S Ç . . . . . è Ö ù
128D04  C4 14 83 C8 FF EB 4D 8B 45 08 3B C3 74 DC 56 89    Ä . . È ÿ ë M . E . ; Ã t
128D14  45 E8 89 45 E0 8D 45 10 50 53 FF 75 0C 8D 45 E0    E è . E à . E . P S ÿ u .
128D24  50 C7 45 E4 FF FF FF 7F C7 45 EC 42 00 00 00 E8    P Ç E ä ÿ ÿ ÿ . Ç E ì B .
128D34  AE 47 00 00 83 C4 10 FF 4D E4 8B F0 78 07 8B 45
```

Name	Raw Addr.	Raw size	Virtual Addr.	Virtual Size	Characteristics	Ptr to Reloc.	Num. of Reloc.	Nu
.text	400	15D400	1000	15D39C	60000020	0	0	0
.rdata	15D800	5B400	15F000	5B326	40000040	0	0	0
.data	1B8C00	16800	1BB000	1C3C8	C0000040	0	0	0
.tls	1CF400	200	1D8000	2	C0000040	0	0	0
.rsrc	1CF600	400	1D9000	400	40000040	0	0	0

Debugger analysis

After we opened the new unpacked file, we can see that it is now full of functions and strings. Let's start the analysis to get a bigger picture of how this ransomware is functioning.



Function name

```
sub_401000
sub_40101C
sub_40104C
sub_4010C0
sub_40125E
sub_4013E9
sub_401402
sub_40141B
sub_401426
sub_401448
sub_401464
sub_401480
sub_401493
sub_4014D6
sub_4014F3
sub_401501
sub_40151D
sub_401535
```

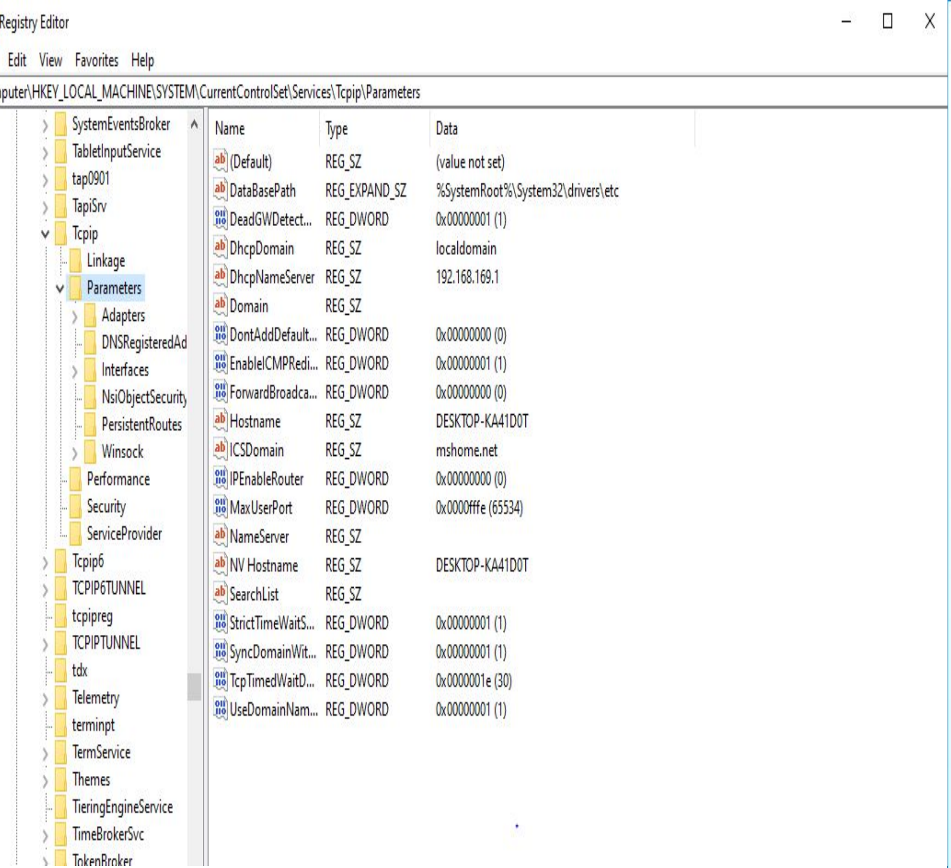
Line 1 of 5908

```
arg_0= byte ptr  4

push    esi
mov     esi, ecx
call    sub_40101C
test    [esp+4+arg_0], 1
jz      short loc_401016
```

```
push    esi
call    sub_528E04
pop     ecx
```

```
loc_401016:
mov     eax, esi
pop     esi
retn    4
sub_401000 endp
```

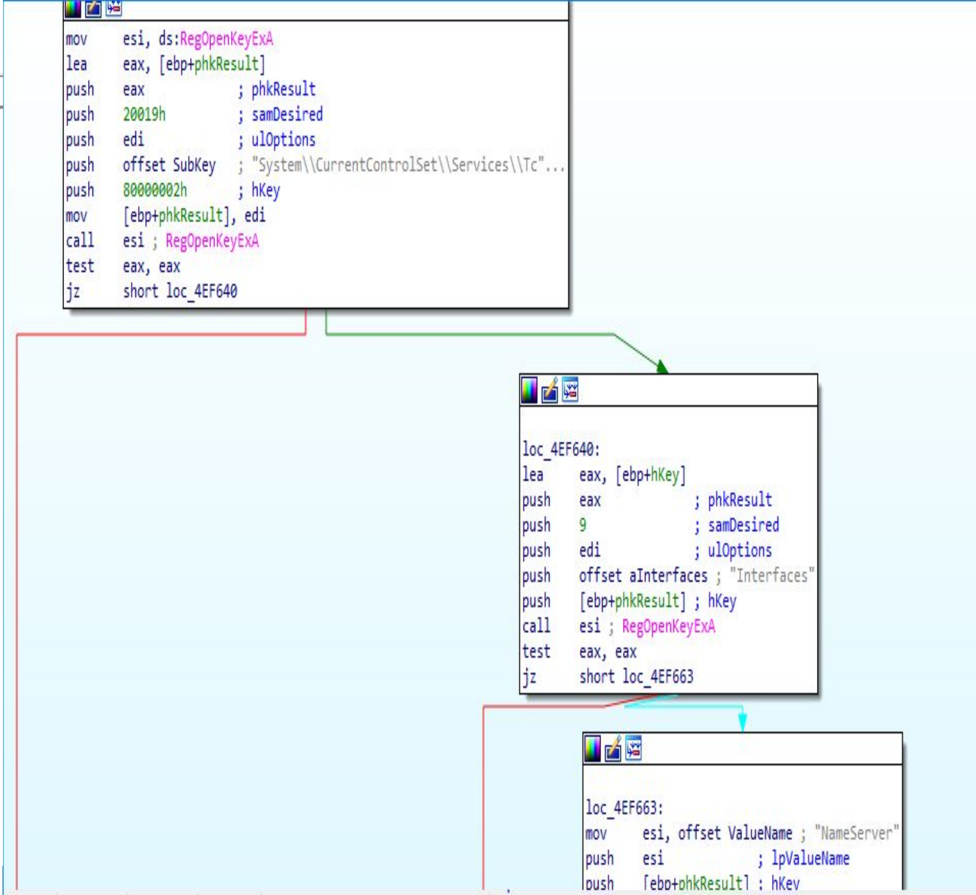
```
100.00% (-287,589) (211,527) 00000400 00401000: sub_401000
```



puter\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters

SystemEventsBroker
TabletInputService
tap0901
TapiSrv
Tcpip
Linkage
Parameters
Adapters
DNSRegisteredAd
Interfaces
NsiObjectSecurity
PersistentRoutes
Winsock
Performance
Security
ServiceProvider
Tcpip6
TCPIP6TUNNEL
tcpipreg
TCPIPTUNNEL
tdx
Telemetry
terminpt
TermService
Themes
TieringEngineService
TimeBrokerSvc
TokenBroker

Name	Type	Data
(Default)	REG_SZ	(value not set)
DataBasePath	REG_EXPAND_SZ	%SystemRoot%\System32\drivers\etc
DeadGWDetect...	REG_DWORD	0x00000001 (1)
DhcpDomain	REG_SZ	localdomain
DhcpNameServer	REG_SZ	192.168.169.1
Domain	REG_SZ	
DontAddDefault...	REG_DWORD	0x00000000 (0)
EnableICMPRedi...	REG_DWORD	0x00000001 (1)
ForwardBroadca...	REG_DWORD	0x00000000 (0)
Hostname	REG_SZ	DESKTOP-KA41D0T
ICSDomain	REG_SZ	mshome.net
IPEnableRouter	REG_DWORD	0x00000000 (0)
MaxUserPort	REG_DWORD	0x0000fffe (65534)
NameServer	REG_SZ	
NV Hostname	REG_SZ	DESKTOP-KA41D0T
SearchList	REG_SZ	
StrictTimeWaitS...	REG_DWORD	0x00000001 (1)
SyncDomainWit...	REG_DWORD	0x00000001 (1)
TcpTimedWaitD...	REG_DWORD	0x0000001e (30)
UseDomainNam...	REG_DWORD	0x00000001 (1)



```
mov     esi, ds:RegOpenKeyExA
lea     eax, [ebp+phkResult]
push    eax             ; phkResult
push    20019h          ; samDesired
push    edi             ; ulOptions
push    offset SubKey   ; "System\\CurrentControlSet\\Services\\Tc"...
push    80000002h       ; hKey
mov     [ebp+phkResult], edi
call    esi ; RegOpenKeyExA
test    eax, eax
jz      short loc_4EF640
```

```
loc_4EF640:
lea     eax, [ebp+hKey]
push    eax                 ; phkResult
push    9                   ; samDesired
push    edi                 ; ulOptions
push    offset aInterfaces ; "Interfaces"
push    [ebp+phkResult] ; hKey
call    esi ; RegOpenKeyExA
test    eax, eax
jz      short loc_4EF663
```

```
loc_4EF663:
mov     esi, offset ValueName ; "NameServer"
push    esi                 ; lpValueName
push    [ebp+phkResult] ; hKey
```

We can see the first IOC this function is loading nameservers from registry to his data like DhcpDomain as we can see below all the registers he changing.

```
HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\Client Server Runtime Subsystem: ""C:\Users\tojme\Desktop\NoMoreRansom.exe""

HKU\S-1-5-21-83331929-1780821005-3884141752-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:000000000003025C

HKU\S-1-5-21-83331929-1780821005-3884141752-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Explorer\SessionInfo\1\ApplicationViewManagement\W32:00000000000500D0

HKU\S-1-5-21-83331929-1780821005-3884141752-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024040620240407

HKU\S-1-5-21-83331929-1780821005-3884141752-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\5.0\Cache\Extensible Cache\MSHist012024040720240408

HKU\S-1-5-21-83331929-1780821005-3884141752-1001\SOFTWARE\System32

HKU\S-1-5-21-83331929-1780821005-3884141752-1001\SOFTWARE\System32\Configuration

HKU\S-1-5-18\Software\Microsoft\Windows\Windows Error Reporting

HKU\S-1-5-21-83331929-1780821005-3884141752-1001\Control Panel\Desktop\WallPaper: "C:\Users\tojme\AppData\Roaming\135E12AD135E12AD.bmp
```

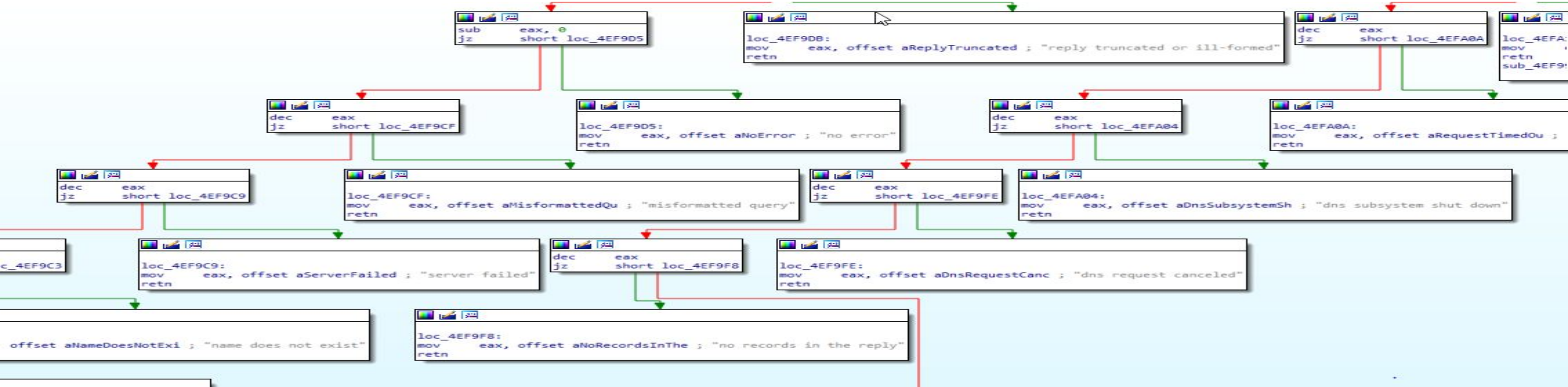
HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\Tcpip\\Parameters

HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\Tcpip\\Parameters\\Interfaces

HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\Tcpip\\Parameters\\DhcpNameServer

HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Services\\VxD\\MSTCP

The malware is taking the NT_KEY from the victim's machine and attempting to locate nameservers using it. From the registry, it is extracting the NT_KEYs and seeding random DNS addresses to create a command-and-control (C2C) server for communicating with the infected machine.



```
sub     eax, 0
jz      short loc_4EF9D5
```

```
loc_4EF9DB:
mov     eax, offset aReplyTruncated ; "reply truncated or ill-formed"
retn
```

```
dec     eax
jz      short loc_4EFA0A
```

```
loc_4EFA
mov
retn
sub_4EF9
```

```
dec     eax
jz      short loc_4EF9CF
```

```
loc_4EF9D5:
mov     eax, offset aNoError ; "no error"
retn
```

```
dec     eax
jz      short loc_4EFA04
```

```
loc_4EFA0A:
mov     eax, offset aRequestTimedOu ;
retn
```

```
dec     eax
jz      short loc_4EF9C9
```

```
loc_4EF9CF:
mov     eax, offset aMisformattedQu ; "misformatted query"
retn
```

```
dec     eax
jz      short loc_4EF9FE
```

```
loc_4EFA04:
mov     eax, offset aDnsSubsystemSh ; "dns subsystem shut down"
retn
```

```
c_4EF9C3
```

```
loc_4EF9C9:
mov     eax, offset aServerFailed ; "server failed"
retn
```

```
dec     eax
jz      short loc_4EF9F8
```

```
loc_4EF9FE:
mov     eax, offset aDnsRequestCanc ; "dns request canceled"
retn
```

```
offset aNameDoesNotExi ; "name does not exist"
```

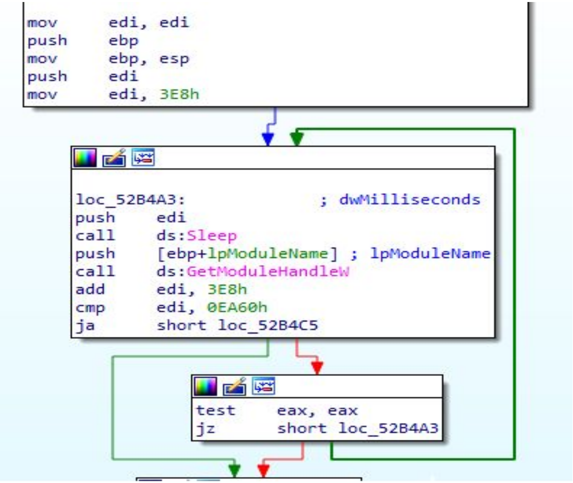
```
loc_4EF9F8:
mov     eax, offset aNoRecordsInThe ; "no records in the reply"
retn
```

the presence of TlsGetValue, along with functions such as GetModuleHandleW, GetProcAddress, and a delay using Sleep, suggests several potential behaviors:

Dynamic Function Resolution: GetProcAddress is used to dynamically resolve the address of "decodePointer" and "encodePointer" from kernel32.dll, indicating adaptability and potential obfuscation strategies.

Evasion and Delay Tactics: The presence of a Sleep call suggests evasion tactics to bypass automated analysis, delaying execution by 16 minutes before proceeding

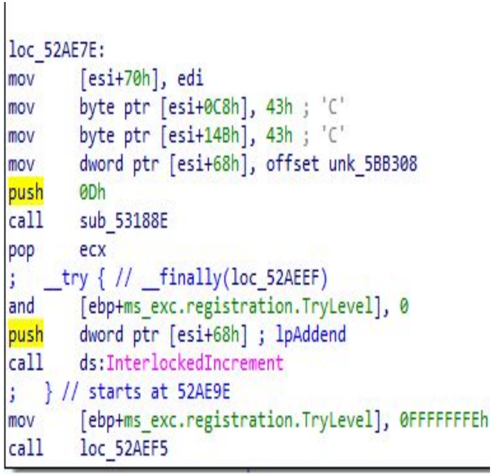
InterlockedIncrement provides a way for malware to safely increment shared variables in a multi-threaded environment, enabling synchronization, concurrency control, and other related tasks



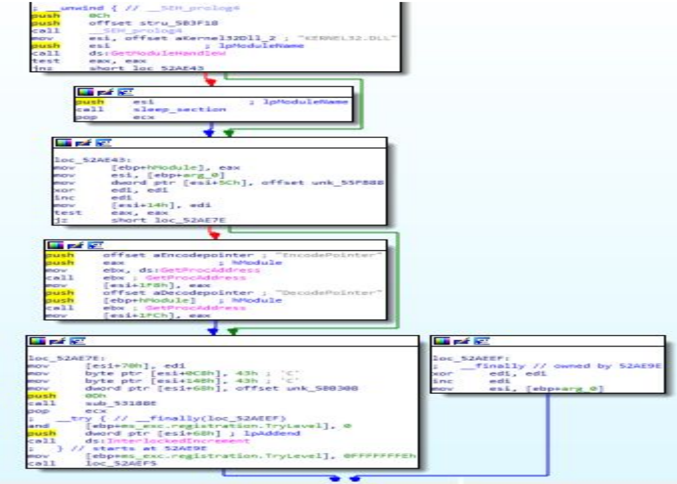
```
mov     edi, edi
push    ebp
mov     ebp, esp
push    edi
mov     edi, 3E8h
```

```
loc_52B4A3:                 ; dwMilliseconds
push    edi
call    ds:Sleep
push    [ebp+lpModuleName] ; lpModuleName
call    ds:GetModuleHandleW
add     edi, 3E8h
cmp     edi, 0EA60h
ja      short loc_52B4C5
```

```
test    eax, eax
jz      short loc_52B4A3
```



```
loc_52AE7E:
mov     [esi+70h], edi
mov     byte ptr [esi+0C8h], 43h ; 'C'
mov     byte ptr [esi+14Bh], 43h ; 'C'
mov     dword ptr [esi+68h], offset unk_5BB308
push    0Dh
call    sub_53188E
pop     ecx
;   __try { // __finally(loc_52AEEF)
and     [ebp+ms_exc.registration.TryLevel], 0
push    dword ptr [esi+68h] ; lpAddend
call    ds:InterlockedIncrement
;   } // starts at 52AE9E
mov     [ebp+ms_exc.registration.TryLevel], 0FFFFFFFEh
call    loc_52AEF5
```



```
; __unwind { // __SEH_prolog4
push    0Ch
push    offset stru_5B3F18
call    __SEH_prolog4
mov     esi, offset aKernel32Dll_2 ; "KERNEL32.DLL"
push    esi             ; lpModuleName
call    ds:GetModuleHandleW
test    eax, eax
jnz     short loc_52AE43
```

```
push    esi             ; lpModuleName
call    sleep_section
pop     ecx
```

```
loc_52AE43:
mov     [ebp+hModule], eax
mov     esi, [ebp+arg_0]
mov     dword ptr [esi+5Ch], offset unk_55F888
xor     edi, edi
inc     edi
mov     [esi+14h], edi
test    eax, eax
jz      short loc_52AE7E
```

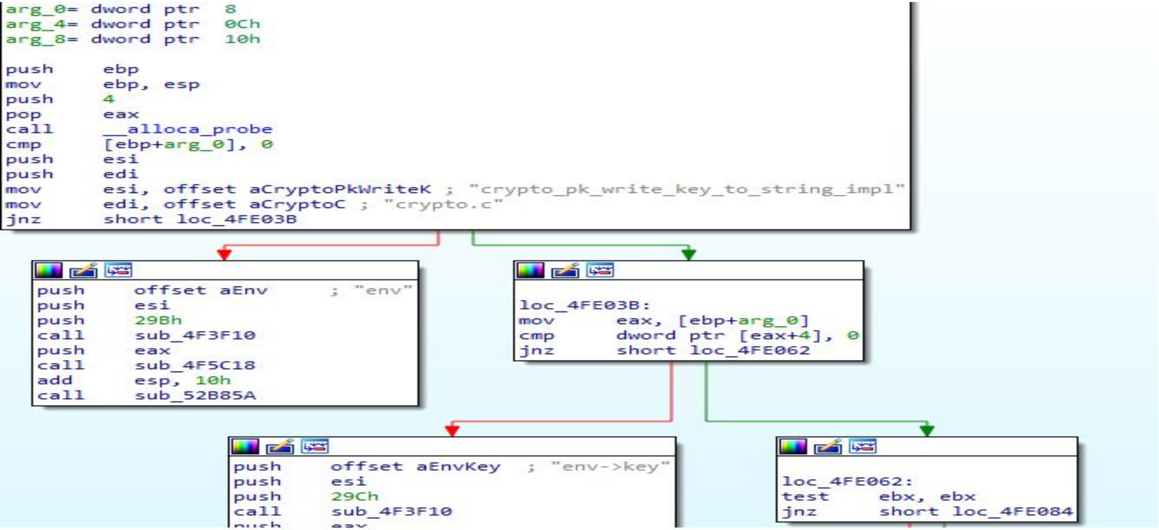
```
push    offset aEncodepointer ; "EncodePointer"
push    eax             ; hModule
mov     ebx, ds:GetProcAddress
call    ebx ; GetProcAddress
mov     [esi+1F8h], eax
push    offset aDecodepointer ; "DecodePointer"
push    [ebp+hModule]   ; hModule
call    ebx ; GetProcAddress
mov     [esi+1FCh], eax
```

```
loc_52AE7E:
mov     [esi+70h], edi
mov     byte ptr [esi+0C8h], 43h ; 'C'
mov     byte ptr [esi+14Bh], 43h ; 'C'
mov     dword ptr [esi+68h], offset unk_5B8308
push    0Dh
call    sub_53188E
pop     ecx
;   __try { // __finally(loc_52AEEF)
and     [ebp+ms_exc.registration.TryLevel], 0
push    dword ptr [esi+68h] ; lpAddend
call    ds:InterlockedIncrement
;   } // starts at 52AE9E
mov     [ebp+ms_exc.registration.TryLevel], 0FFFFFFFEh
call    loc_52AEF5
```

```
loc_52AEEF:
;   __finally // owned by 52AE9E
xor     edi, edi
inc     edi
mov     esi, [ebp+arg_0]
```

Encryption

As we can see in this code, the malware is creating a file called 'crypto.c' and storing all of the encryption data there, such as the RSA and AES keys. We can see that it's using both symmetric and asymmetric encryption for the data, but we need to find its communication with the server. It's using functions from this file, like 'importPK' and 'writeToString', to handle the encryption and communication.



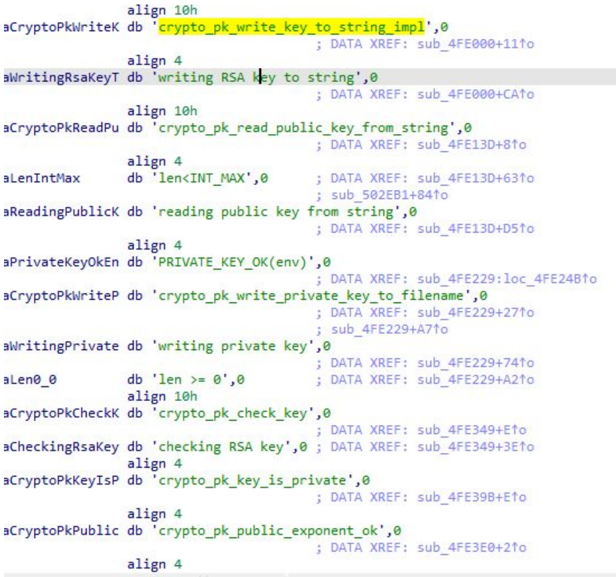
```
arg_0= dword ptr  8
arg_4= dword ptr  0Ch
arg_8= dword ptr  10h

push    ebp
mov     ebp, esp
push    4
pop     eax
call    __alloca_probe
cmp     [ebp+arg_0], 0
push    esi
push    edi
mov     esi, offset aCryptoPkWriteK ; "crypto_pk_write_key_to_string_impl"
mov     edi, offset aCryptoC ; "crypto.c"
jnz     short loc_4FE03B
```

```
push    offset aEnv     ; "env"
push    esi
push    29Bh
call    sub_4F3F10
push    eax
call    sub_4F5C18
add     esp, 10h
call    sub_52B85A
```

```
loc_4FE03B:
mov     eax, [ebp+arg_0]
cmp     dword ptr [eax+4], 0
jnz     short loc_4FE062
```

```
push    offset aEnvKey  ; "env->key"
push    esi
push    29Ch
call    sub_4F3F10
```

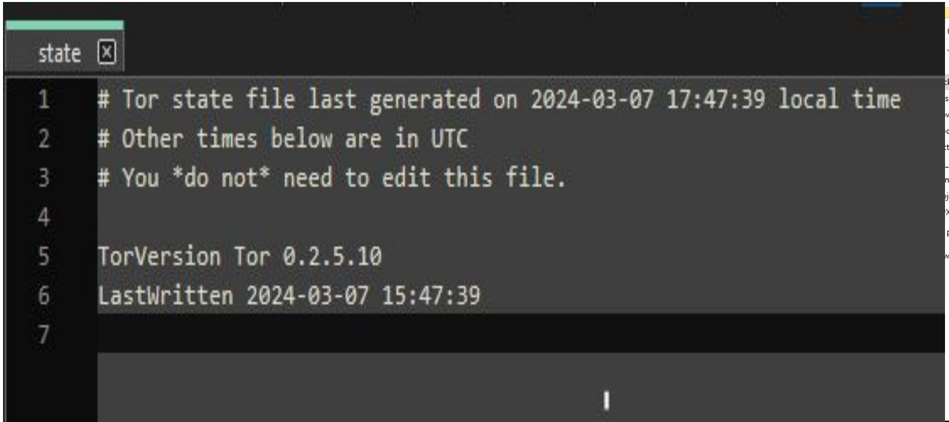
```
loc_4FE062:
test    ebx, ebx
jnz     short loc_4FE084
```



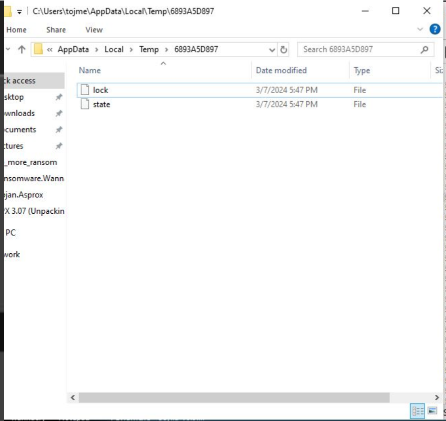
```
                align 10h
aCryptoPkWriteK db 'crypto_pk_write_key_to_string_impl',0
                                        ; DATA XREF: sub_4FE000+11↑o
                align 4
aWritingRsaKeyT db 'writing RSA key to string',0
                                        ; DATA XREF: sub_4FE000+CA↑o
                align 10h
aCryptoPkReadPu db 'crypto_pk_read_public_key_from_string',0
                                        ; DATA XREF: sub_4FE13D+8↑o
                align 4
aLenIntMax      db 'len<INT_MAX',0      ; DATA XREF: sub_4FE13D+63↑o
                                        ; sub_502EB1+84↑o
aReadingPublicK db 'reading public key from string',0
                                        ; DATA XREF: sub_4FE13D+D5↑o
                align 4
aPrivateKeyOkEn db 'PRIVATE_KEY_OK(env)',0
                                        ; DATA XREF: sub_4FE229:loc_4FE24B↑o
aCryptoPkWriteP db 'crypto_pk_write_private_key_to_filename',0
                                        ; DATA XREF: sub_4FE229+27↑o
                                        ; sub_4FE229+A7↑o
aWritingPrivate db 'writing private key',0
                                        ; DATA XREF: sub_4FE229+74↑o
aLen0_0         db 'len >= 0',0         ; DATA XREF: sub_4FE229+A2↑o
                align 10h
aCryptoPkCheckK db 'crypto_pk_check_key',0
                                        ; DATA XREF: sub_4FE349+E↑o
aCheckingRsaKey db 'checking RSA key',0 ; DATA XREF: sub_4FE349+3E↑o
                align 4
aCryptoPkKeyIsP db 'crypto_pk_key_is_private',0
                                        ; DATA XREF: sub_4FE39B+E↑o
                align 4
aCryptoPkPublic db 'crypto_pk_public_exponent_ok',0
                                        ; DATA XREF: sub_4FE3E0+2↑o
                align 4
```

Dynamic analysis

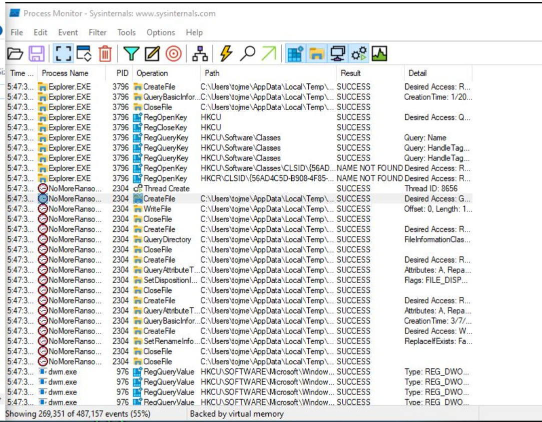
Another Indicator of Compromise (IOC) is that when I ran the malware and followed it in Process Monitor, I observed it creating files in the %TEMP% directory. Specifically, I found two files, and when I opened the one with data (the 'state' file), I could see that its contents were related to the Tor browser. This suggests that the malware is creating a connection, likely to its Tor-based C2 server, to start the process of encrypting the victim's files.



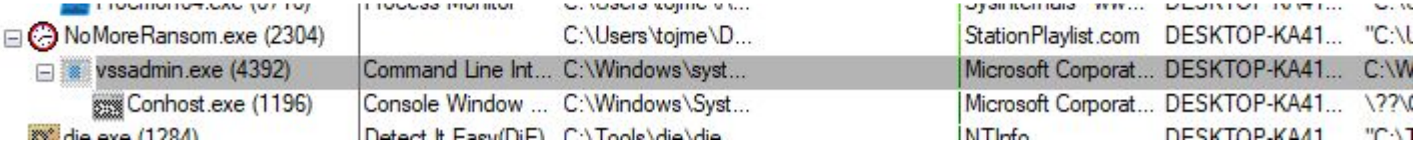
```
# Tor state file last generated on 2024-03-07 17:47:39 local time
# Other times below are in UTC
# You *do not* need to edit this file.

TorVersion Tor 0.2.5.10
LastWritten 2024-03-07 15:47:39
```



Name	Date modified	Type
lock	3/7/2024 5:47 PM	File
state	3/7/2024 5:47 PM	File

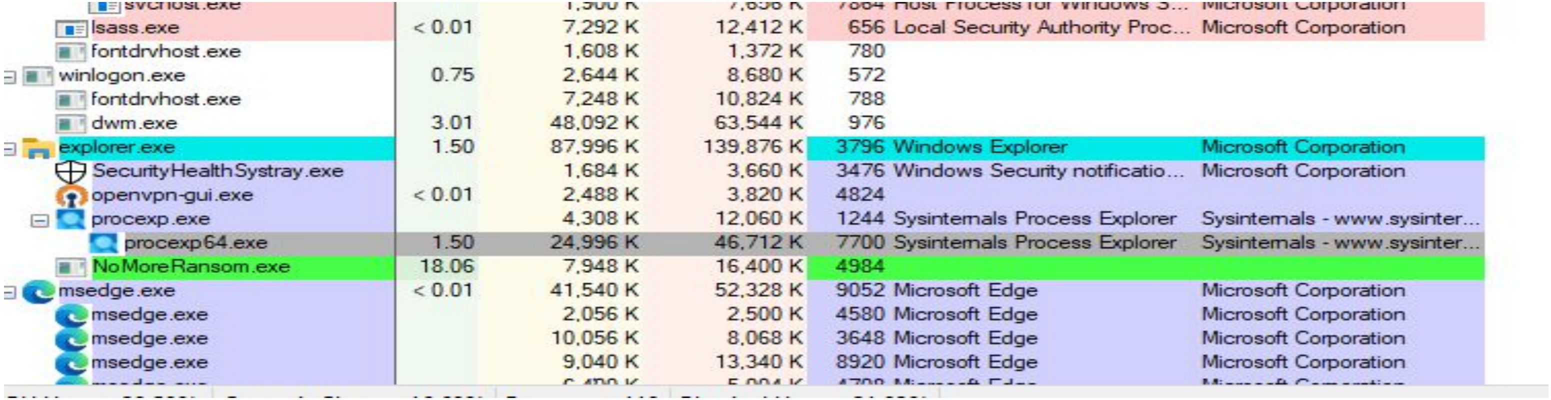


```
Time ...  Process Name     PID   Operation          Path                                      Result           Detail
5:47:3... Explorer.EXE     3796  CreateFile         C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Desired Access: R...
5:47:3... Explorer.EXE     3796  QueryBasicInfor... C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          CreationTime: 1/20...
5:47:3... Explorer.EXE     3796  CloseFile          C:\Users\tojme\AppData\Local\Temp\...     SUCCESS
5:47:3... Explorer.EXE     3796  RegOpenKey         HKCU                                      SUCCESS          Desired Access: Q...
5:47:3... Explorer.EXE     3796  RegCloseKey        HKCU                                      SUCCESS
5:47:3... Explorer.EXE     3796  RegQueryKey        HKCU\Software\Classes                     SUCCESS          Query: Name
5:47:3... Explorer.EXE     3796  RegQueryKey        HKCU\Software\Classes                     SUCCESS          Query: HandleTag...
5:47:3... Explorer.EXE     3796  RegQueryKey        HKCU\Software\Classes                     SUCCESS          Query: HandleTag...
5:47:3... Explorer.EXE     3796  RegOpenKey         HKCU\Software\Classes\CLSID\{56AD...      NAME NOT FOUND   Desired Access: R...
5:47:3... Explorer.EXE     3796  RegOpenKey         HKCR\CLSID\{56AD4C5D-B908-4F85-...        NAME NOT FOUND   Desired Access: R...
5:47:3... NoMoreRanso...   2304  Thread Create                                                SUCCESS          Thread ID: 8656
5:47:3... NoMoreRanso...   2304  CreateFile         C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Desired Access: G...
5:47:3... NoMoreRanso...   2304  WriteFile          C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Offset: 0, Length: 1...
5:47:3... NoMoreRanso...   2304  CloseFile          C:\Users\tojme\AppData\Local\Temp\...     SUCCESS
5:47:3... NoMoreRanso...   2304  CreateFile         C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Desired Access: R...
5:47:3... NoMoreRanso...   2304  QueryDirectory     C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          FileInformationClas...
5:47:3... NoMoreRanso...   2304  CloseFile          C:\Users\tojme\AppData\Local\Temp\...     SUCCESS
5:47:3... NoMoreRanso...   2304  CreateFile         C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Desired Access: R...
5:47:3... NoMoreRanso...   2304  QueryAttributeT... C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Attributes: A, Repa...
5:47:3... NoMoreRanso...   2304  SetDispositionI... C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Flags: FILE_DISP...
5:47:3... NoMoreRanso...   2304  CloseFile          C:\Users\tojme\AppData\Local\Temp\...     SUCCESS
5:47:3... NoMoreRanso...   2304  CreateFile         C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Desired Access: R...
5:47:3... NoMoreRanso...   2304  QueryAttributeT... C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Attributes: A, Repa...
5:47:3... NoMoreRanso...   2304  QueryBasicInfor... C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          CreationTime: 3/7/...
5:47:3... NoMoreRanso...   2304  CreateFile         C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          Desired Access: W...
5:47:3... NoMoreRanso...   2304  SetRenameInfo...   C:\Users\tojme\AppData\Local\Temp\...     SUCCESS          ReplaceIfExists: Fa...
5:47:3... NoMoreRanso...   2304  CloseFile          C:\Users\tojme\AppData\Local\Temp\...     SUCCESS
5:47:3... NoMoreRanso...   2304  CloseFile          C:\Users\tojme\AppData\Local\Temp\...     SUCCESS
5:47:3... dwm.exe           976  RegQueryValue      HKCU\SOFTWARE\Microsoft\Window...         SUCCESS          Type: REG_DWO...
5:47:3... dwm.exe           976  RegQueryValue      HKCU\SOFTWARE\Microsoft\Window...         SUCCESS          Type: REG_DWO...
5:47:3... dwm.exe           976  RegQueryValue      HKCU\SOFTWARE\Microsoft\Window...         SUCCESS          Type: REG_DWO...
5:47:3... dwm.exe           976  RegQueryValue      HKCU\SOFTWARE\Microsoft\Window...         SUCCESS          Type: REG_DWO...
Showing 269,351 of 487,157 events (55%)      Backed by virtual memory
```

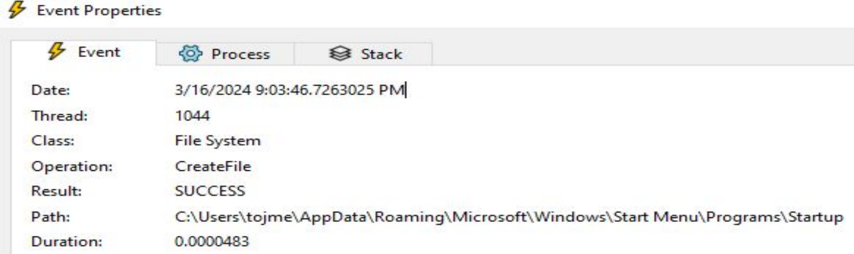


NoMoreRansom.exe (2304)		C:\Users\tojme\D...	StationPlaylist.com	DESKTOP-KA41...	"C:\U
vssadmin.exe (4392)	Command Line Int...	C:\Windows\syst...	Microsoft Corporat...	DESKTOP-KA41...	C:\W
Conhost.exe (1196)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-KA41...	\??\
die.exe (1284)	Detect It Easy(DiE)	C:\Tools\die\die	NTInfo	DESKTOP-KA41	"C:\T

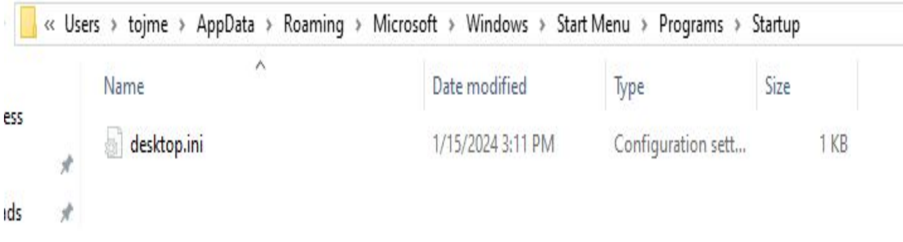
First indication of unpacking is that it's not creating another process or child process like injection, it's just unpacking itself. As we can see in the picture, it's creating another process called vssadmin.exe, which is probably to delete snapshots of the VM, so that means your backup is gone, and you can't restore to an older version before you opened the malware.



lsass.exe	< 0.01	7,292 K	12,412 K	656	Local Security Authority Proc...	Microsoft Corporation
fontdrvhost.exe		1,608 K	1,372 K	780		
winlogon.exe	0.75	2,644 K	8,680 K	572		
fontdrvhost.exe		7,248 K	10,824 K	788		
dwm.exe	3.01	48,092 K	63,544 K	976		
explorer.exe	1.50	87,996 K	139,876 K	3796	Windows Explorer	Microsoft Corporation
SecurityHealthSystray.exe		1,684 K	3,660 K	3476	Windows Security notificatio...	Microsoft Corporation
openvpn-gui.exe	< 0.01	2,488 K	3,820 K	4824		
procexp.exe		4,308 K	12,060 K	1244	Sysinternals Process Explorer	Sysinternals - www.sysinter...
procexp64.exe	1.50	24,996 K	46,712 K	7700	Sysinternals Process Explorer	Sysinternals - www.sysinter...
NoMoreRansom.exe	18.06	7,948 K	16,400 K	4984		
msedge.exe	< 0.01	41,540 K	52,328 K	9052	Microsoft Edge	Microsoft Corporation
msedge.exe		2,056 K	2,500 K	4580	Microsoft Edge	Microsoft Corporation
msedge.exe		10,056 K	8,068 K	3648	Microsoft Edge	Microsoft Corporation
msedge.exe		9,040 K	13,340 K	8920	Microsoft Edge	Microsoft Corporation



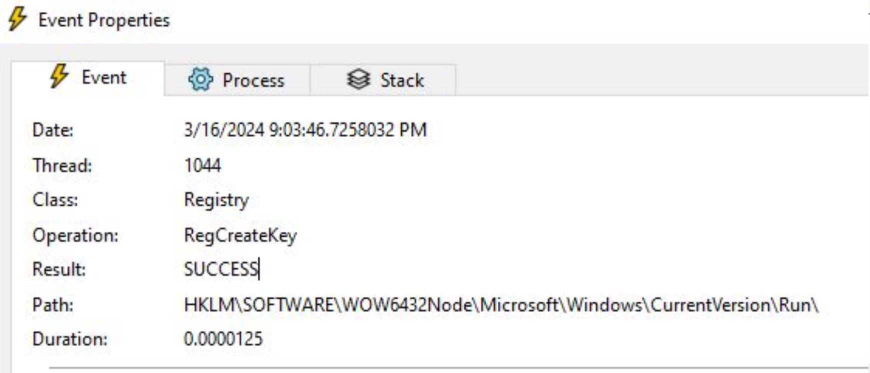
Date: 3/16/2024 9:03:46.7263025 PM
Thread: 1044
Class: File System
Operation: CreateFile
Result: SUCCESS
Path: C:\Users\tojme\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup
Duration: 0.0000483



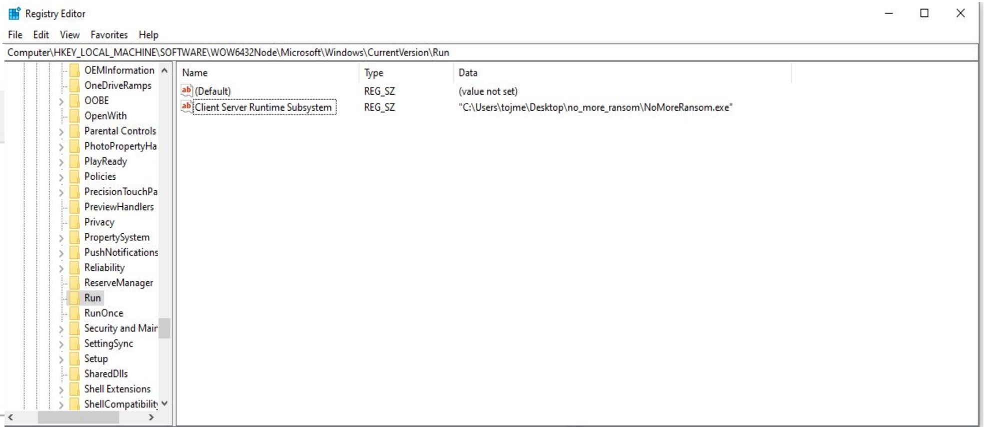
« Users › tojme › AppData › Roaming › Microsoft › Windows › Start Menu › Programs › Startup
ess
ıds

Name	Date modified	Type	Size
desktop.ini	1/15/2024 3:11 PM	Configuration sett...	1 KB

The creation of the registry entry means that whenever the victim restarts their computer or logs into Windows, the malware executable referenced by that registry entry will automatically launch. This effectively re-infects the system each time the computer starts up. Additionally, the malware is injecting this data into the startup programs folder, further ensuring its persistence on the infected system.

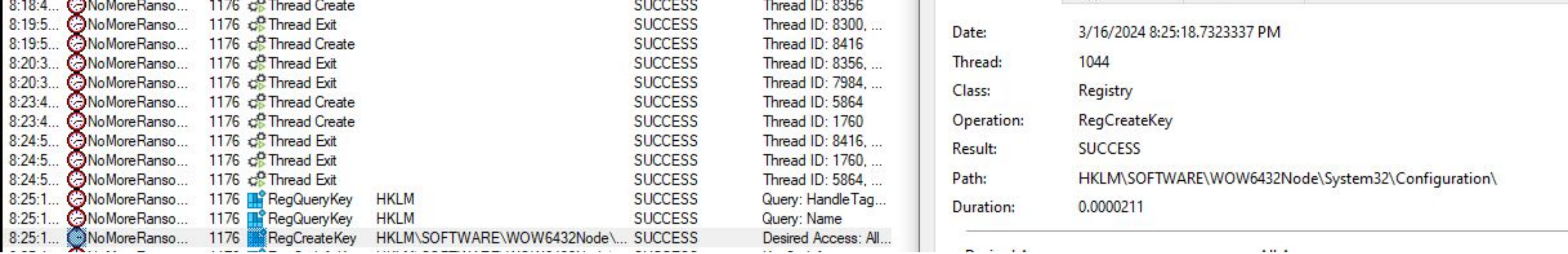


Date: 3/16/2024 9:03:46.7258032 PM
Thread: 1044
Class: Registry
Operation: RegCreateKey
Result: SUCCESS
Path: HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\
Duration: 0.0000125



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run

Name	Type	Data
(Default)	REG_SZ	(value not set)
Client Server Runtime Subsystem	REG_SZ	"C:\Users\tojme\Desktop\no_more_ransom\NoMoreRansom.exe"



```
8:18:4... NoMoreRanso... 1176 Thread Create                                     SUCCESS  Thread ID: 8356
8:19:5... NoMoreRanso... 1176 Thread Exit                                       SUCCESS  Thread ID: 8300, ...
8:19:5... NoMoreRanso... 1176 Thread Create                                     SUCCESS  Thread ID: 8416
8:20:3... NoMoreRanso... 1176 Thread Exit                                       SUCCESS  Thread ID: 8356, ...
8:20:3... NoMoreRanso... 1176 Thread Exit                                       SUCCESS  Thread ID: 7984, ...
8:23:4... NoMoreRanso... 1176 Thread Create                                     SUCCESS  Thread ID: 5864
8:23:4... NoMoreRanso... 1176 Thread Create                                     SUCCESS  Thread ID: 1760
8:24:5... NoMoreRanso... 1176 Thread Exit                                       SUCCESS  Thread ID: 8416, ...
8:24:5... NoMoreRanso... 1176 Thread Exit                                       SUCCESS  Thread ID: 1760, ...
8:24:5... NoMoreRanso... 1176 Thread Exit                                       SUCCESS  Thread ID: 5864, ...
8:25:1... NoMoreRanso... 1176 RegQueryKey   HKLM                                SUCCESS  Query: HandleTag...
8:25:1... NoMoreRanso... 1176 RegQueryKey   HKLM                                SUCCESS  Query: Name
8:25:1... NoMoreRanso... 1176 RegCreateKey  HKLM\SOFTWARE\WOW6432Node\...       SUCCESS  Desired Access: All...
```

```
Date:       3/16/2024 8:25:18.7323337 PM
Thread:     1044
Class:      Registry
Operation:  RegCreateKey
Result:     SUCCESS
Path:       HKLM\SOFTWARE\WOW6432Node\System32\Configuration\
Duration:   0.0000211
```

Another IOC is the public key he's bringing, he's setting it as a registry. This is asymmetric encryption which means he's sending his public key to start encrypt files on the victim machine.

Public key:

–MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigKCAYEAZXhnkH11n+xqxQcisQj5

OefrHjVnqNj+WJAhxscQ4711oTW8X82MNpwTr6ZWWWHTNB0uoppja4vH34ZPFFow

5F/vnPoHa027gaWAZg701CI1UeMrKQvRSDYjW8HEHp016qfsPDWqOIUCpI/oAgpY

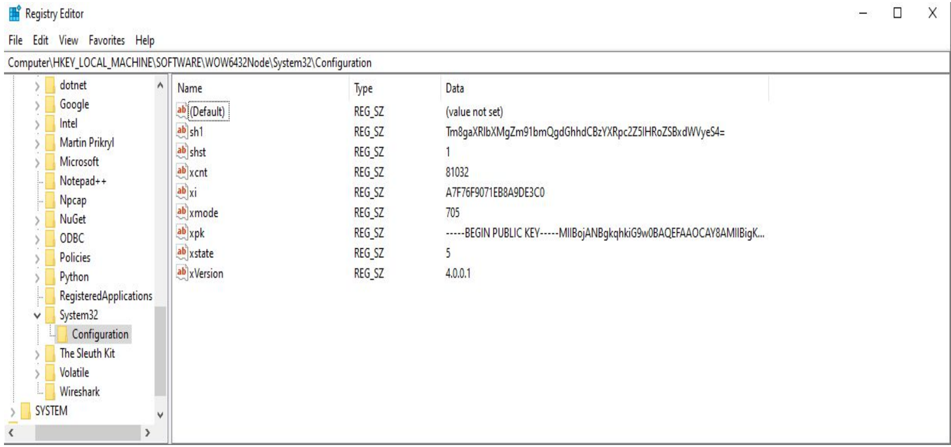
XC5neQgNUgQcc06edxoZipUS1LZ5H8c+/996RNOMONZawLBOLOWAHSDYLVHgt2z

vsn43Z+nQbTzJtjHn9rtwv7ppecgE3JHTYQ4qI3T0CtF6Ss082mDqk7UPG3kqMb2

013/g2G7u6vCtB951pbvG9A6z//zD2zwhufn608LRURVOUDRQaQGIxgCWD8KsLLS

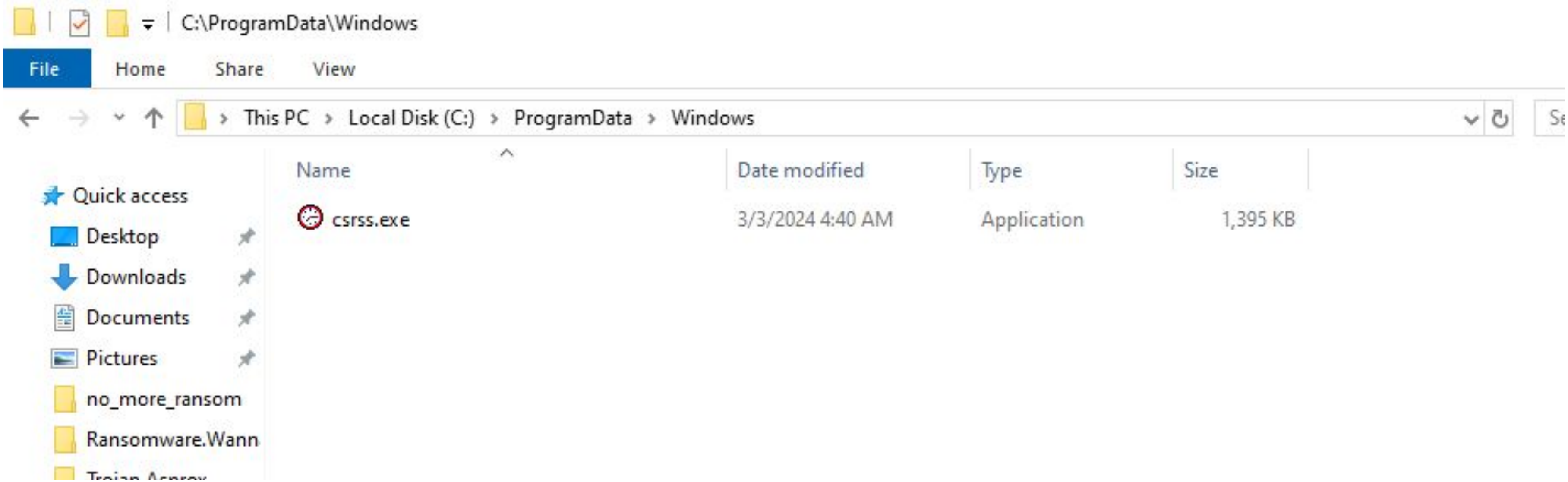
fiXIBiemeVuHbOzK6cgaBR8K0Lcy1nnXo4gNZdDSRKFDCVAh4bS18GztPYUSVFMG 5m8weQyyuABQ300/AKTCHZ1JPF00uyGfJkzc3UjfgMrJD5EgF1dwA9kTZIi1K7Tp

giHSsh+/Mht6w97yUw/RiCOvbln FC8JV/sn7Tc3/q767AgMBAAE–



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\System32\Configuration

Name	Type	Data
(Default)	REG_SZ	(value not set)
sh1	REG_SZ	Tm8gaXRlbXMgZm91bmQgdGhhdCBzYXRpc2Z5IHRoZSBxdWVyeS4=
shst	REG_SZ	1
xcnt	REG_SZ	81032
xi	REG_SZ	A7F76F9071EB8A9DE3C0
xmode	REG_SZ	705
xpk	REG_SZ	-----BEGIN PUBLIC KEY-----MIIBojANBgkqhkiG9w0BAQEFAAOCAY8AMIIBigK...
xstate	REG_SZ	5
xVersion	REG_SZ	4.0.0.1



Name	Date modified	Type	Size
csrss.exe	3/3/2024 4:40 AM	Application	1,395 KB

Also the malware duplicated itself and changed its name to csrss.exe, By placing a copy of the malware executable in the ProgramData folder, the ransomware is ensuring that it will persist and run automatically on the system, even after a reboot

Network Analysis

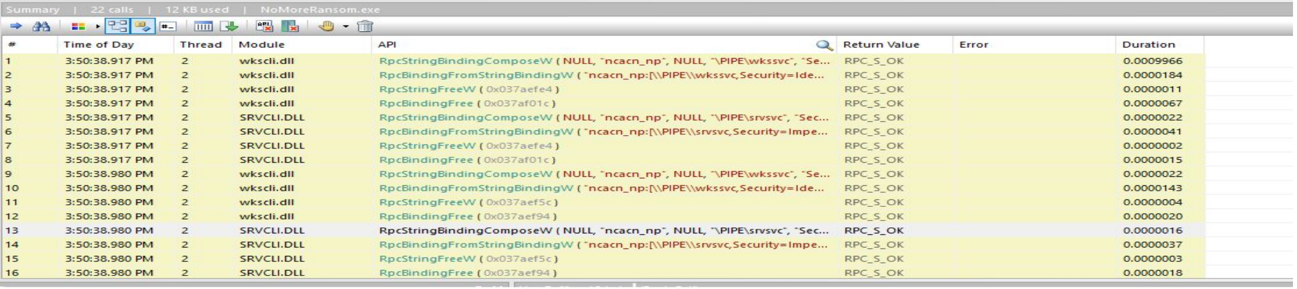
This network analysis was pretty hard because the malware was using encrypted connections, so you couldn't see it under Wireshark because it relies on analyzing clear-text network traffic. What I did instead was trace its network APIs under API Monitor and found out that it was creating a pipe to its C2 server using the RpcStringBindingCompose API. This API is used to create a 'connection string' that identifies how two software components can communicate with each other over a network

the connection string: `ncacn_np:[\\PIPE\srvsvc,Security=Impersonation Dynamic False]`

`ncacn_np:[\\PIPE\srvsvc,Security=Impersonation Dynamic False]`

This connection string is telling the Windows networking system a few things:

1. It wants to use the "Named Pipes" protocol to communicate (`ncacn_np`).
2. It specifically wants to connect to the `srvsvc` named pipe on the local system.
3. It wants to impersonate the current user's security credentials when making the connection (`Security=Impersonation Dynamic False`).

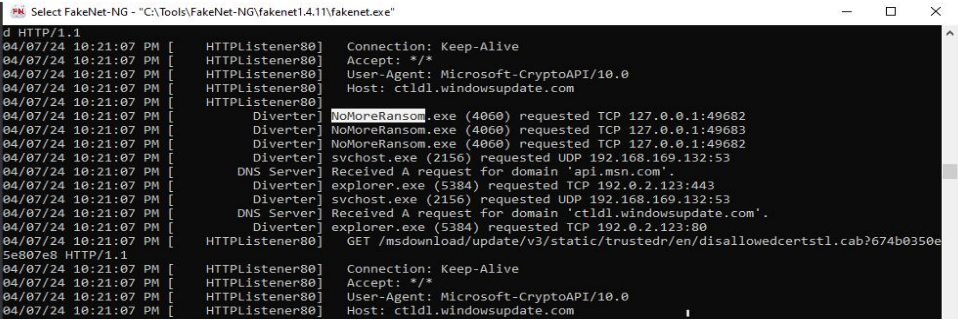


Summary | 22 calls | 12 KB used | NoMoreRansom.exe

#	Time of Day	Thread	Module	API	Return Value	Error	Duration
1	3:50:38.917 PM	2	wkscli.dll	RpcStringBindingComposeW (NULL, "ncacn_np", NULL, "\PIPE\wkssvc", "Se...	RPC_S_OK		0.0009966
2	3:50:38.917 PM	2	wkscli.dll	RpcBindingFromStringBindingW ("ncacn_np:[\\PIPE\\wkssvc,Security=Ide...	RPC_S_OK		0.0000184
3	3:50:38.917 PM	2	wkscli.dll	RpcStringFreeW (0x037aefe4)	RPC_S_OK		0.0000011
4	3:50:38.917 PM	2	wkscli.dll	RpcBindingFree (0x037af01c)	RPC_S_OK		0.0000067
5	3:50:38.917 PM	2	SRVCLI.DLL	RpcStringBindingComposeW (NULL, "ncacn_np", NULL, "\PIPE\srvsvc", "Sec...	RPC_S_OK		0.0000022
6	3:50:38.917 PM	2	SRVCLI.DLL	RpcBindingFromStringBindingW ("ncacn_np:[\\PIPE\\srvsvc,Security=Impe...	RPC_S_OK		0.0000041
7	3:50:38.917 PM	2	SRVCLI.DLL	RpcStringFreeW (0x037aefe4)	RPC_S_OK		0.0000002
8	3:50:38.917 PM	2	SRVCLI.DLL	RpcBindingFree (0x037af01c)	RPC_S_OK		0.0000015
9	3:50:38.980 PM	2	wkscli.dll	RpcStringBindingComposeW (NULL, "ncacn_np", NULL, "\PIPE\wkssvc", "Se...	RPC_S_OK		0.0000022
10	3:50:38.980 PM	2	wkscli.dll	RpcBindingFromStringBindingW ("ncacn_np:[\\PIPE\\wkssvc,Security=Ide...	RPC_S_OK		0.0000143
11	3:50:38.980 PM	2	wkscli.dll	RpcStringFreeW (0x037aef5c)	RPC_S_OK		0.0000004
12	3:50:38.980 PM	2	wkscli.dll	RpcBindingFree (0x037aef94)	RPC_S_OK		0.0000020
13	3:50:38.980 PM	2	SRVCLI.DLL	RpcStringBindingComposeW (NULL, "ncacn_np", NULL, "\PIPE\srvsvc", "Sec...	RPC_S_OK		0.0000016
14	3:50:38.980 PM	2	SRVCLI.DLL	RpcBindingFromStringBindingW ("ncacn_np:[\\PIPE\\srvsvc,Security=Impe...	RPC_S_OK		0.0000037
15	3:50:38.980 PM	2	SRVCLI.DLL	RpcStringFreeW (0x037aef5c)	RPC_S_OK		0.0000003
16	3:50:38.980 PM	2	SRVCLI.DLL	RpcBindingFree (0x037aef94)	RPC_S_OK		0.0000018

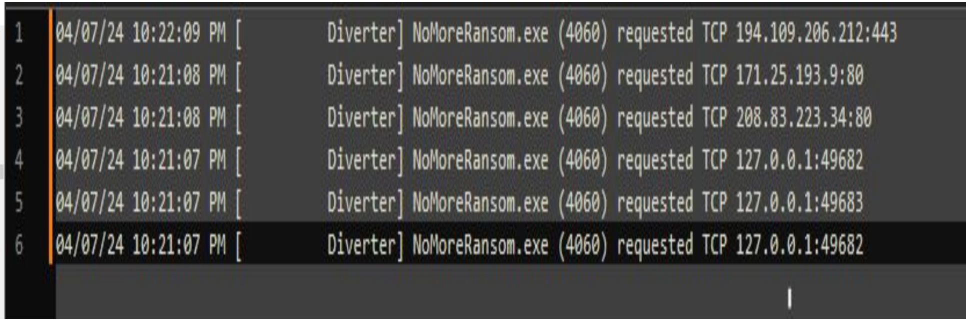
I captured the malware's network traffic using Fakenet-NG and found that it was making TCP requests to its command-and-control server. These requests were likely part of the malware's process of unpacking and encrypting files on the infected system.

```
[           Diverter] NoMoreRansom.exe (4060) requested TCP 194.109.206.212:443

[           Diverter] NoMoreRansom.exe (4060) requested TCP 171.25.193.9:80

[           Diverter] NoMoreRansom.exe (4060) requested TCP 208.83.223.34:80

[           Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49682

[           Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49683

[           Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49682
```



Select FakeNet-NG - "C:\Tools\FakeNet-NG\fakenet1.4.11\fakenet.exe"

```
d HTTP/1.1
04/07/24 10:21:07 PM [    HTTPListener80]   Connection: Keep-Alive
04/07/24 10:21:07 PM [    HTTPListener80]   Accept: */*
04/07/24 10:21:07 PM [    HTTPListener80]   User-Agent: Microsoft-CryptoAPI/10.0
04/07/24 10:21:07 PM [    HTTPListener80]   Host: ctldl.windowsupdate.com
04/07/24 10:21:07 PM [    HTTPListener80]
04/07/24 10:21:07 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49682
04/07/24 10:21:07 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49683
04/07/24 10:21:07 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49682
04/07/24 10:21:07 PM [          Diverter] svchost.exe (2156) requested UDP 192.168.169.132:53
04/07/24 10:21:07 PM [        DNS Server] Received A request for domain 'api.msn.com'.
04/07/24 10:21:07 PM [          Diverter] explorer.exe (5384) requested TCP 192.0.2.123:443
04/07/24 10:21:07 PM [          Diverter] svchost.exe (2156) requested UDP 192.168.169.132:53
04/07/24 10:21:07 PM [        DNS Server] Received A request for domain 'ctldl.windowsupdate.com'.
04/07/24 10:21:07 PM [          Diverter] explorer.exe (5384) requested TCP 192.0.2.123:80
04/07/24 10:21:07 PM [    HTTPListener80]   GET /msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?674b0350e
5e807e8 HTTP/1.1
04/07/24 10:21:07 PM [    HTTPListener80]   Connection: Keep-Alive
04/07/24 10:21:07 PM [    HTTPListener80]   Accept: */*
04/07/24 10:21:07 PM [    HTTPListener80]   User-Agent: Microsoft-CryptoAPI/10.0
04/07/24 10:21:07 PM [    HTTPListener80]   Host: ctldl.windowsupdate.com
```



```
04/07/24 10:22:09 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 194.109.206.212:443
04/07/24 10:21:08 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 171.25.193.9:80
04/07/24 10:21:08 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 208.83.223.34:80
04/07/24 10:21:07 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49682
04/07/24 10:21:07 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49683
04/07/24 10:21:07 PM [          Diverter] NoMoreRansom.exe (4060) requested TCP 127.0.0.1:49682
```

C2 server communication and commands

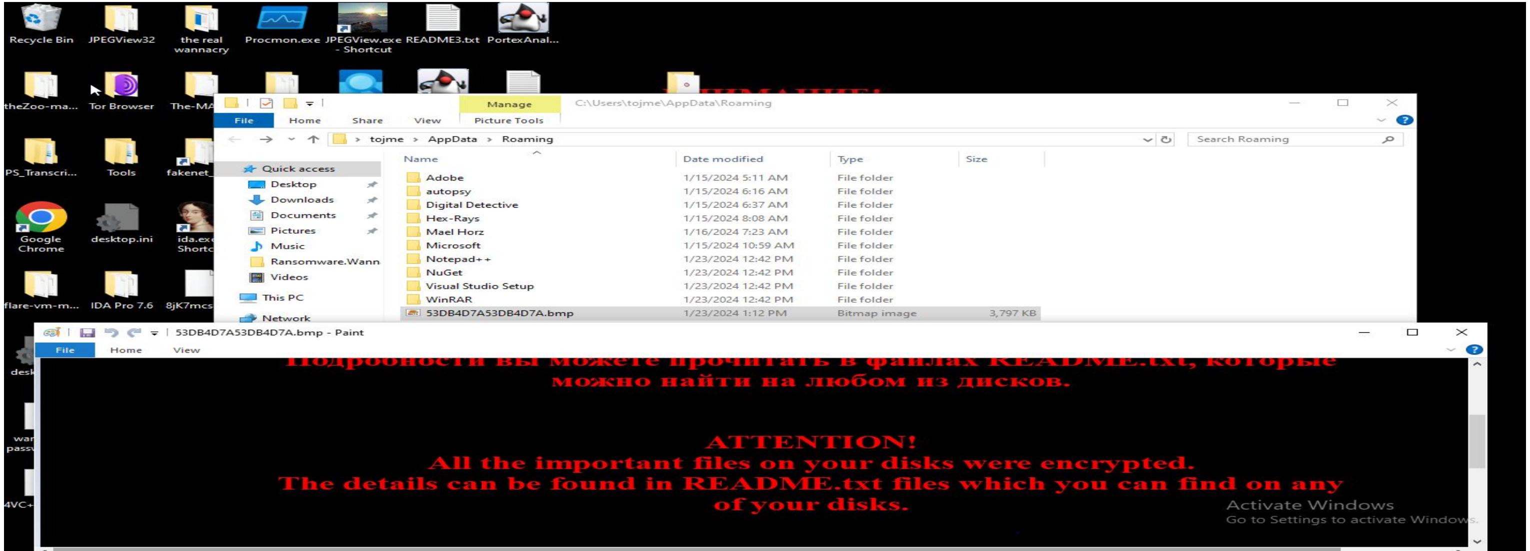
The malware has C2C server communication Malware authors often use command and control servers to remotely control and issue commands to infected systems, enabling them to perform various malicious actions and receive stolen data. C2 servers provide a channel for the malware to communicate with the attacker, receive updates or new configurations, and manage large-scale malware campaigns or botnets. By using C2 servers, attackers can maintain persistent access, obfuscate their infrastructure, and coordinate their malicious activities while hiding their true identities

command	usage
--quiet	Suppresses output or runs in quiet mode
--dump-config	Dumps or prints the current configuration settings.
--version	Displays the version information of the software or tool.
--digests	Possibly related to displaying digests or hashes of files or data.
--list-torrc-options	Suggests a connection to the Tor network or Tor configuration options.
–help	Displays help or usage information.
--library-versions	Lists the versions of libraries or dependencies used by the software.

Wallpaper file Detection

with this registry change I could detect the wallpaper file location.

HKU\S-1-5-21-83331929-1780821005-3884141752-1001\Control Panel\Desktop\WallPaper: "C:\Users\tojme\AppData\Roaming\135E12AD135E12AD.bmp

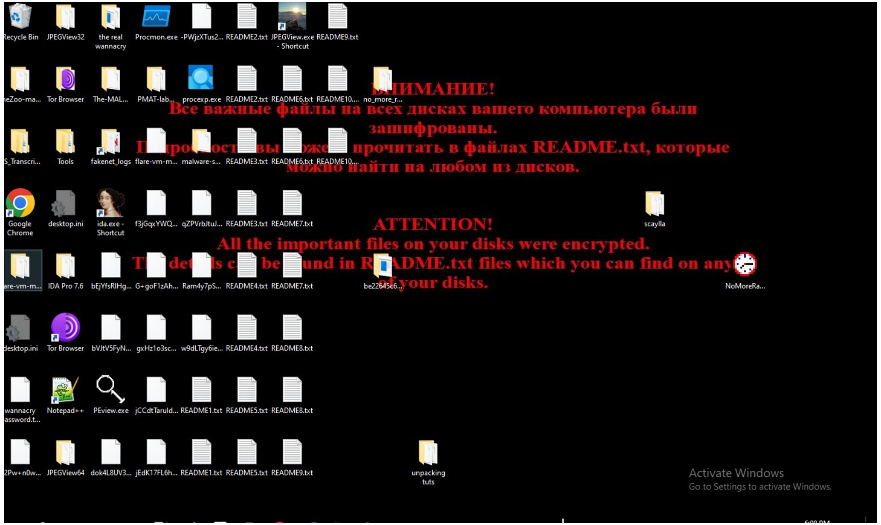


Name	Date modified	Type	Size
Adobe	1/15/2024 5:11 AM	File folder	
autopsy	1/15/2024 6:16 AM	File folder	
Digital Detective	1/15/2024 6:37 AM	File folder	
Hex-Rays	1/15/2024 8:08 AM	File folder	
Mael Horz	1/16/2024 7:23 AM	File folder	
Microsoft	1/15/2024 10:59 AM	File folder	
Notepad++	1/23/2024 12:42 PM	File folder	
NuGet	1/23/2024 12:42 PM	File folder	
Visual Studio Setup	1/23/2024 12:42 PM	File folder	
WinRAR	1/23/2024 12:42 PM	File folder	
53DB4D7A53DB4D7A.bmp	1/23/2024 1:12 PM	Bitmap image	3,797 KB

Подробности вы можете прочитать в файлах README.txt, которые
можно найти на любом из дисков.

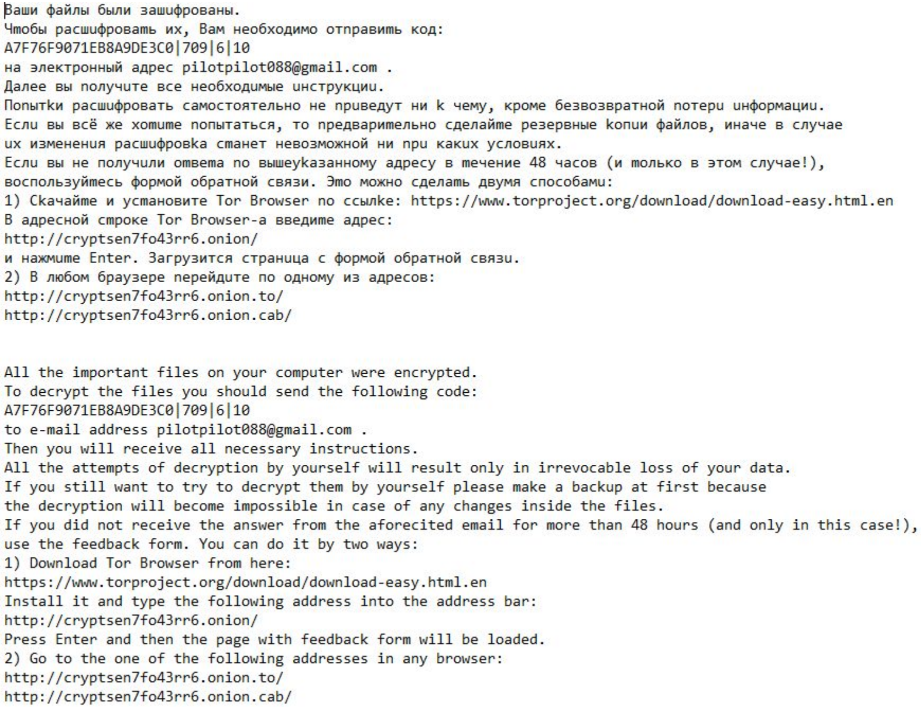
ATTENTION!
All the important files on your disks were encrypted.
The details can be found in README.txt files which you can find on any
of your disks.

When the ransomware is importing the ransom note he’s duplicating it 10 times and calling it README[1-10].TXT



НИМАНИЕ!
Все важные файлы на всех дисках вашего компьютера были зашифрованы.
П про ост вы же прочитать в файлах README.txt, которые можно найти на любом из дисков.

ATTENTION!
All the important files on your disks were encrypted.
T det s c be und in R ADME.txt files which you can find on any of your disks.



Ваши файлы были зашифрованы.
Чтобы расшифровать их, Вам необходимо отправить код:
A7F76F9071EB8A9DE3C0|709|6|10
на электронный адрес pilotpilot088@gmail.com .
Далее вы получите все необходимые инструкции.
Попытки расшифровать самостоятельно не приведут ни к чему, кроме безвозвратной потери информации.
Если вы всё же хотите попытаться, то предварительно сделайте резервные копии файлов, иначе в случае
их изменения расшифровка станет невозможной ни при каких условиях.
Если вы не получили ответа по вышеуказанному адресу в течение 48 часов (и только в этом случае!),
воспользуйтесь формой обратной связи. Это можно сделать двумя способами:
1) Скачайте и установите Tor Browser по ссылке: https://www.torproject.org/download/download-easy.html.en
В адресной строке Tor Browser-а введите адрес:
http://cryptsen7fo43rr6.onion/
и нажмите Enter. Загрузится страница с формой обратной связи.
2) В любом браузере перейдите по одному из адресов:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/

All the important files on your computer were encrypted.
To decrypt the files you should send the following code:
A7F76F9071EB8A9DE3C0|709|6|10
to e-mail address pilotpilot088@gmail.com .
Then you will receive all necessary instructions.
All the attempts of decryption by yourself will result only in irrevocable loss of your data.
If you still want to try to decrypt them by yourself please make a backup at first because
the decryption will become impossible in case of any changes inside the files.
If you did not receive the answer from the aforecited email for more than 48 hours (and only in this case!),
use the feedback form. You can do it by two ways:
1) Download Tor Browser from here:
https://www.torproject.org/download/download-easy.html.en
Install it and type the following address into the address bar:
http://cryptsen7fo43rr6.onion/
Press Enter and then the page with feedback form will be loaded.
2) Go to the one of the following addresses in any browser:
http://cryptsen7fo43rr6.onion.to/
http://cryptsen7fo43rr6.onion.cab/

How to avoid ransomware attacks

1. Keep software updated: Ensure your operating system, applications, and antivirus/anti-malware software are always up-to-date. Software updates often include security patches that can protect against the latest ransomware threats.

2. Use strong, unique passwords: Use long, complex passwords for all your accounts and enable two-factor authentication whenever possible. This makes it harder for attackers to gain access to your systems.

3. Back up your data regularly: Regularly back up your important data to an external hard drive or cloud storage. This way, if you do get hit by ransomware, you can restore your files without having to pay the ransom.

4. Be cautious with email attachments and links: Ransomware is often spread through phishing emails with malicious attachments or links. Be very careful about opening emails, attachments, or links from untrusted sources.