I literally can't think of a fitting pun - MrDec Ransomware

dissectingmalwa.re/i-literally-cant-think-of-a-fitting-pun-mrdec-ransomware.html

Mon 23 December 2019 in Ransomware

I took notice of the Ransomware Family after a series of posts in the Bleeping Computer Forum.

It employs techniques that are not seen very often in other ransomware samples, so the Analysis is actually quite difficult, but I'm hoping reading this is also a bit interesting atleast.

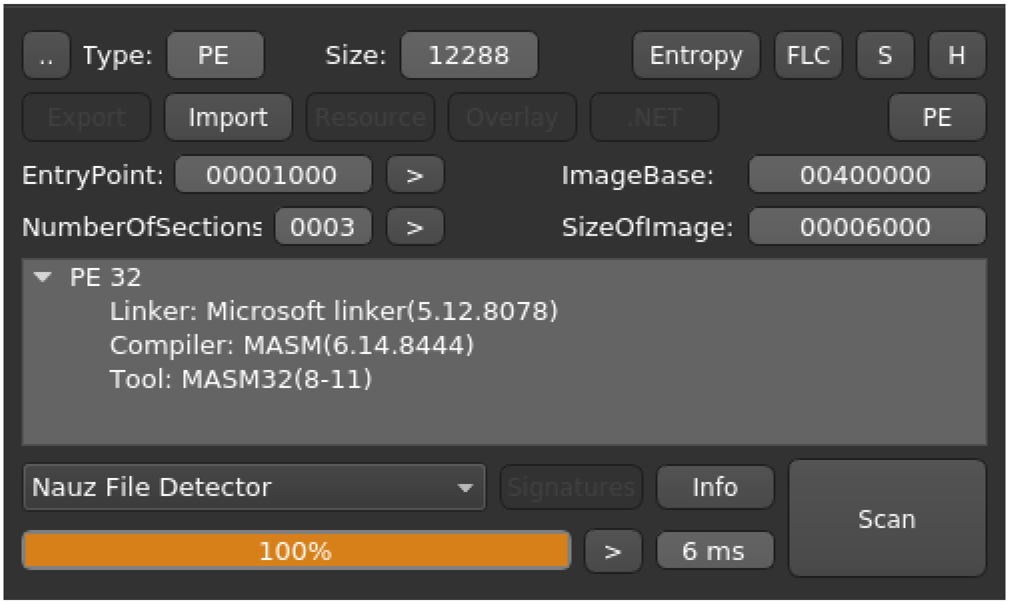
Work in Progress

Because Christmas and 36c3 is coming up in the next few I days I might have to push this analysis back a bit.

A general disclaimer as always: downloading and running the samples linked below will lead to the encryption of your personal data, so be f$cking careful. Also check with your local laws as owning malware binaries/ sources might be illegal depending on where you live.

MrDec @ AnyRun | VirusTotal | HybridAnalysis --> `sha256 a700f9ced75c4143da6c4d1e09d6778e84ff570ea7d297fc130a0844e56c96ad`

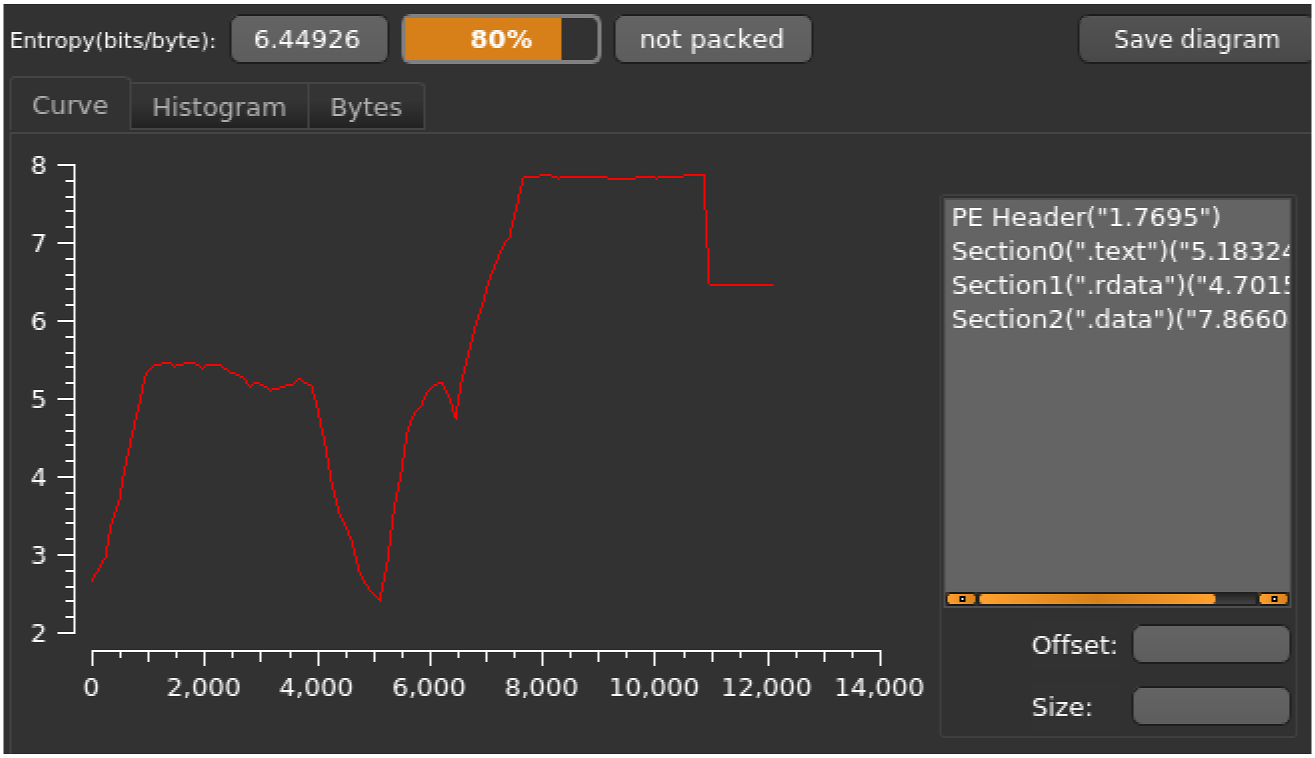
Let's see what we're dealing with here and fire up Detect it easy:



Type: PE
Size: 12288
EntryPoint: 00001000
ImageBase: 00400000
NumberOfSections 0003
SizeOfImage: 00006000

PE 32
Linker: Microsoft linker(5.12.8078)
Compiler: MASM(6.14.8444)
Tool: MASM32(8-11)

100%
6 ms

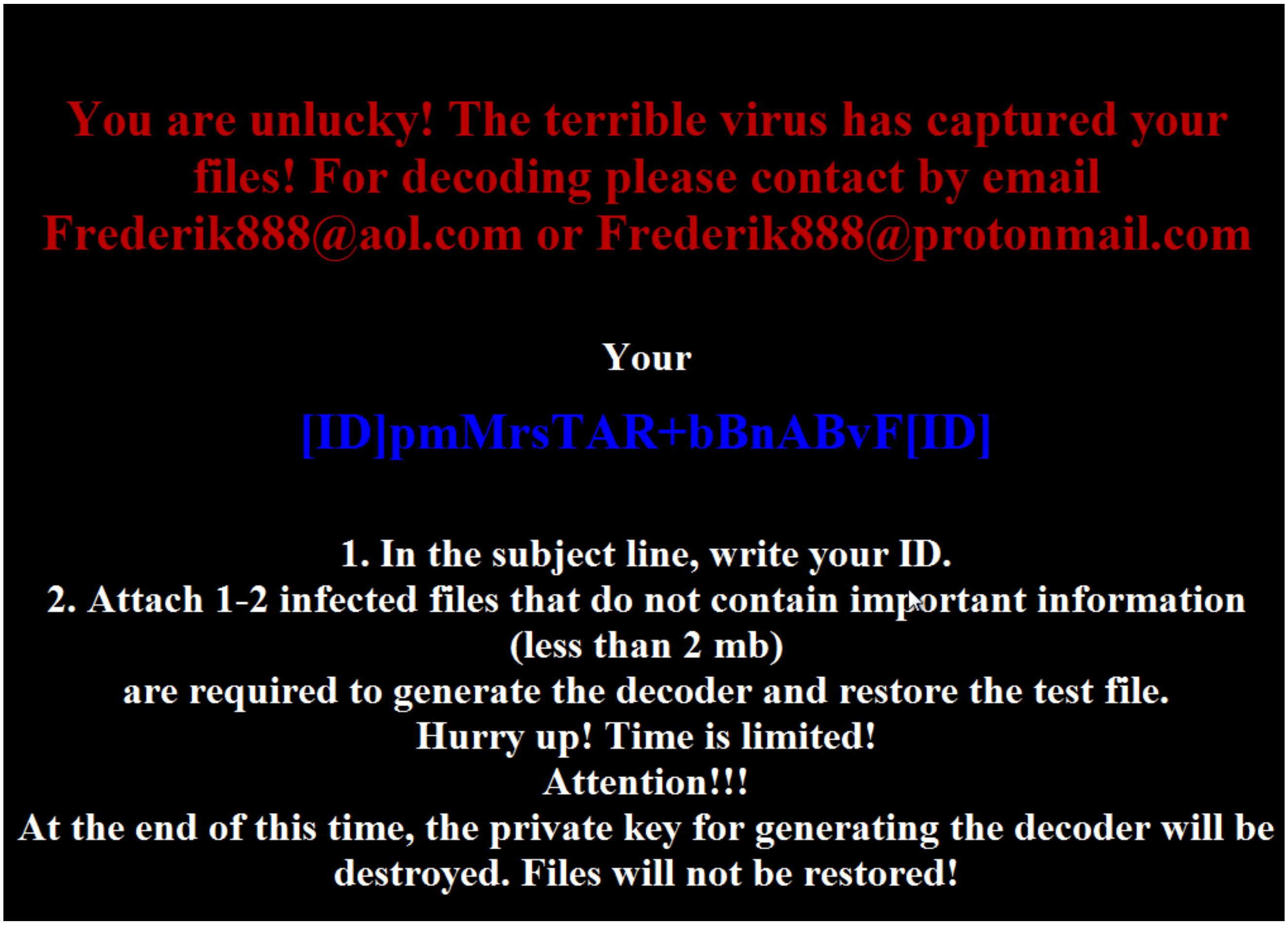


Entropy(bits/byte): 6.44926 80% not packed

PE Header("1.7695")
Section0(".text")("5.18324
Section1(".rdata")("4.7015
Section2(".data")("7.8660

Offset:
Size:

The Ransomnote is delivered via a *.hta* file. Like most other strains active in the last few month the criminals use two E-Mail addresses: a "primary" and a "backup". In this case they are using Protonmail and AOL which has been kind of a pattern for them (Tutanota is their third preferred service, a list of previously used mailboxes is available down below in the IOCs Section).



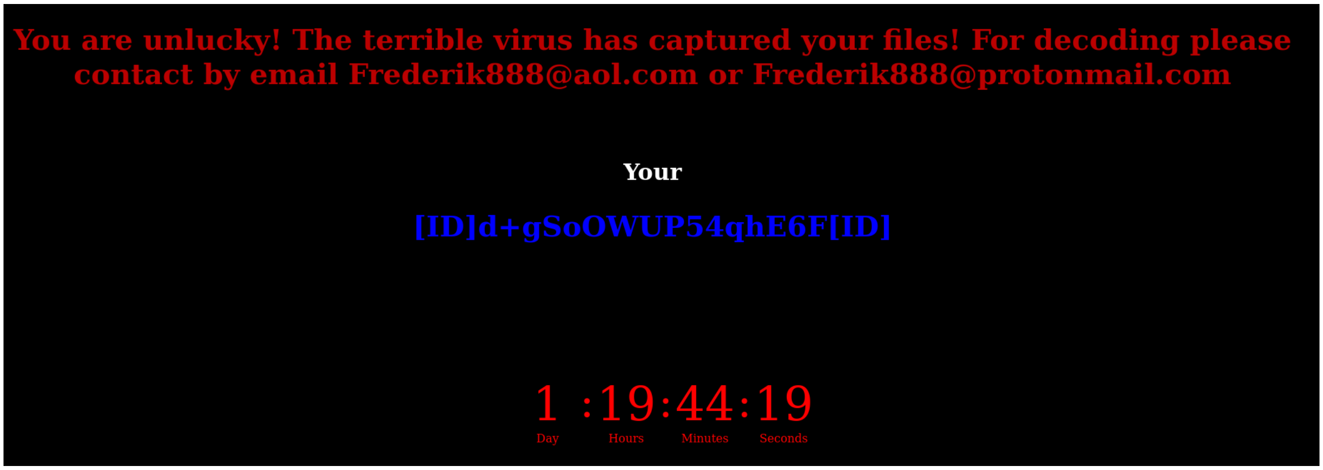
You are unlucky! The terrible virus has captured your files! For decoding please contact by email Frederik888@aol.com or Frederik888@protonmail.com

Your

[ID]pmMrsTAR+bBnABvF[ID]

1. In the subject line, write your ID.
2. Attach 1-2 infected files that do not contain important information (less than 2 mb)
are required to generate the decoder and restore the test file.
Hurry up! Time is limited!
Attention!!!
At the end of this time, the private key for generating the decoder will be destroyed. Files will not be restored!

Opening the note in another browser (Chrome in this case) won't show the instructions but a countdown timer. The victim won't be able to see the timer in most cases because when using Internet Explorer because scrolling is disabled :D



You are unlucky! The terrible virus has captured your files! For decoding please contact by email Frederik888@aol.com or Frederik888@protonmail.com

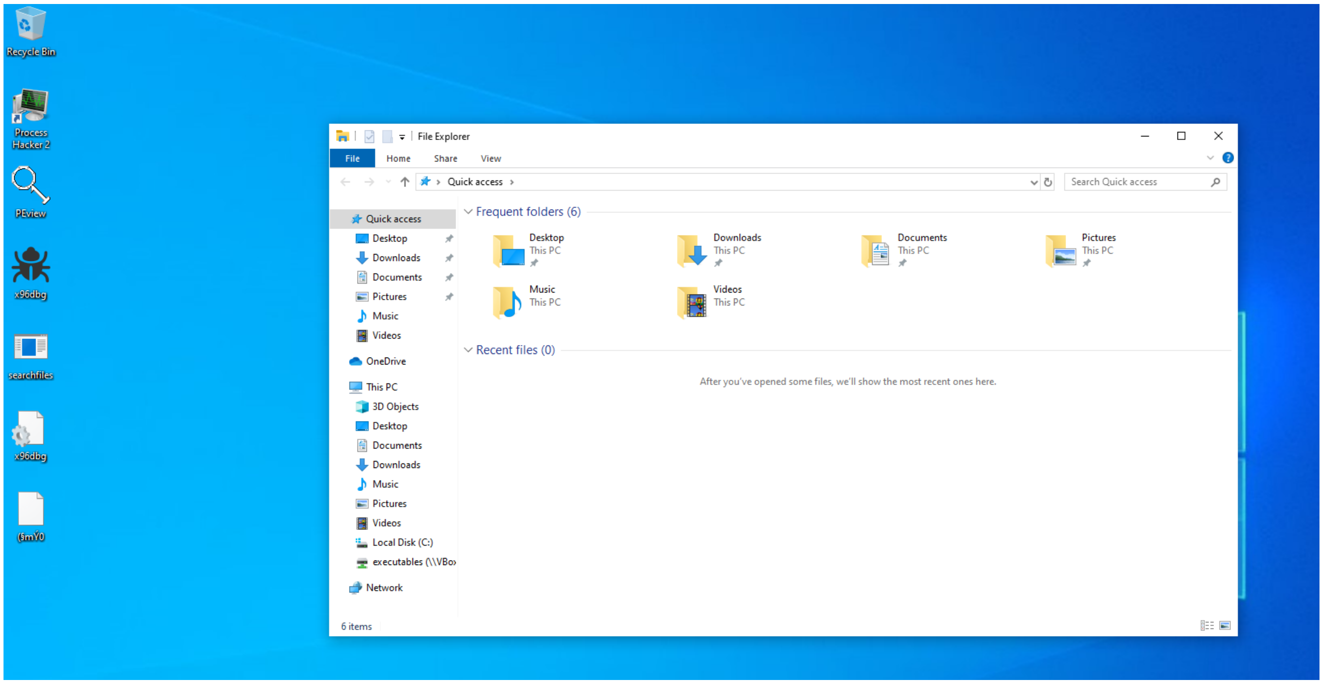
Your

[ID]d+gSoOWUP54qhE6F[ID]

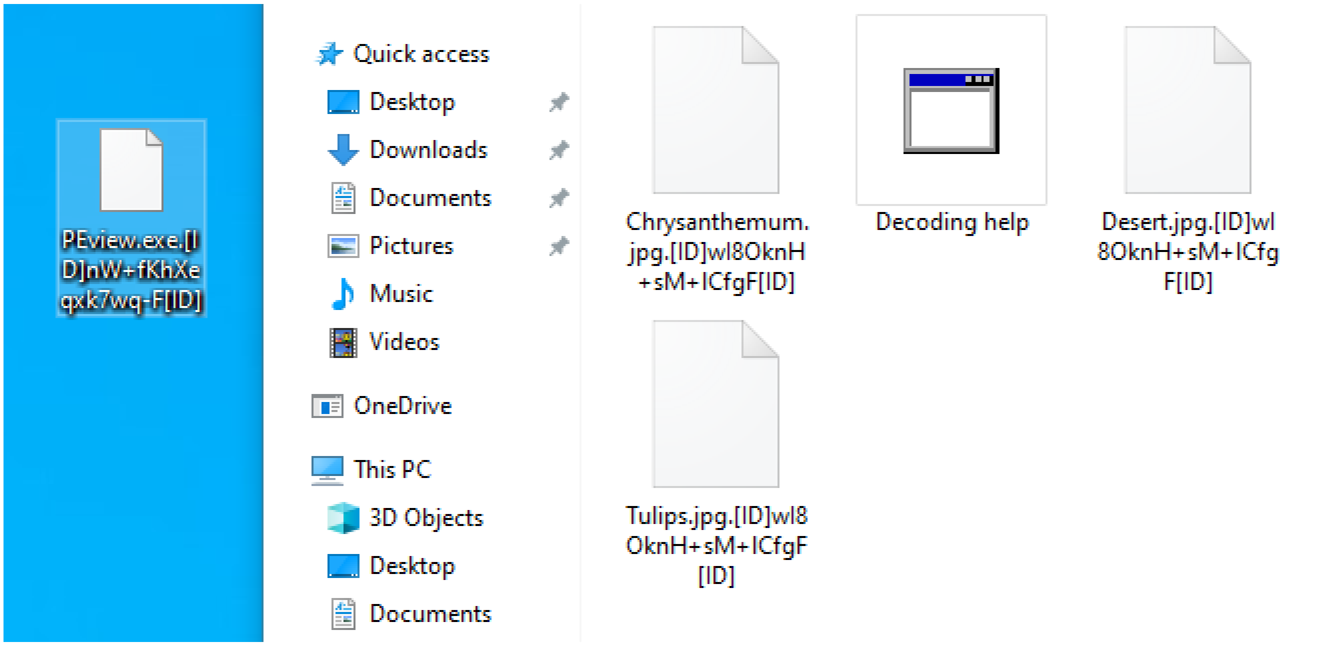
1 :19:44:19

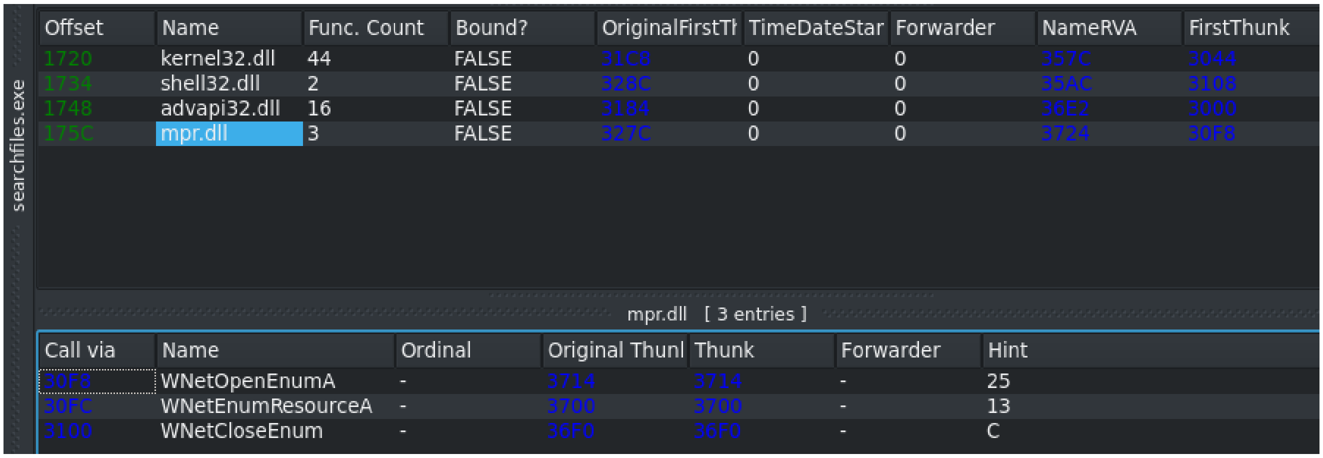
Day Hours Minutes Seconds

Ransomnote in Chrome



After you've opened some files, we'll show the most recent ones here.


PEview.exe.[ID]nW+fKhXeqxk7wq-F[ID]
Quick access
Desktop
Downloads
Documents
Pictures
Music
Videos
OneDrive
This PC
3D Objects
Desktop
Documents
Chrysanthemum.jpg.[ID]wl8OknH+sM+ICfgF[ID]
Decoding help
Desert.jpg.[ID]wl8OknH+sM+ICfgF[ID]
Tulips.jpg.[ID]wl8OknH+sM+ICfgF[ID]

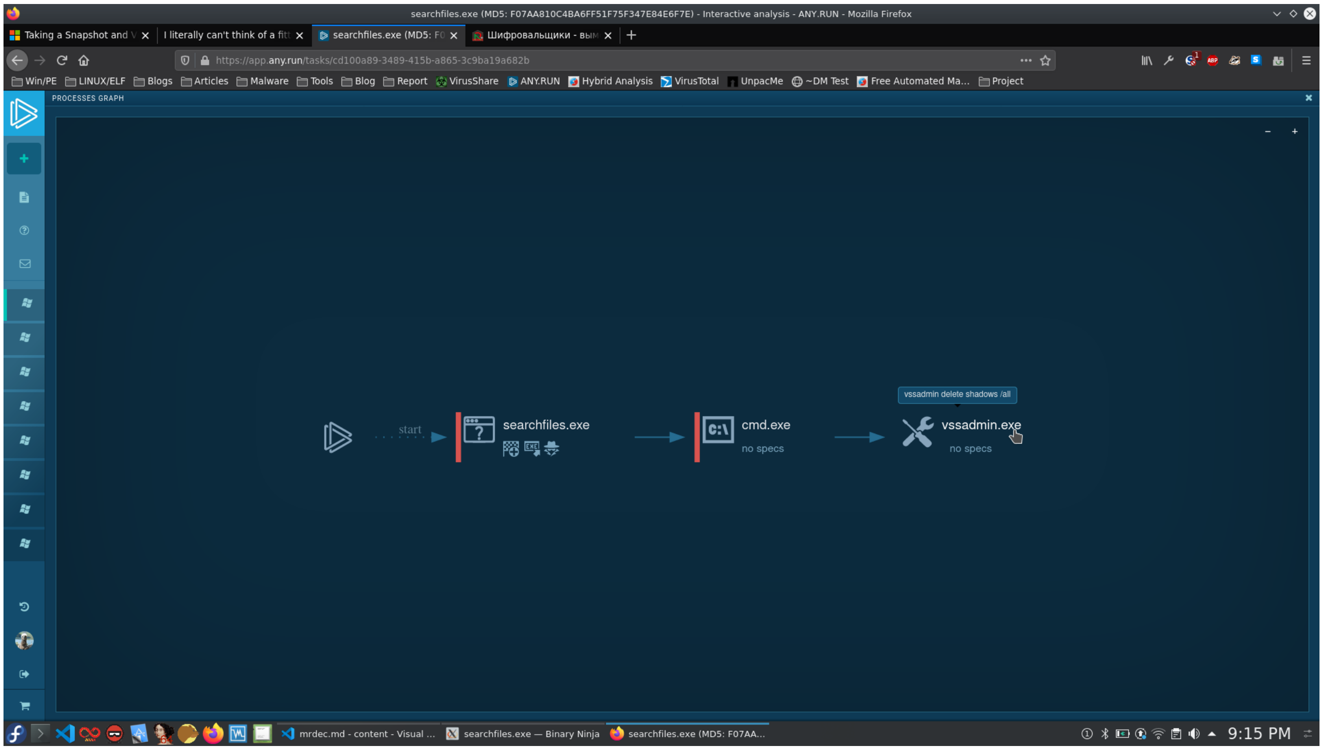


searchfiles.exe

Offset	Name	Func. Count	Bound?	OriginalFirstTh	TimeDateStar	Forwarder	NameRVA	FirstThunk
1720	kernel32.dll	44	FALSE	31C8	0	0	357C	3044
1734	shell32.dll	2	FALSE	328C	0	0	35AC	3108
1748	advapi32.dll	16	FALSE	3184	0	0	36E2	3000
175C	mpr.dll	3	FALSE	327C	0	0	3724	30F8

mpr.dll [3 entries]

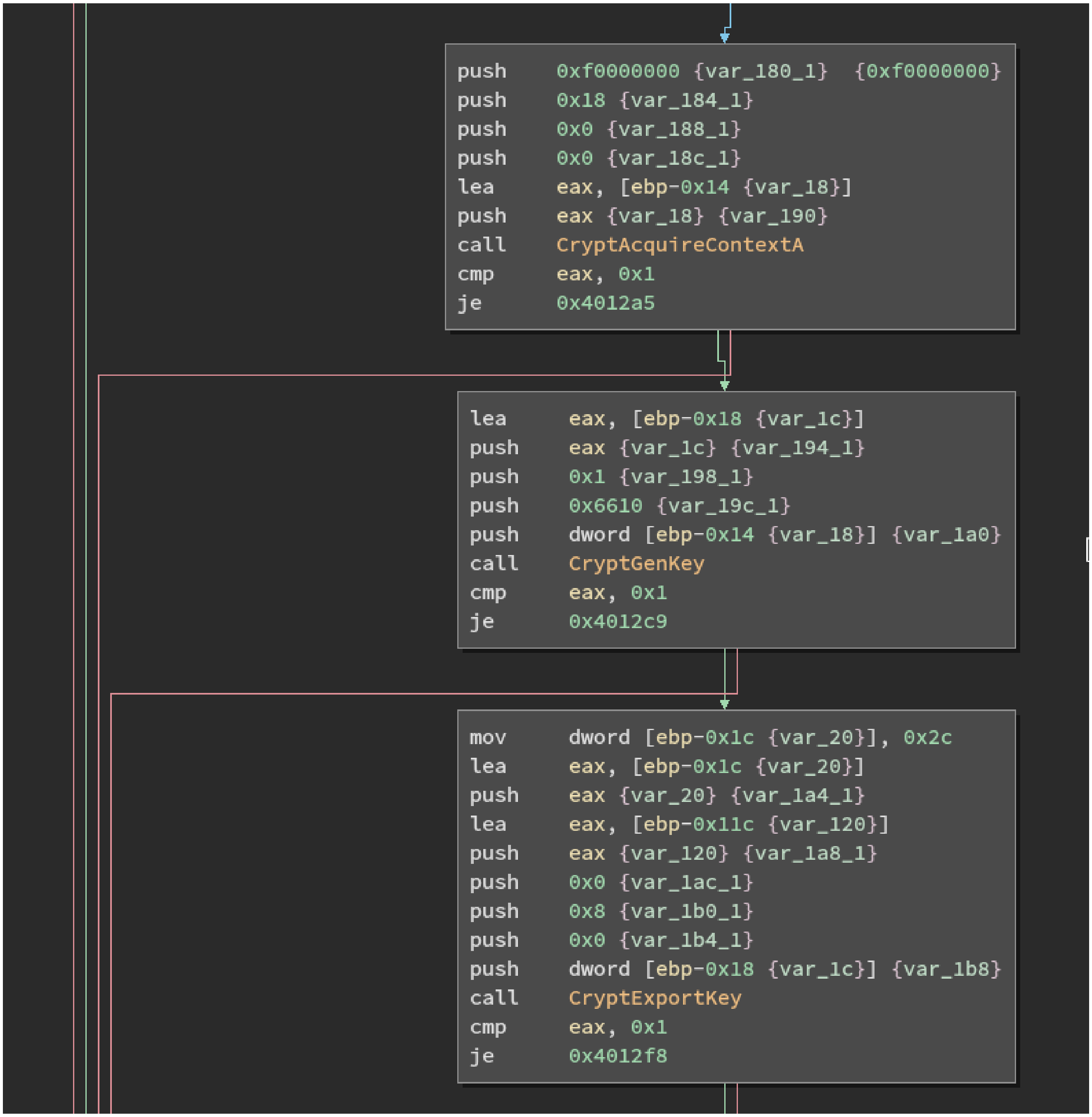
Call via	Name	Ordinal	Original Thunl	Thunk	Forwarder	Hint
30F8	WNetOpenEnumA	-	3714	3714	-	25
30FC	WNetEnumResourceA	-	3700	3700	-	13
3100	WNetCloseEnum	-	36F0	36F0	-	C



searchfiles.exe (MD5: F07AA810C4BA6FF51F75F347E84E6F7E) - Interactive analysis - ANY.RUN - Mozilla Firefox

https://app.any.run/tasks/cd100a89-3489-415b-a865-3c9ba19a682b

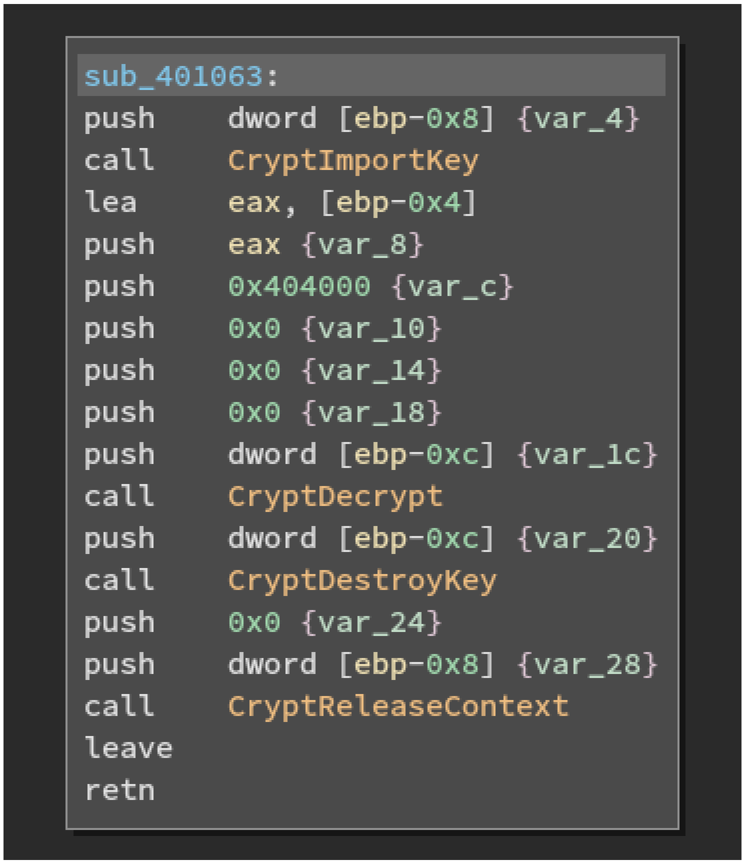
vssadmin delete shadows /all



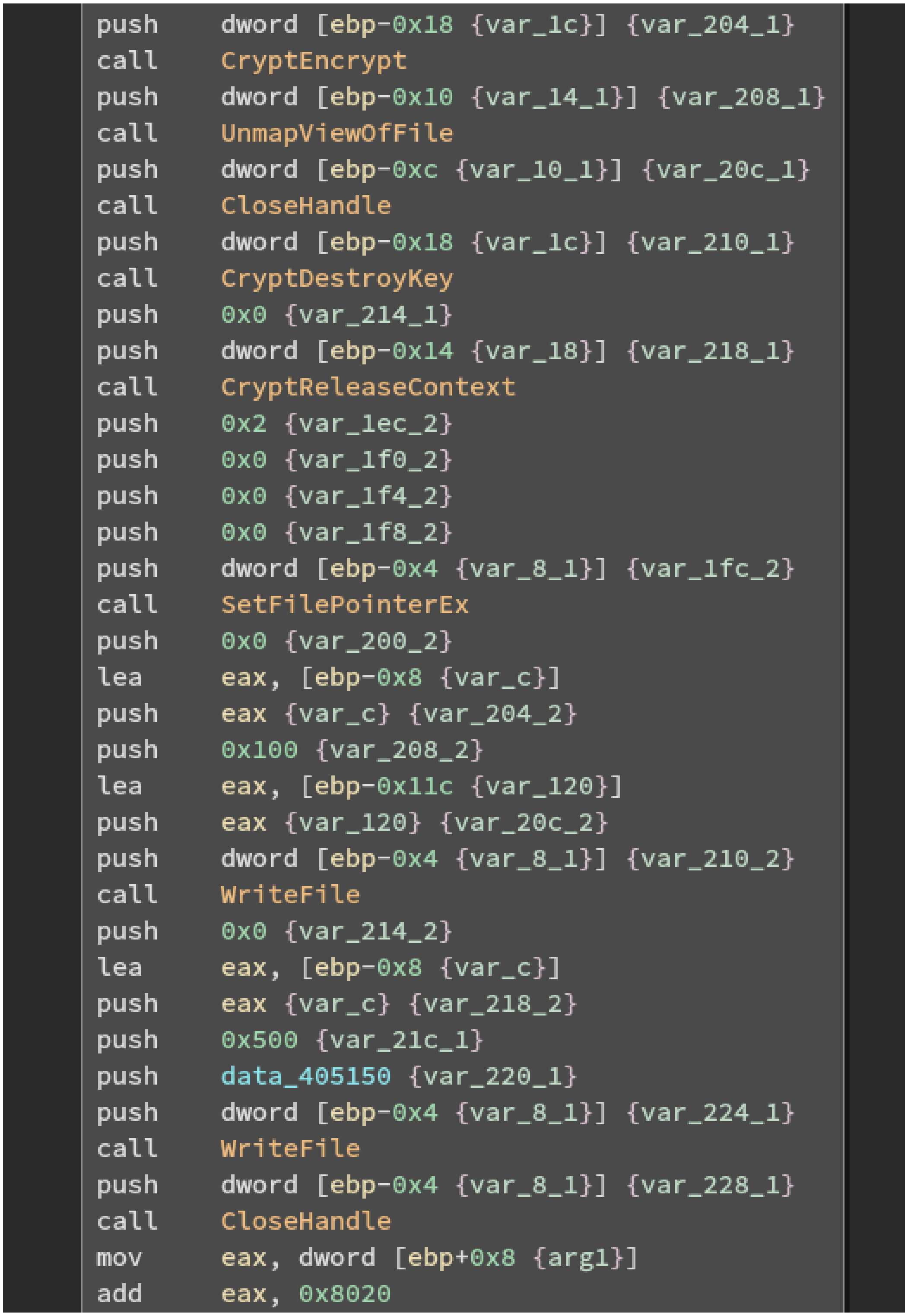
```
push    0xf0000000 {var_180_1}  {0xf0000000}
push    0x18 {var_184_1}
push    0x0 {var_188_1}
push    0x0 {var_18c_1}
lea     eax, [ebp-0x14 {var_18}]
push    eax {var_18} {var_190}
call    CryptAcquireContextA
cmp     eax, 0x1
je      0x4012a5
```

```
lea     eax, [ebp-0x18 {var_1c}]
push    eax {var_1c} {var_194_1}
push    0x1 {var_198_1}
push    0x6610 {var_19c_1}
push    dword [ebp-0x14 {var_18}] {var_1a0}
call    CryptGenKey
cmp     eax, 0x1
je      0x4012c9
```

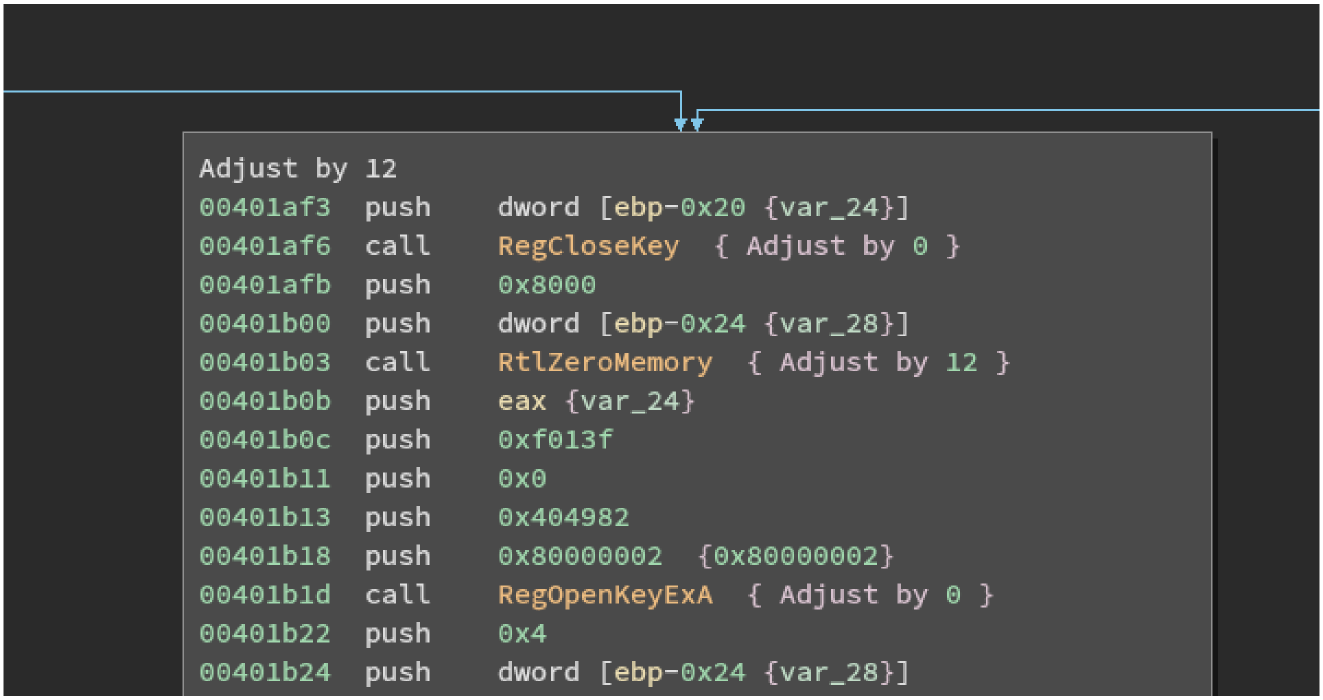
```
mov     dword [ebp-0x1c {var_20}], 0x2c
lea     eax, [ebp-0x1c {var_20}]
push    eax {var_20} {var_1a4_1}
lea     eax, [ebp-0x11c {var_120}]
push    eax {var_120} {var_1a8_1}
push    0x0 {var_1ac_1}
push    0x8 {var_1b0_1}
push    0x0 {var_1b4_1}
push    dword [ebp-0x18 {var_1c}] {var_1b8}
call    CryptExportKey
cmp     eax, 0x1
je      0x4012f8
```



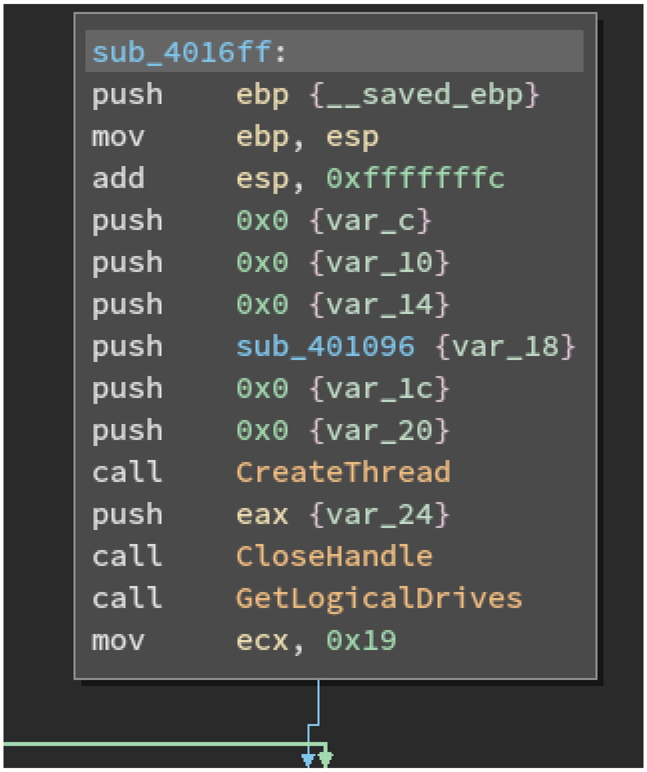
```
sub_401063:
push    dword [ebp-0x8] {var_4}
call    CryptImportKey
lea     eax, [ebp-0x4]
push    eax {var_8}
push    0x404000 {var_c}
push    0x0 {var_10}
push    0x0 {var_14}
push    0x0 {var_18}
push    dword [ebp-0xc] {var_1c}
call    CryptDecrypt
push    dword [ebp-0xc] {var_20}
call    CryptDestroyKey
push    0x0 {var_24}
push    dword [ebp-0x8] {var_28}
call    CryptReleaseContext
leave
retn
```



```
push    dword [ebp-0x18 {var_1c}] {var_204_1}
call    CryptEncrypt
push    dword [ebp-0x10 {var_14_1}] {var_208_1}
call    UnmapViewOfFile
push    dword [ebp-0xc {var_10_1}] {var_20c_1}
call    CloseHandle
push    dword [ebp-0x18 {var_1c}] {var_210_1}
call    CryptDestroyKey
push    0x0 {var_214_1}
push    dword [ebp-0x14 {var_18}] {var_218_1}
call    CryptReleaseContext
push    0x2 {var_1ec_2}
push    0x0 {var_1f0_2}
push    0x0 {var_1f4_2}
push    0x0 {var_1f8_2}
push    dword [ebp-0x4 {var_8_1}] {var_1fc_2}
call    SetFilePointerEx
push    0x0 {var_200_2}
lea     eax, [ebp-0x8 {var_c}]
push    eax {var_c} {var_204_2}
push    0x100 {var_208_2}
lea     eax, [ebp-0x11c {var_120}]
push    eax {var_120} {var_20c_2}
push    dword [ebp-0x4 {var_8_1}] {var_210_2}
call    WriteFile
push    0x0 {var_214_2}
lea     eax, [ebp-0x8 {var_c}]
push    eax {var_c} {var_218_2}
push    0x500 {var_21c_1}
push    data_405150 {var_220_1}
push    dword [ebp-0x4 {var_8_1}] {var_224_1}
call    WriteFile
push    dword [ebp-0x4 {var_8_1}] {var_228_1}
call    CloseHandle
mov     eax, dword [ebp+0x8 {arg1}]
add     eax, 0x8020
```

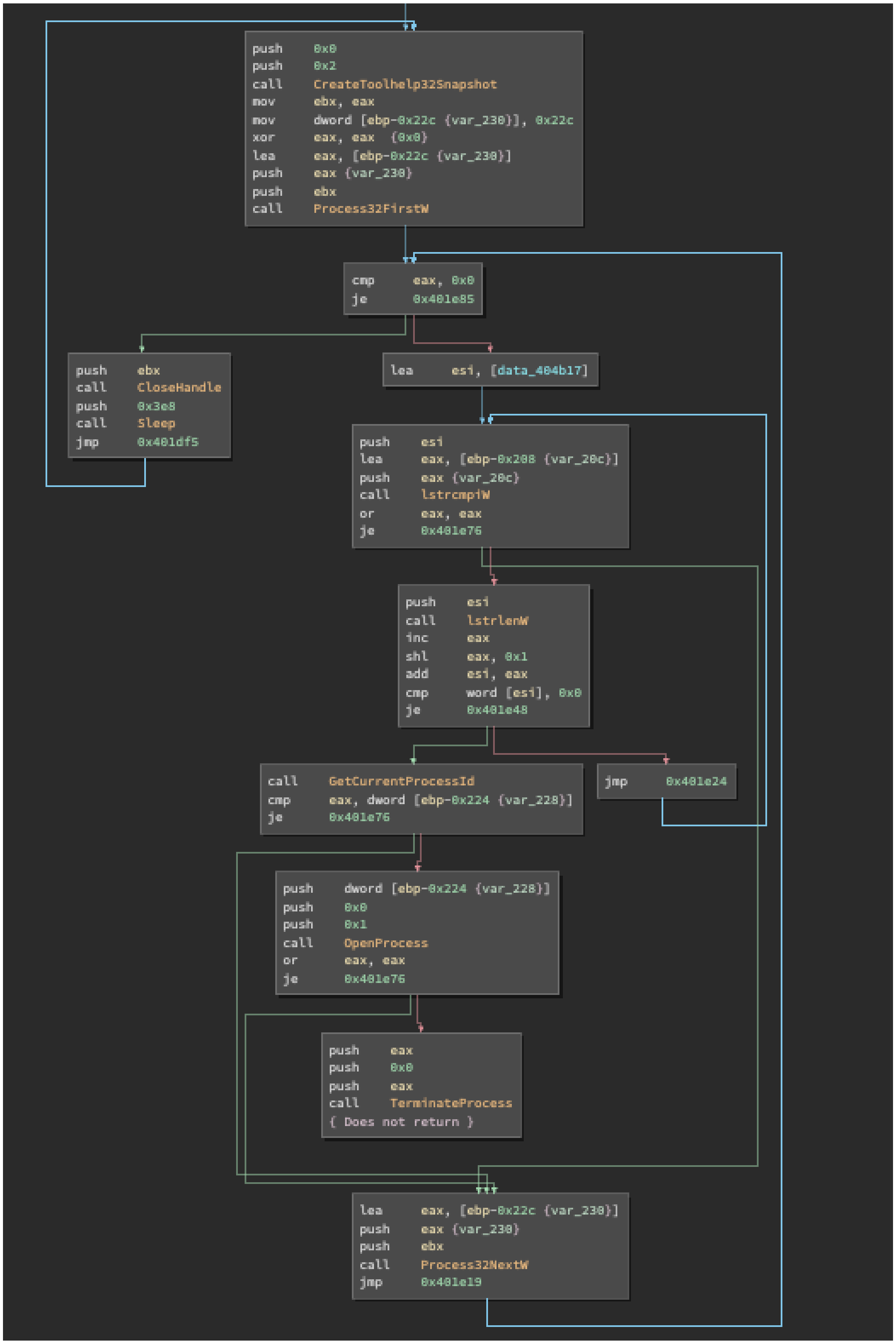


```
Adjust by 12
00401af3  push    dword [ebp-0x20 {var_24}]
00401af6  call    RegCloseKey  { Adjust by 0 }
00401afb  push    0x8000
00401b00  push    dword [ebp-0x24 {var_28}]
00401b03  call    RtlZeroMemory  { Adjust by 12 }
00401b0b  push    eax {var_24}
00401b0c  push    0xf013f
00401b11  push    0x0
00401b13  push    0x404982
00401b18  push    0x80000002  {0x80000002}
00401b1d  call    RegOpenKeyExA  { Adjust by 0 }
00401b22  push    0x4
00401b24  push    dword [ebp-0x24 {var_28}]
```



```
sub_4016ff:
push    ebp {__saved_ebp}
mov     ebp, esp
add     esp, 0xfffffffc
push    0x0 {var_c}
push    0x0 {var_10}
push    0x0 {var_14}
push    sub_401096 {var_18}
push    0x0 {var_1c}
push    0x0 {var_20}
call    CreateThread
push    eax {var_24}
call    CloseHandle
call    GetLogicalDrives
mov     ecx, 0x19
```

In the following screenshot you can see the "Process Killing" routine of MrDec.



```
push    0x0
push    0x2
call    CreateToolhelp32Snapshot
mov     ebx, eax
mov     dword [ebp-0x22c {var_230}], 0x22c
xor     eax, eax  {0x0}
lea     eax, [ebp-0x22c {var_230}]
push    eax {var_230}
push    ebx
call    Process32FirstW
```

```
cmp     eax, 0x0
je      0x401e85
```

```
push    ebx
call    CloseHandle
push    0x3e8
call    Sleep
jmp     0x401df5
```

```
lea     esi, [data_404b17]
```

```
push    esi
lea     eax, [ebp-0x208 {var_20c}]
push    eax {var_20c}
call    lstrcmpiW
or      eax, eax
je      0x401e76
```

```
push    esi
call    lstrlenW
inc     eax
shl     eax, 0x1
add     esi, eax
cmp     word [esi], 0x0
je      0x401e48
```

```
call    GetCurrentProcessId
cmp     eax, dword [ebp-0x224 {var_228}]
je      0x401e76
```

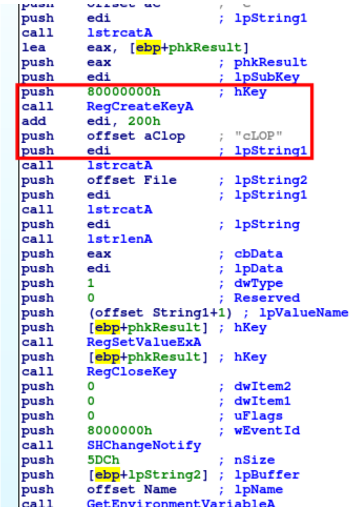
```
jmp     0x401e24
```

```
push    dword [ebp-0x224 {var_228}]
push    0x0
push    0x1
call    OpenProcess
or      eax, eax
je      0x401e76
```

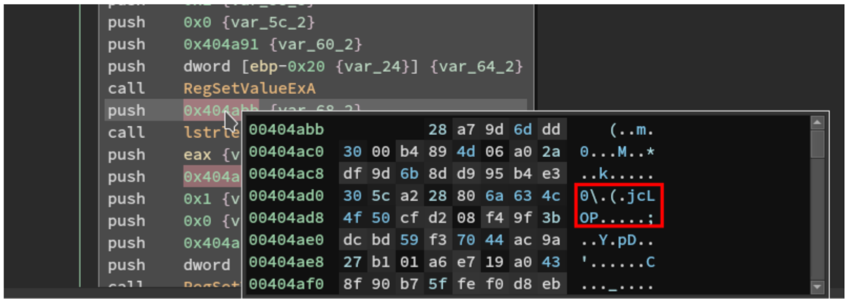
```
push    eax
push    0x0
push    eax
call    TerminateProcess
{ Does not return }
```

```
lea     eax, [ebp-0x22c {var_230}]
push    eax {var_230}
push    ebx
call    Process32NextW
jmp     0x401e19
```

Last but not least we have a weird discovery.



```
push    edi             ; lpString1
call    lstrcatA
lea     eax, [ebp+phkResult]
push    eax             ; phkResult
push    edi             ; lpSubKey
push    80000000h       ; hKey
call    RegCreateKeyA
add     edi, 200h
push    offset aClop    ; "cLOP"
push    edi             ; lpString1
call    lstrcatA
push    offset File     ; lpString2
push    edi             ; lpString1
call    lstrcatA
push    edi             ; lpString
call    lstrlenA
push    eax             ; cbData
push    edi             ; lpData
push    1               ; dwType
push    0               ; Reserved
push    (offset String1+1) ; lpValueName
push    [ebp+phkResult] ; hKey
call    RegSetValueExA
push    [ebp+phkResult] ; hKey
call    RegCloseKey
push    0               ; dwItem2
push    0               ; dwItem1
push    0               ; uFlags
push    8000000h        ; wEventId
call    SHChangeNotify
push    5DCh            ; nSize
push    [ebp+lpString2] ; lpBuffer
push    offset Name     ; lpName
call    GetEnvironmentVariableA
```



```
push    0x0 {var_5c_2}
push    0x404a91 {var_60_2}
push    dword [ebp-0x20 {var_24}] {var_64_2}
call    RegSetValueExA
push    0x404abb
call    lstrle  00404abb          28 a7 9d 6d dd      (..m.
push    eax {v  00404ac0 30 00 b4 89 4d 06 a0 2a   0...M..*
push    0x404a  00404ac8 df 9d 6b 8d d9 95 b4 e3   ..k.....
push    0x1 {v  00404ad0 30 5c a2 28 80 6a 63 4c   0\.(.jcL
push    0x0 {v  00404ad8 4f 50 cf d2 08 f4 9f 3b   OP.....;
push    0x404a  00404ae0 dc bd 59 f3 70 44 ac 9a   ..Y.pD..
push    dword   00404ae8 27 b1 01 a6 e7 19 a0 43   '......C
                00404af0 8f 90 b7 5f fe f0 d8 eb   ..._....
```

MITRE ATT&CK

T1215 --> Kernel Modules and Extensions --> Persistence

T1179 --> Hooking --> Persistence

T1060 --> Registry Run Keys / Start Folder --> Persistence

T1055 --> Process Injection --> Privilege Escalation

T1179 --> Hooking --> Privilege Escalation

T1055 --> Process Injection --> Defense Evasion

T1045 --> Software Packing --> Defense Evasion

T1112 --> Modify Registry --> Defense Evasion

T1107 --> File Deletion --> Defense Evasion

T1179 --> Hooking --> Credential Access

T1012 --> Query Registry --> Discovery

T1057 --> Process Discovery --> Discovery

T1076 --> Remote Desktop Protocol --> Lateral Movement

IOCs

MrDec

```
searchfiles.exe --> SHA256:
a700f9ced75c4143da6c4d1e09d6778e84ff570ea7d297fc130a0844e56c96ad
                    SSDEEP:
192:QEsTzSIs3HIuvipDu3uTtKTzTwmH+STs8fpgiRHIYGL4vKrGoO:QE0JoapKeTtKTz8s+S48h5dIYxK
```

Registry Keys

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
unlock --> "c:\Decoding help.hta"
searchfiles -->  C:\windows\searchfiles.exe


HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\DateTime
orsa--> 06 02 00 00 00 A4 00 00  52 53 41 31 00 08 00 00 01 00 01 00 07 AF 04 2E  A4
1A 3C 08 5E 32 C7 4F 6A DB C8 7C 91 6B C1 FE  73 38 2F 4F 7C EA B8 B6 BC BD CB 22 5C
6B E6 1C  E0 35 24 58 ED C8 BC EF A9 A6 EC AE 4F 84 AF BC  E8 D7 50 4B C5 2A 6F 85 5E
E9 A1 46 5F 2A 65 E7  0E 97 74 4B 16 D5 C4 4C 28 6B 17 47 EC F0 B9 A5  72 C4 DB EE 67
1D C6 0D DD 58 93 FF CE 38 64 5D  92 0E 93 AC A6 BC 31 B5 6D ED A6 74 8F 59 F3 40  EF
FD A9 7D 18 12 4F 0A 51 AF D6 1F EE 1E 17 4B  A2 D7 CD 20 B4 4F FD DF 5C BB CD B6 A4
BC D2 8D  85 17 F9 95 BF FD 67 16 36 15 69 7A BC A2 FD 0F  EC F6 D4 A4 92 94 3A AC FC
78 77 81 4B F4 E8 2E  AD 55 52 27 67 EF E9 48 1F 1D 8B F5 35 8F 71 AA  DA 84 75 79 A2
1C BD 32 90 8B EB 54 88 3F CC 51  C9 48 2A 47 76 79 CE EB B4 A7 ED D5 DF C3 EB 50  09
25 CC FE F3 DB 49 29 A6 6B 4F 69 AF 10 3A 1F  2F 86 1A 0C B4 90 EB 21 DF 4E 43 B3
rsa -->  3C 53 81 1E 96 58 52 7C  67 7D 5F 60 14 15 29 1B 72 AC F5 F6 B7 B8 54 32  B7
63 1A 24 4F B2 9E B5 C7 8B 29 68 40 6B 44 80  FA E4 5E 53 7B 4A 1D DE AD 28 4A E0 EF
65 1E 09  00 75 34 15 79 59 86 C9 61 ED DD E2 AE 4F 3C DA  45 7A 20 3F 85 85 FB 05 22
1E 9D 12 D2 C7 96 AB  8A 99 46 60 F0 CB 10 6C 2E A0 39 FF 07 80 A1 A4  3B 62 E6 71 93
C6 5D 42 00 1B 00 37 76 56 14 2F  72 78 F9 A2 A6 98 49 A7 38 E0 B0 A6 81 B8 F5 7F  79
7C 29 88 79 C3 98 65 C0 69 47 93 59 28 A8 BF  36 6F 88 C0 08 98 0F 6E C8 27 28 9A C8
12 F2 B2  09 7B F0 A3 1E 9A 3A 48 CE 04 C3 61 82 6B AF 2E  0D 46 14 3A F9 47 3E 26 B0
B3 67 49 81 56 DF E8  DF A4 FC 86 88 A0 80 7C 68 6D 46 84 3E 6F 30 FA  20 AC 54 3F AC
8B C3 E9 24 C3 27 31 4C A1 07 98  C2 BD D8 84 02 17 D7 3D 63 83 8F 7C 35 D3 6C C8  29
69 E6 F5 DD D8 DB AA A5 0D 9A 12 43 5D CE CA  47 6E E5 CA A5 DB D8 A6 9F FE FD DE C2
94 24 92  43 C9 08 88 FB B2 33 2B C8 59 1D B6 F2 55 71 E2  83 C7 F5 67 89 03 06 F1 E4
FC F1 13 2D 38 7B 15  DE 05 BE 27 0A AE CD A9 84 2C 3B 66 4B 18 F7 8D  76 31 BD 37 07
ED 1C D9 68 82 94 EF 08 5C B6 29  C4 69 A9 AB 07 6B B7 46 9C 0F DD A9 76 32 B2 D7  F7
FA 3A 25 15 9B A6 F7 55 93 77 DF 67 24 E0 48  B9 CC B0 39 22 B0 51 36 5B F8 DC 2A 0D
19 CC 7E  EC D3 9E 9C 68 38 E4 11 DE BD 2B AE 2E A2 FA AC  86 35 D6 DC C8 4E 9D E5 8A
BE B3 EC 6C 5B BB BD  CB 61 F1 81 99 1F 5E 1A 80 AF 72 75 CA 55 7E 7B  93 ED F3 EB 7A
2F 5E D9 61 32 99 0C 95 3B 4C 9C  CD F7 4C A5 4C 5D DB CA 72 2E BB 7B 4D 76 C5 5D  CA
27 76 29 C1 4A 36 3E 66 7F 5F 29 A1 A8 AD FC  BB FF 2A 11 16 29 63 8C A8 92 75 FC 0E
56 72 DC  01 9B B9 81 1C E0 14 84 8F F2 1B 15 F8 AC 0A BA  07 22 6D E0 DA A0 8B CF C1
26 0C 69 78 48 BE 24  53 E6 5E A7 A7 10 24 58 EA 26 30 6A 37 0E 30 9A  FF 6E 18 90 2F
93 33 61 11 C1 7B 62 85 A8 A0 E8  3F EA 65 FC 58 3E FD BC 20 55 03 C3 95 63 2E AD  9D
0A 8E 45 87 F6 19 34 D3 48 7E 2E F2 06 BE D0  EE B9 6D 82 62 3E 51 C9 27 96 64 07 84
70 50 C0  A1 2B 13 D3 25 EA C8 62 F1 1F C5 59 B0 6B 3B 52  54 3B 1B 21 42 7B 80 CB E7
58 3D F2 A3 7F F8 48  C0 9E 1E 78 E4 0F F0 7F 50 4D D8 06 C2 53 47 3A  93 B0 AD D7 BF
5A 3F 5A F8 5B BF 60 66 0B EC B6  AF 50 5B 52 9C 82 E3 F8 EC 40 FF ED AB 4C 5C 29  E7
C4 41 87 48 B4 C1 92 74 54 A1 47 70 8A 03 94  AE AE 57 86 FF E2 BE 14 E6 F8 0C D1 73
D9 1A 2E  2E 1E B1 9E 31 3A 3D 0A F1 19 6C 4C 48 F9 C0 7A  58 9E 8F 46 F7 9C 14 26 64
2A 57 A1 88 2A A7 D5  02 6B 76 AE AB 69 C8 64 16 7A 7F E0 43 A7 14 DE  29 19 A7 3B 78
D7 02 8C 9F F5 BF 09 1E 6B BB 47  88 3E 30 76 3B DF AF 87 CB 47 2A 84 D8 B9 88 96  09
A1 EF B0 1E 99 B1 0E 07 8D 37 FF 94 BF C6 94  17 AD 95 15 30 78 FE FC 9A AB 6E B8 8B
C2 9E F0  B9 8B 83 30 45 DF F3 22 28 AD 4A 8D 69 E4 7E B6  83 1E 80 C9 8B 9C 97 BE ED
FD 72 D8 A8 68 21 79  CC 53 87 54 FE CB D7 38 A0 44 ED E3 15 48 D6 CD  E1 14 32 0A 49
72 FC 08 7F 36 17 60 5B CA B1 BE  89 21 08 09 02 25 94 AC E2 A0 B8 F5 B6 DF 49 17  86
C6 A3 4A 7D 48 0F 27 EF 1E 48 91 71 A1 A3 2A  D3 2F CF 4F B8 39 B7 04 76 CA 26 EA CF
C8 A7 0F  42 BD 7B A7 50 FC 01 D3 94 1B 8B 2C F3 1C 87 CA  E0 9F E3 CA B9 FF 31 69 ED
DB 5F E2 2E 04 64 52  08 C8 B3 F5 9F 04 CB 31 7C D3 AD 78 76 83 5F 53  8F 5C 3C D8 CD
4D 2D 49 8A 2C CA 4D C9 43 AC B0  88 45 E5 41 7F FA 1D BF 92 9D BF C0 06 5C 24 CE  44
A1 F6 D0 ED 0C 46 BF 88 F2 DA B1 71 D6 E6 EE  87 85 29 36 AD 84 ED 7D F8 4C 8F BB 5A
44 DA 4C  A4 4B B7 60 17 B8 BE 49 12 DB 15 DC 84 D4 89 08  B5 27 84 71 92 5E 3D 5A A3
```

```
0A AA 0D FD 5E 32 56  DC A3 4B 89 F9 9D 28 A6 AC C3 31 68 F3 98 31 D3  0A 38 B6 E4 DD
87 8E 2E 95 A8 D4 BE 23 FB 48 42  BD 07 80 AC 8E D8 97 0F 46 C6 55 D8 F0 98 3F 33  26
47 A8 05 82 B3 D7 5D 08 A1 4A 30 F9 80 5D 7F  8A 80 98 A0 F5 C8 8A 56 FF EC 44 C3 20
40 AB 06  1C 8C 3B D1 E5 79 5B 02 F2 25 F8 06 31 54 B5 60  38 68 C7 EC 42 E9 36 BD 47
B6 BE 06 A8 1B 5B 92  0D 29 CD B3 E9 F5 7A EB E5 27 83 BC 0E 48 F6 93  21 62 81 0B CE
E4 92 67 35 4E AB 23 B7 AA 86 25  78 91 22 38 CC C1 95 A5 D4 4D 20 FE E3 AE F8 8F  24
E9 38 75 B2 31 82 49 00 D4 8F 9A 93 E0 A0 DD  D3 B1 F8 B9 B9 3D 2D 02
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
PromptOnSecureDesktop --> 0
EnableLUA --> 0
ConsentPromptBehaviorAdmin --> 0
```

```
HKEY_CLASSES_ROOT\[ID]PFOzv5ecUnxnfV9F[ID]_auto_file
HKEY_CLASSES_ROOT\.[ID]PFOBHpZYUnxnfV9F[ID] --> HKEY_CLASSES_ROOT\
[ID]PFOBHpZYUnxnfV9F[ID]_auto_file
HKEY_CLASSES_ROOT\[ID]PFOBHpZYUnxnfV9F[ID]_auto_file\shell\open\command -->
%SystemRoot%\System32\rundll32.exe "%ProgramFiles%\Windows Photo
Viewer\PhotoViewer.dll", ImageView_Fullscreen %1
HKEY_CLASSES_ROOT\[ID]PFOBHpZYUnxnfV9F[ID]_auto_file\shell\open\DropTarget -->
{FFE2A43C-56B9-4bf5-9A79-CC6D4285608A}
HKEY_CLASSES_ROOT\[ID]PFOBHpZYUnxnfV9F[ID]_auto_file\shell\open -->
@photoviewer.dll,-3043
HKEY_CLASSES_ROOT\[ID]PFOBHpZYUnxnfV9F[ID]_auto_file\shell\print\command -->
%SystemRoot%\System32\rundll32.exe "%ProgramFiles%\Windows Photo
Viewer\PhotoViewer.dll", ImageView_Fullscreen %1
HKEY_CLASSES_ROOT\[ID]PFOBHpZYUnxnfV9F[ID]_auto_file\shell\print\DropTarget -->
{60fd46de-f830-4894-a628-6fa81bc0190d}
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.
[ID]PFOBHpZYUnxnfV9F[ID]\OpenWithList --> PhotoViewer.dll
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.
[ID]PFOBHpZYUnxnfV9F[ID]\OpenWithProgids --> ID]PFOBHpZYUnxnfV9F[ID]_auto_file
```

E-Mail Addresses

```
First campaign (May 2018):

shine1@tutanota[.]com
shine2@protonmail.com

Second campaign (September/October 2019):

JonStokton@Protonmail[.]com
JonStokton@tutanota[.]com
filessnoop@aol[.]com
filessnoop@tutanota[.]com

Third campaign:

localgroup@protonmail[.]com
localgroup@tutanota[.]com
ZiCoyote@protonmail[.]com
ZiCoyote@aol[.]com

Forth campaign:

mr.dec@protonmail[.]com
mr.dec@tutanota[.]com

Frederik888@protonmail[.]com
Frederik888@aol[.]com
```

Ransomnote V1

```
You are unlucky! The terrible virus has captured your files! For decoding please
contact by email Frederik888@aol.com or Frederik888@protonmail.com
Your
[ID]PFOBHpZYUnxnfV9F[ID]
1. In the subject line, write your ID.
2. Attach 1-2 infected files that do not contain important information (less than 2
mb)
are required to generate the decoder and restore the test file.
Hurry up! Time is limited!
Attention!!!
At the end of this time, the private key for generating the decoder will be
destroyed. Files will not be restored!
```