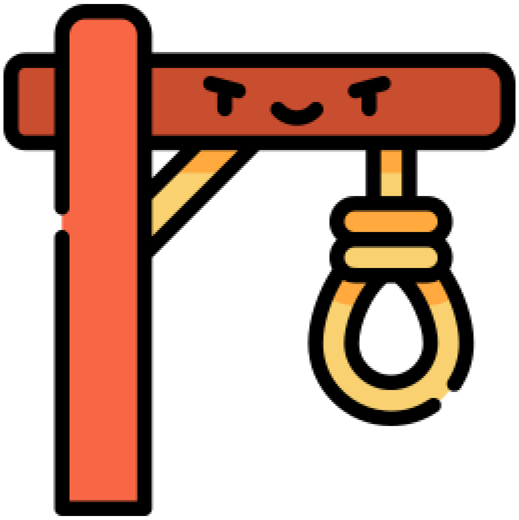
Quick and painless - Reversing DeathRansom / "Wacatac"

dissectingmalwa.re/quick-and-painless-reversing-deathransom-wacatac.html

Tue 19 November 2019 in Ransomware

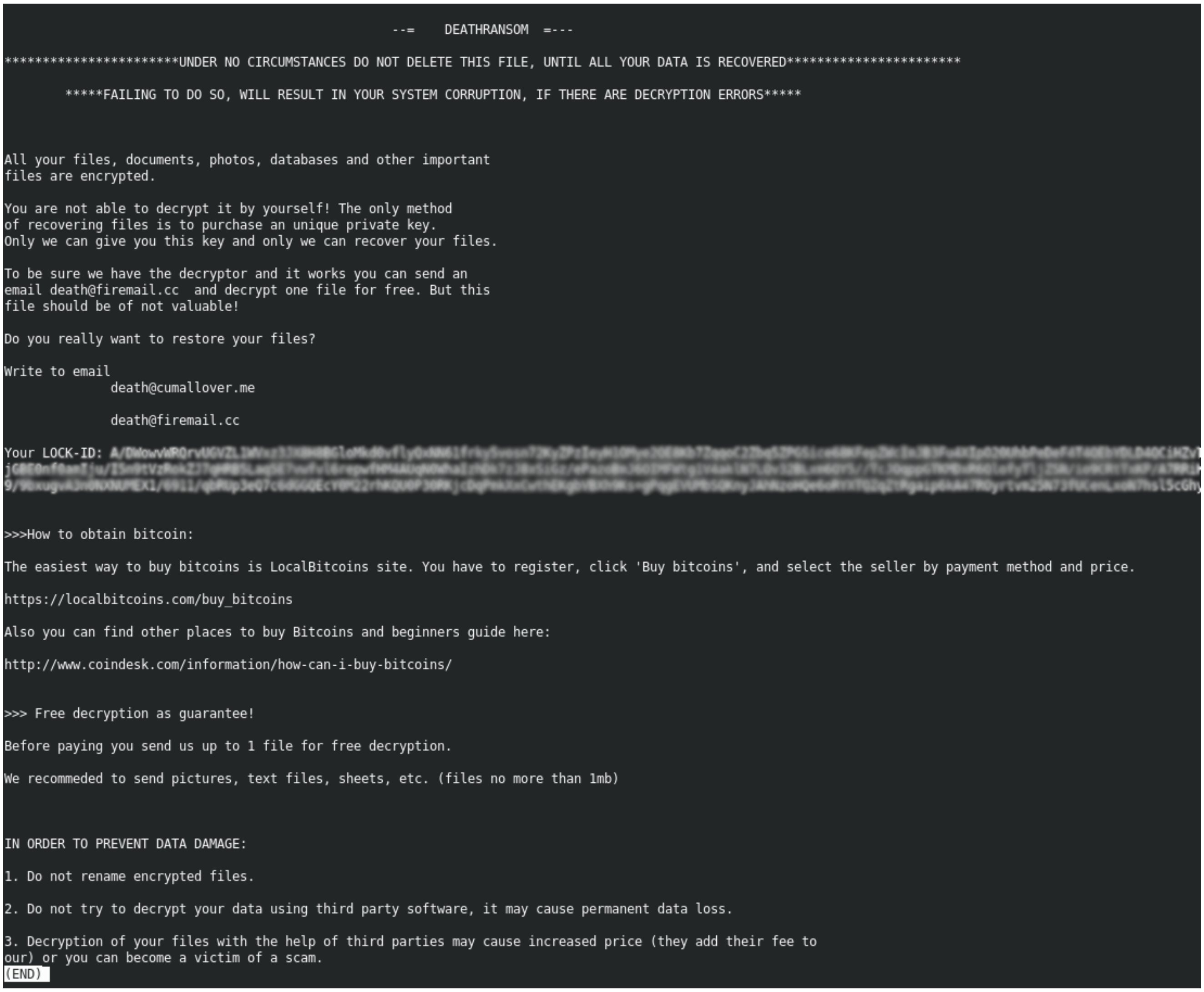
No flashy wallpapers or other bells and whistles, but if you aren't careful and maintain backups as you should DeathRansom will take your data with it to its grave. Or will it ?



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.

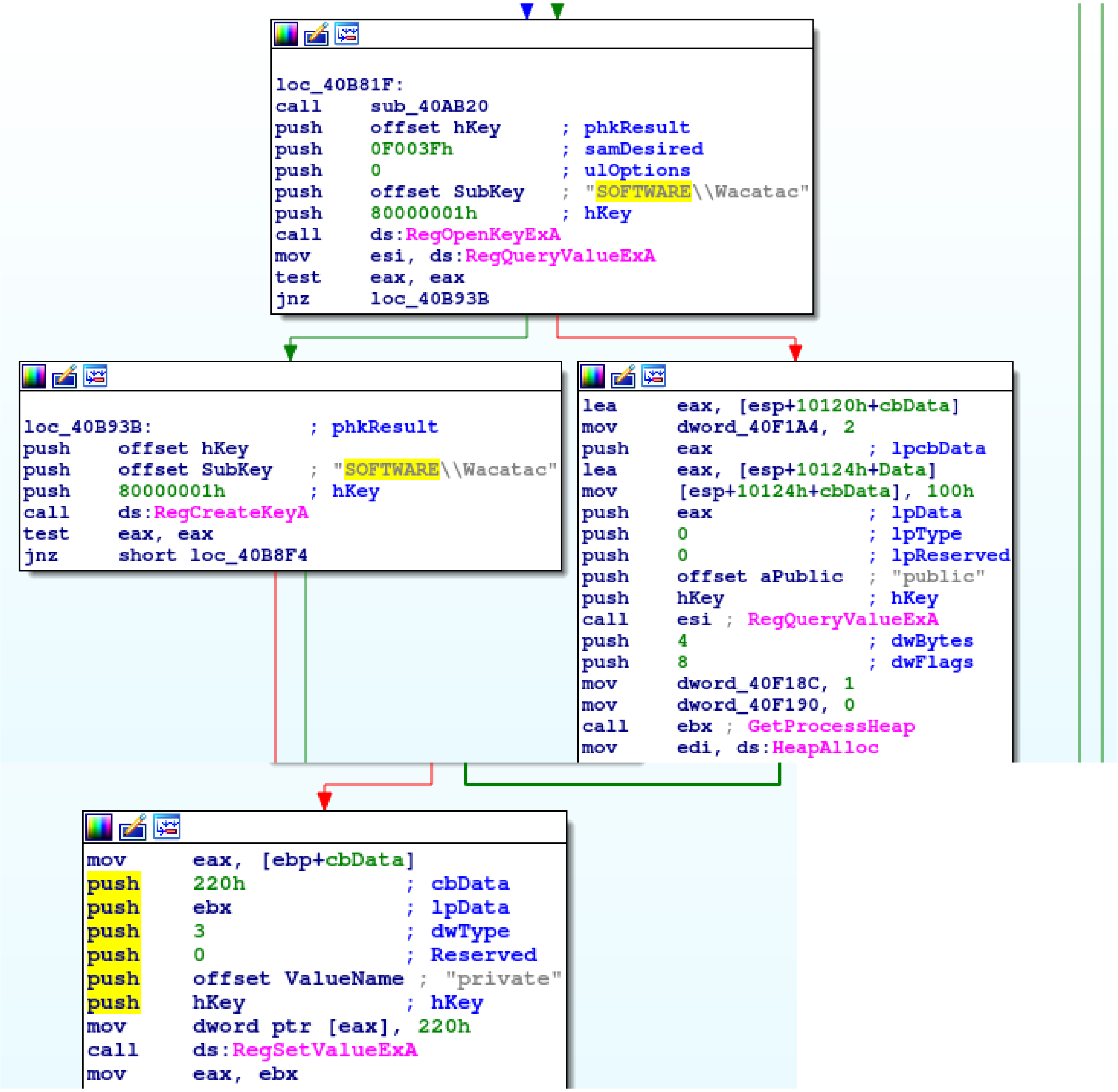
DeathRansom @ AnyRun | VirusTotal | HybridAnalysis --> `sha256 3a5b015655f3aad4b4fd647aa34fda4ce784d75a20d12a73f8dc0e0d866e7e01`

The plain text note doesn't look that special. I'll be refering to this strain as Deathransom, since the Wacatac Trojan doesn't seem to be affiliated with the sample.



```
                                                       --=    DEATHRANSOM  =---

***********************UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR DATA IS RECOVERED***********************

        *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE DECRYPTION ERRORS*****



All your files, documents, photos, databases and other important
files are encrypted.

You are not able to decrypt it by yourself! The only method
of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.

To be sure we have the decryptor and it works you can send an
email death@firemail.cc  and decrypt one file for free. But this
file should be of not valuable!

Do you really want to restore your files?

Write to email
               death@cumallover.me

               death@firemail.cc

Your LOCK-ID: [redacted]


>>>How to obtain bitcoin:

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the seller by payment method and price.

https://localbitcoins.com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

http://www.coindesk.com/information/how-can-i-buy-bitcoins/


>>> Free decryption as guarantee!

Before paying you send us up to 1 file for free decryption.

We recommeded to send pictures, text files, sheets, etc. (files no more than 1mb)



IN ORDER TO PREVENT DATA DAMAGE:

1. Do not rename encrypted files.

2. Do not try to decrypt your data using third party software, it may cause permanent data loss.

3. Decryption of your files with the help of third parties may cause increased price (they add their fee to
our) or you can become a victim of a scam.
(END)
```

The "Wacatac" Registry Keys are most likely an attempt at a false flag manouver. The Ransomware will set three Regkeys in total: The main Key **HKEY_CURRENT_USER\SOFTWARE\Wacatac** and two sub keys called **private** and **public**. The hex value set in the "private" acutally corresponds to the Lock ID referenced in the Ransomnote. Analysing the encryption loop will probably present the relation between these values, so I'll keep going.



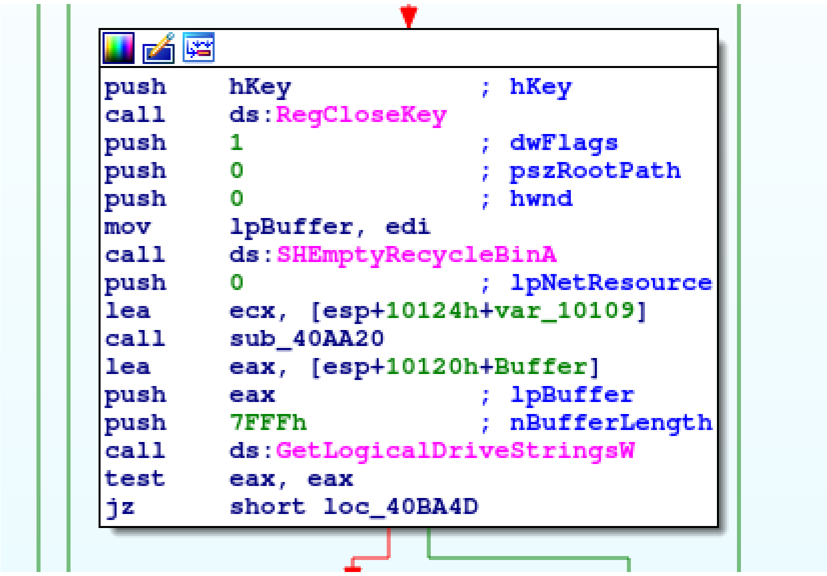
```
loc_40B81F:
call    sub_40AB20
push    offset hKey     ; phkResult
push    0F003Fh         ; samDesired
push    0               ; ulOptions
push    offset SubKey   ; "SOFTWARE\\Wacatac"
push    80000001h       ; hKey
call    ds:RegOpenKeyExA
mov     esi, ds:RegQueryValueExA
test    eax, eax
jnz     loc_40B93B
```

```
loc_40B93B:             ; phkResult
push    offset hKey
push    offset SubKey   ; "SOFTWARE\\Wacatac"
push    80000001h       ; hKey
call    ds:RegCreateKeyA
test    eax, eax
jnz     short loc_40B8F4
```

```
lea     eax, [esp+10120h+cbData]
mov     dword_40F1A4, 2
push    eax             ; lpcbData
lea     eax, [esp+10124h+Data]
mov     [esp+10124h+cbData], 100h
push    eax             ; lpData
push    0               ; lpType
push    0               ; lpReserved
push    offset aPublic  ; "public"
push    hKey            ; hKey
call    esi ; RegQueryValueExA
push    4               ; dwBytes
push    8               ; dwFlags
mov     dword_40F18C, 1
mov     dword_40F190, 0
call    ebx ; GetProcessHeap
mov     edi, ds:HeapAlloc
```

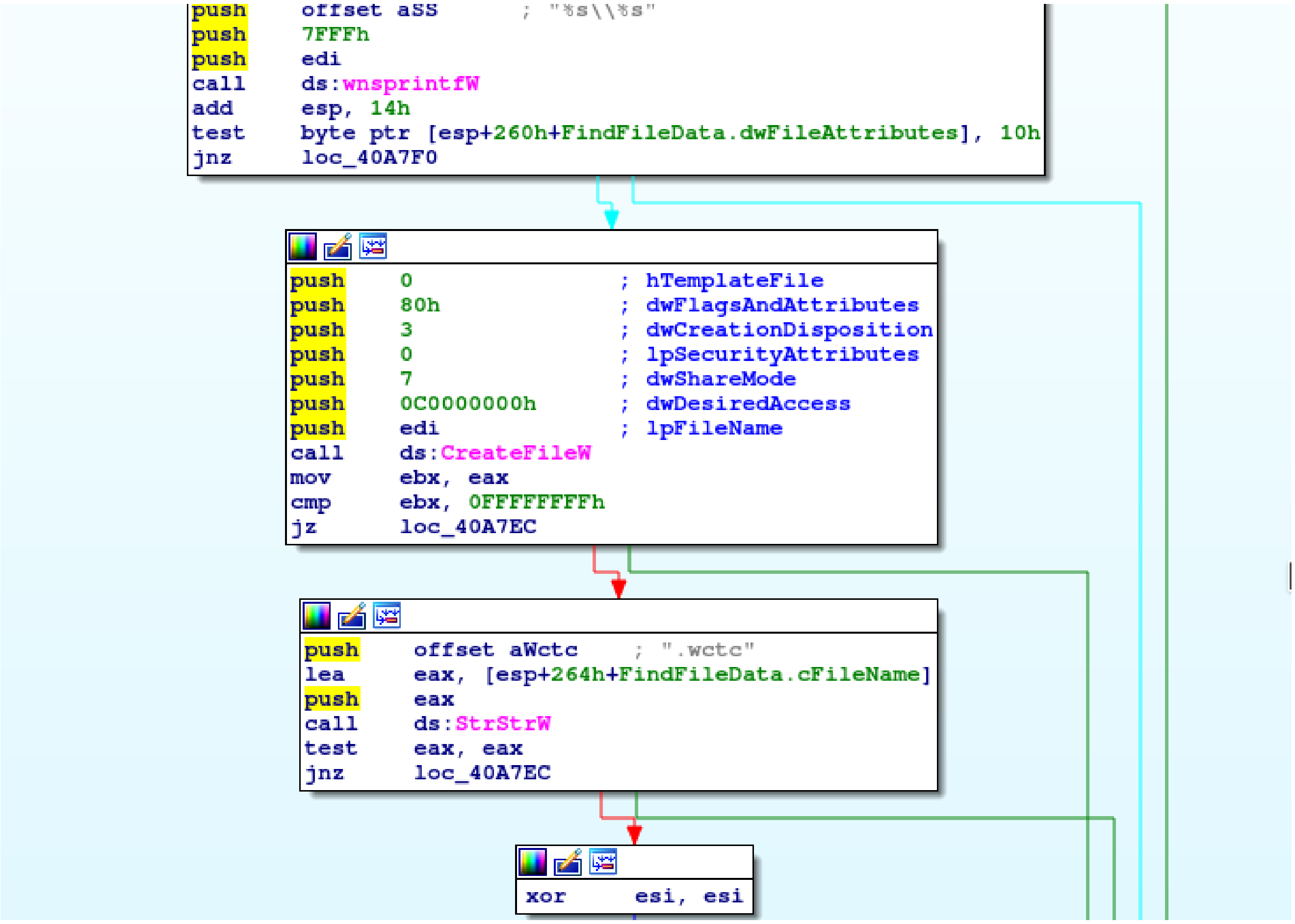
```
mov     eax, [ebp+cbData]
push    220h            ; cbData
push    ebx             ; lpData
push    3               ; dwType
push    0               ; Reserved
push    offset ValueName ; "private"
push    hKey            ; hKey
mov     dword ptr [eax], 220h
call    ds:RegSetValueExA
mov     eax, ebx
```

Somewhat of a rare occurance, but Deathransom will actually take out the trash for you by clearing the recycling bin.



```
push    hKey                ; hKey
call    ds:RegCloseKey
push    1                   ; dwFlags
push    0                   ; pszRootPath
push    0                   ; hwnd
mov     lpBuffer, edi
call    ds:SHEmptyRecycleBinA
push    0                   ; lpNetResource
lea     ecx, [esp+10124h+var_10109]
call    sub_40AA20
lea     eax, [esp+10120h+Buffer]
push    eax                 ; lpBuffer
push    7FFFh               ; nBufferLength
call    ds:GetLogicalDriveStringsW
test    eax, eax
jz      short loc_40BA4D
```

Generally this sample seems to be very limited in features, but let's see how they implemented the encryption routine. Looking for *CreateFileW* we can see that it appends the *.wctc* extension to the name of the current file. But where's the encryption happening? Either they hid it very well or they just plainly forgot about it 🤔



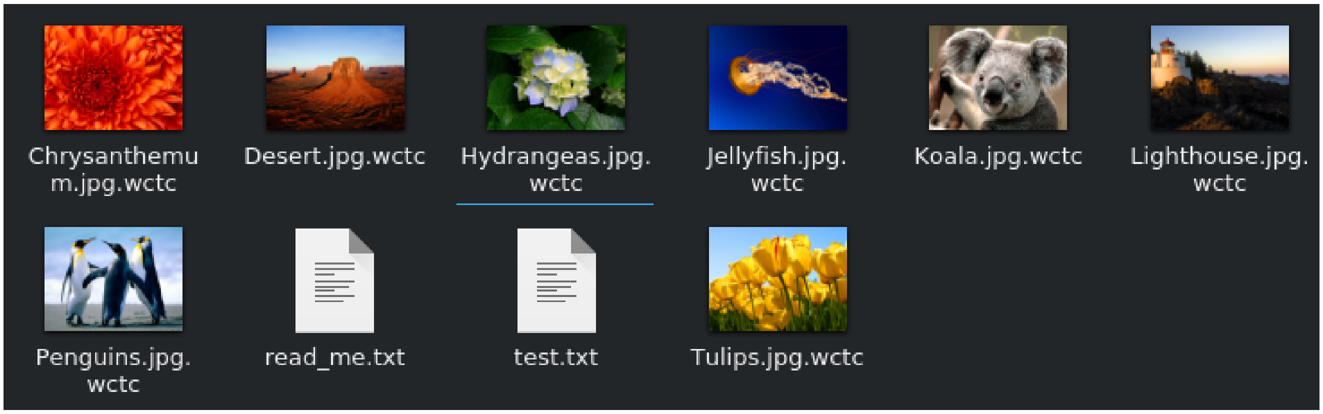
```
push    offset aSS      ; "%s\\%s"
push    7FFFh
push    edi
call    ds:wnsprintfW
add     esp, 14h
test    byte ptr [esp+260h+FindFileData.dwFileAttributes], 10h
jnz     loc_40A7F0
```

```
push    0               ; hTemplateFile
push    80h             ; dwFlagsAndAttributes
push    3               ; dwCreationDisposition
push    0               ; lpSecurityAttributes
push    7               ; dwShareMode
push    0C0000000h      ; dwDesiredAccess
push    edi             ; lpFileName
call    ds:CreateFileW
mov     ebx, eax
cmp     ebx, 0FFFFFFFFh
jz      loc_40A7EC
```

```
push    offset aWctc    ; ".wctc"
lea     eax, [esp+264h+FindFileData.cFileName]
push    eax
call    ds:StrStrW
test    eax, eax
jnz     loc_40A7EC
```

```
xor     esi, esi
```

Let's just fire up a VM and see what happens to the files after the encryption takes place so we have a better idea of what to look for. I got no UAC prompt upon running the sample and the ransom process seemed a bit fast. Checking out the sample files we can see what actually happened:

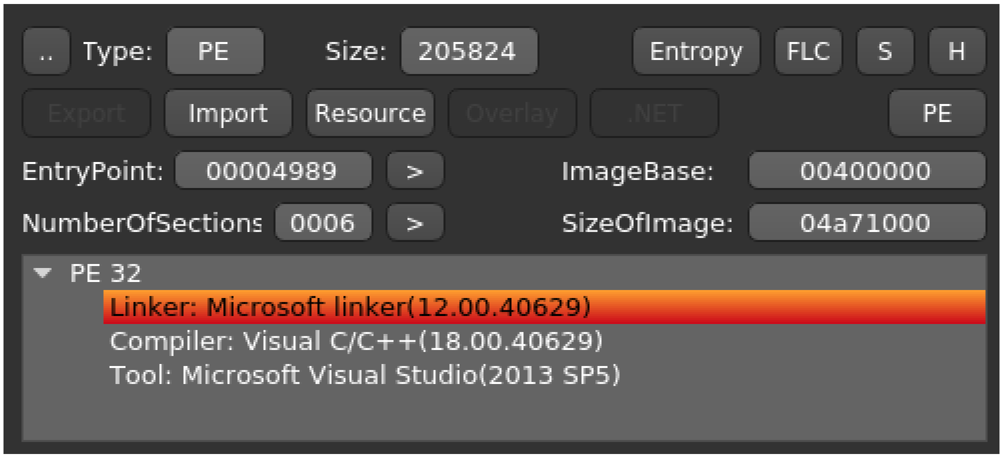


Exactly, nothing. I don't want to jump to conclusions here, but this strain might still be in the testing stage or is just a plain hoax. Regardless it is still possible that another variant turns up that will actually encrypt the files.

Update 25.11.2019:

As predicted there is another version of the Ransomware available now and it seems to do its job a lot more thorough than its predecessor. The new build doesn't seem to append a new suffix to the file and the ransomnote has been adapted slightly because it now features a Bitcoin wallet address and a new E-Mail contact.

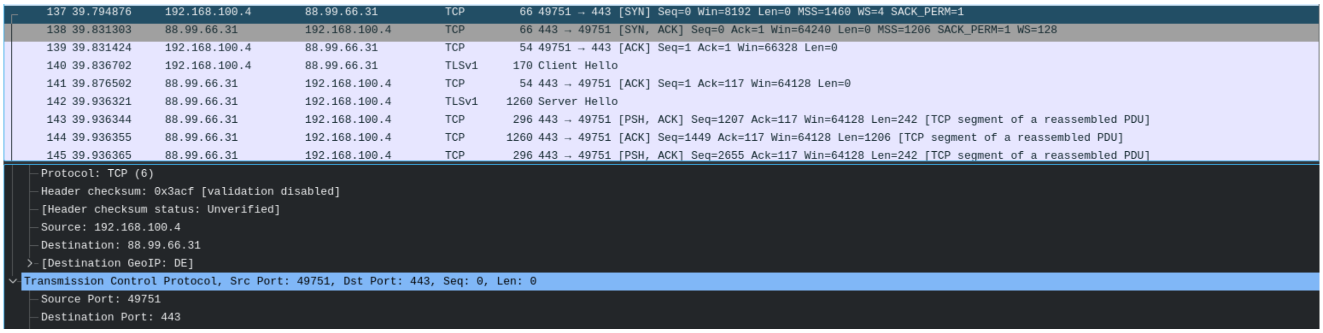
DeathRansom V2 @ AnyRun --> `sha256 fedb4c3b0e080fb86796189ccc77f99b04adb105d322bddd3abfca2d5c5d43c8`



Type: PE
Size: 205824
EntryPoint: 00004989
ImageBase: 00400000
NumberOfSections: 0006
SizeOfImage: 04a71000

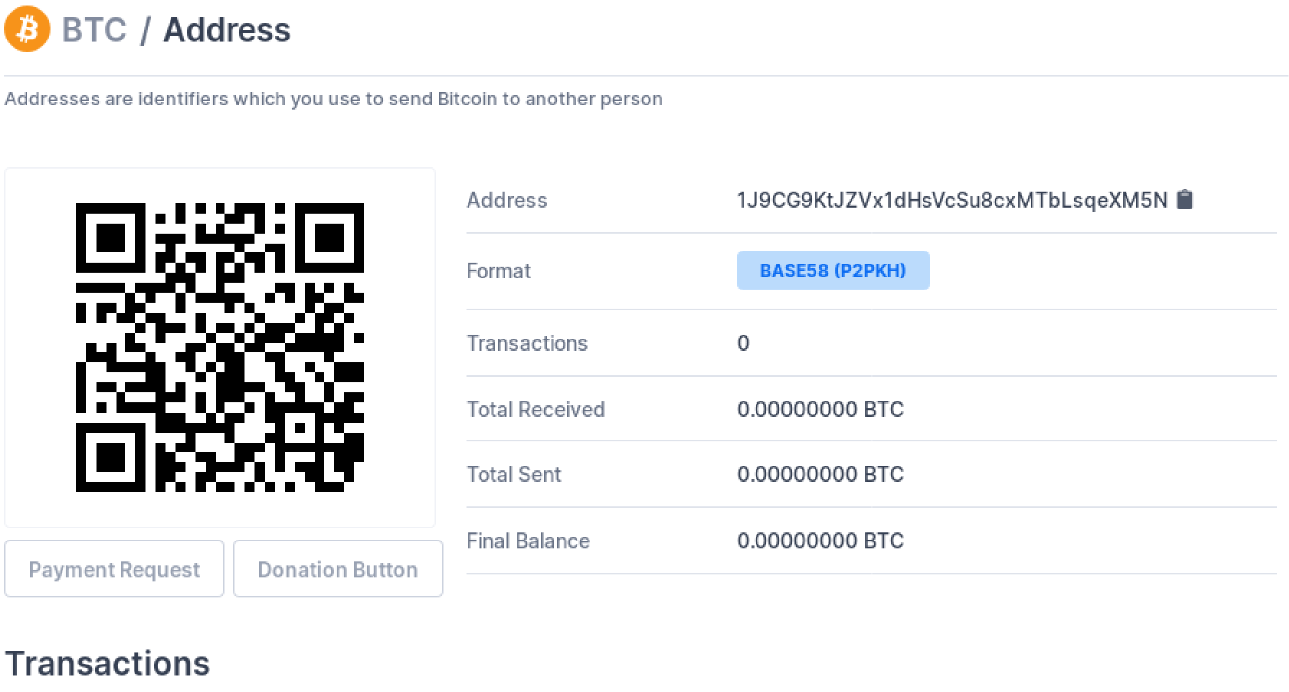
```
PE 32
    Linker: Microsoft linker(12.00.40629)
    Compiler: Visual C/C++(18.00.40629)
    Tool: Microsoft Visual Studio(2013 SP5)
```

Entropy-wise the sample doesn't seem to be packed and nor are there any weird sections or paddings. Compiler and Linker Versions point towards Visual Studio 2013 being utilized by the creators.



```
   137 39.794876    192.168.100.4     88.99.66.31       TCP        66 49751 → 443 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
   138 39.831303    88.99.66.31       192.168.100.4     TCP        66 443 → 49751 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1206 SACK_PERM=1 WS=128
   139 39.831424    192.168.100.4     88.99.66.31       TCP        54 49751 → 443 [ACK] Seq=1 Ack=1 Win=66328 Len=0
   140 39.836702    192.168.100.4     88.99.66.31       TLSv1     170 Client Hello
   141 39.876502    88.99.66.31       192.168.100.4     TCP        54 443 → 49751 [ACK] Seq=1 Ack=117 Win=64128 Len=0
   142 39.936321    88.99.66.31       192.168.100.4     TLSv1    1260 Server Hello
   143 39.936344    88.99.66.31       192.168.100.4     TCP       296 443 → 49751 [PSH, ACK] Seq=1207 Ack=117 Win=64128 Len=242 [TCP segment of a reassembled PDU]
   144 39.936355    88.99.66.31       192.168.100.4     TCP      1260 443 → 49751 [ACK] Seq=1449 Ack=117 Win=64128 Len=1206 [TCP segment of a reassembled PDU]
   145 39.936365    88.99.66.31       192.168.100.4     TCP       296 443 → 49751 [PSH, ACK] Seq=2655 Ack=117 Win=64128 Len=242 [TCP segment of a reassembled PDU]
    ├─Protocol: TCP (6)
    ├─Header checksum: 0x3acf [validation disabled]
    ├─[Header checksum status: Unverified]
    ├─Source: 192.168.100.4
    ├─Destination: 88.99.66.31
    >─[Destination GeoIP: DE]
  ⌄─Transmission Control Protocol, Src Port: 49751, Dst Port: 443, Seq: 0, Len: 0
    ├─Source Port: 49751
    ├─Destination Port: 443
```

Looking at the packets captured during the dynamic analysis we notice a DNS request plus TCP traffic to iplogger[.]org which was not present in the first Version of the Ransomware. Looks like the criminals are trying to track infections over time.



BTC / Address

Addresses are identifiers which you use to send Bitcoin to another person

Address	1J9CG9KtJZVx1dHsVcSu8cxMTbLsqeXM5N
Format	BASE58 (P2PKH)
Transactions	0
Total Received	0.00000000 BTC
Total Sent	0.00000000 BTC
Final Balance	0.00000000 BTC

Transactions

According to Blockchain.com the Bitcoin Wallet mentioned in the V2 Ransomnote doesn't have any transactions on it as of the 30th of November, which is really good news :)

IOCs

DeathRansom

```
deathransom.exe --> SHA256:
7c2dbad516d18d2c1c21ecc5792bc232f7b34dadc1bc19e967190d79174131d1
                    SSDEEP:
1536:gZVYb2bbBisyEcPC00h7sBvvKk+jTc7+T8l7RJV62CzVDL+oWB27evMCUQ:EV+GiVEc6RsMJQ

fyukfuyk.exe    --> SHA256:
ab828f0e0555f88e3005387cb523f221a1933bbd7db4f05902a1e5cc289e7ba4
                    SSDEEP:
6144:f849/IB5jZozuL1itPJAOsF0l+t5Dn0ChC:f8kIB5jZyNVJWF0AHDC

2p1km7pr6l.exe  --> SHA256:
fedb4c3b0e080fb86796189ccc77f99b04adb105d322bddd3abfca2d5c5d43c8
                            3072:ou1DaA5w1KmC5RjPquqavANItF2rv8ojAjAD5m9:Kb6Lq8wHUoe
```

E-Mail Addresses

```
death@firemail[.]cc
death@cumallover[.]me
deathransom@airmail[.]cc
```

Registry Keys

```
HKEY_CURRENT_USER\SOFTWARE\Wacatac

HKEY_CURRENT_USER\SOFTWARE\Wacatac\public
FA DE 13 AA 52 43 DF 85  B2 62 A5 88 1D 17 D0 59 99 BF 6B 69 5F 71 1C 76  D4 4A 36 86
B6 47 CA D4 A2 C0 40 52 D5 FF FC B8  DE E2 F7 7F 5A 75 27 10 1C 64 31 CE 55 82 FD 91
8F 58 65 C3 5E 49 E1 14 DD 89 9B 9C 59 EB 11 54  AC A2 1B 8A E4 DC 62 FF 21 1A F4 5F
44 FB 76 1A  4C D0 07 0F 6A 83 06 B6 32 54 B8 9B EC EF 0F 25  9A FD 95 AC 5B 53 D5 9F
2A 04 CC C4 93 6A 06 02  7D 41 63 A8 BF BB AA E1 1F BD E5 DA F9 7A 46   0A 89 89 D0
EC 62 55 B5 E7 A3 D4 C5 80 C7 34 39  1D 71 27 60 EA 1B 45 2D A0 90 F9 75 E8 D3 A4 DF
E4 C5 E0 5C BB B8 46 91 87 AA 05 E3 06 8D A0 89  F6 12 74 B4 CA 0B 62 A0 F7 E3 A6 93
0C  77 C3  C9 A1 DE DB A0 0F CC D6 A2 0C DD AB 94 9B 25 90  4A A4 56 91 C4 07 BA 13
FA E9 44 23 FB 3C 8E 53  D2 82 6F B5 4B C3 EE 2F E4 1F C0 16 03 89 5F DE  EA E7 76 12
A9 A3 13 0F

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

Ransomnote Version 1

```
                                                    --=    DEATHRANSOM  =---

***********************UNDER NO CIRCUMSTANCES DO NOT DELETE THIS FILE, UNTIL ALL YOUR
DATA IS RECOVERED***********************

    *****FAILING TO DO SO, WILL RESULT IN YOUR SYSTEM CORRUPTION, IF THERE ARE
DECRYPTION ERRORS*****



All your files, documents, photos, databases and other important
files are encrypted.

You are not able to decrypt it by yourself! The only method
of recovering files is to purchase an unique private key.
Only we can give you this key and only we can recover your files.

To be sure we have the decryptor and it works you can send an
email death@firemail.cc  and decrypt one file for free. But this
file should be of not valuable!

Do you really want to restore your files?

Write to email
              death@cumallover[.]me

              death@firemail[.]cc

Your LOCK-ID: [Redacted Base64]

>>>How to obtain bitcoin:

The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click
'Buy bitcoins', and select the seller by payment method and price.

hxxps://localbitcoins[.]com/buy_bitcoins

Also you can find other places to buy Bitcoins and beginners guide here:

hxxp://www.coindesk[.]com/information/how-can-i-buy-bitcoins/


>>> Free decryption as guarantee!

Before paying you send us up to 1 file for free decryption.

We recommeded to send pictures, text files, sheets, etc. (files no more than 1mb)



IN ORDER TO PREVENT DATA DAMAGE:

1. Do not rename encrypted files.

2. Do not try to decrypt your data using third party software, it may cause permanent
```

```
data loss.

3. Decryption of your files with the help of third parties may cause increased price
(they add their fee to
our) or you can become a victim of a scam.
```

Ransomnote Version 2

```
?????????????????????????
??????DEATHRansom ???????
?????????????????????????
Hello dear friend,
Your files were encrypted!
You have only 12 hours to decrypt it
In case of no answer our team will delete your decryption password
Write back to our e-mail: deathransom@airmail[.]cc


In your message you have to write:
1. YOU LOCK-ID:
PUmZiYT3OkC9IpVXHpZFOFzZ5Y7+dLuV9cYUSZ30UyPLeMPEPO4TZ79CCCbiTpSltqKKBv3oFqgH0O6lyre7hv

2. Time when you have paid 0.1 btc to this bitcoin wallet:
1J9CG9KtJZVx1dHsVcSu8cxMTbLsqeXM5N


After payment our team will decrypt your files immediatly


Free decryption as guarantee:
1. File must be less than 1MB
2. Only .txt or .lnk files, no databases
3. Only 1 files


How to obtain bitcoin:
The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click
'Buy bitcoins', and select the seller by payment method and price.
hxxps://localbitcoins[.]com/buy_bitcoins
Also you can find other places to buy Bitcoins and beginners guide here:
hxxp://www.coindesk[.]com/information/how-can-i-buy-bitcoins/
```

Gallow Icon made by Freepik from www.flaticon.com