I literally can't think of a fitting pun - mrdec ransomware

By f0wL

Published: 2019-12-23 · Archived: 2026-04-05 13:58:04 UTC

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.

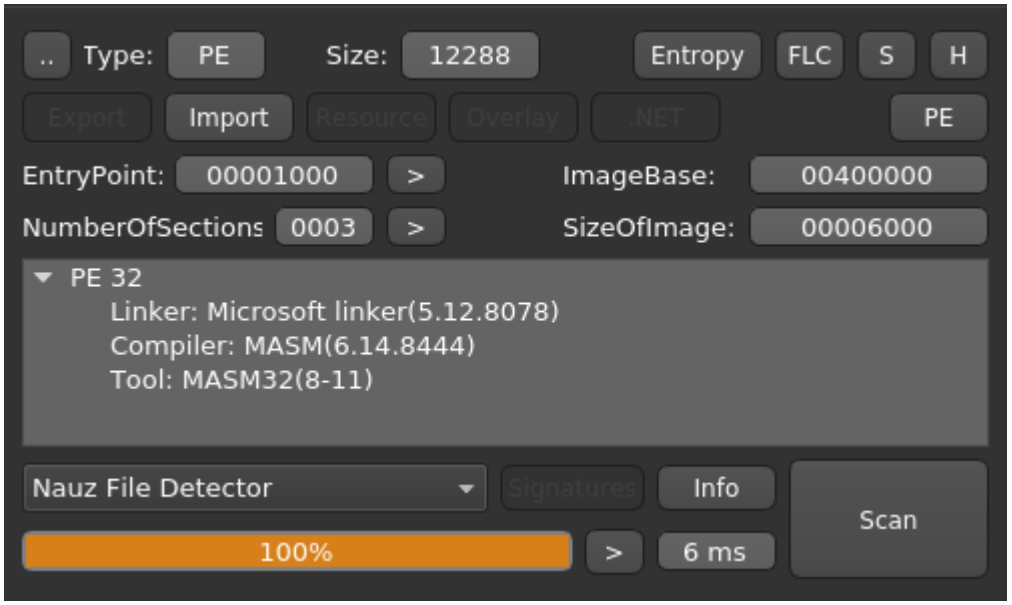
Work in Progress

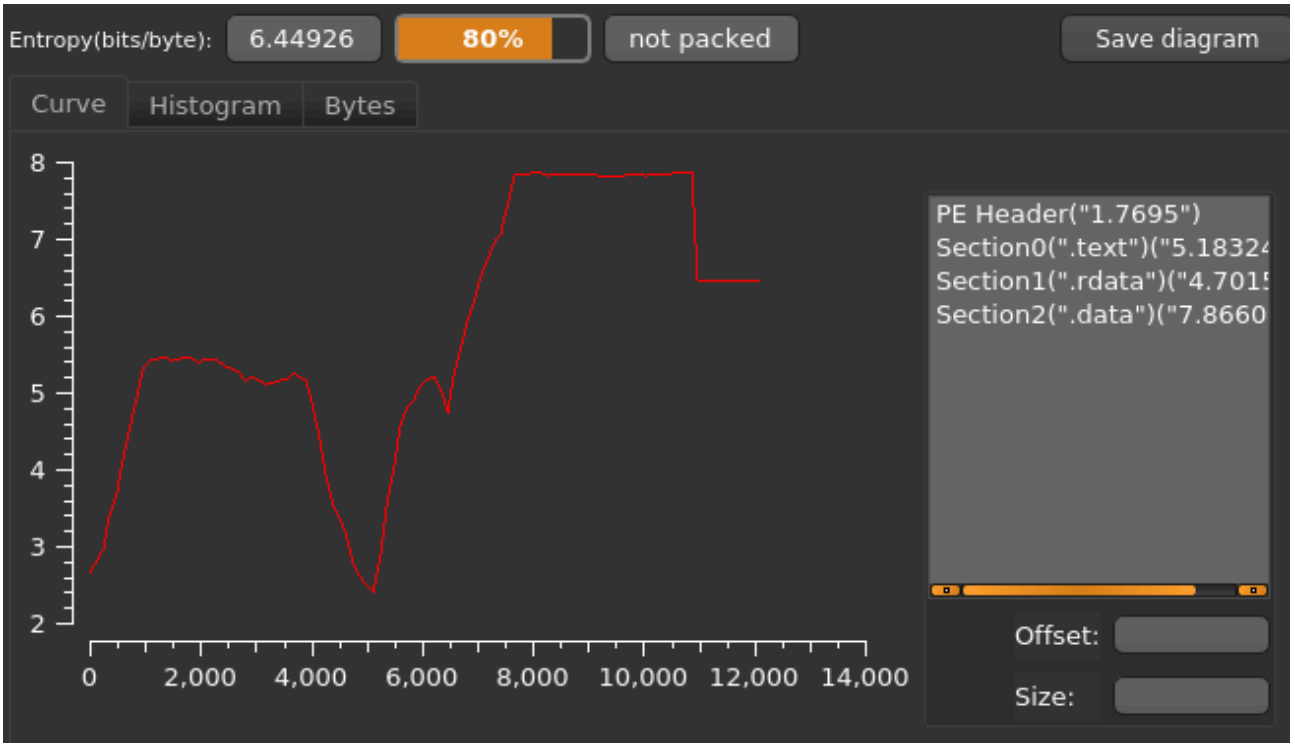
Because Christmas and 36c3 is coming up in the next few I days I might have to push this analysis back a bit.

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.

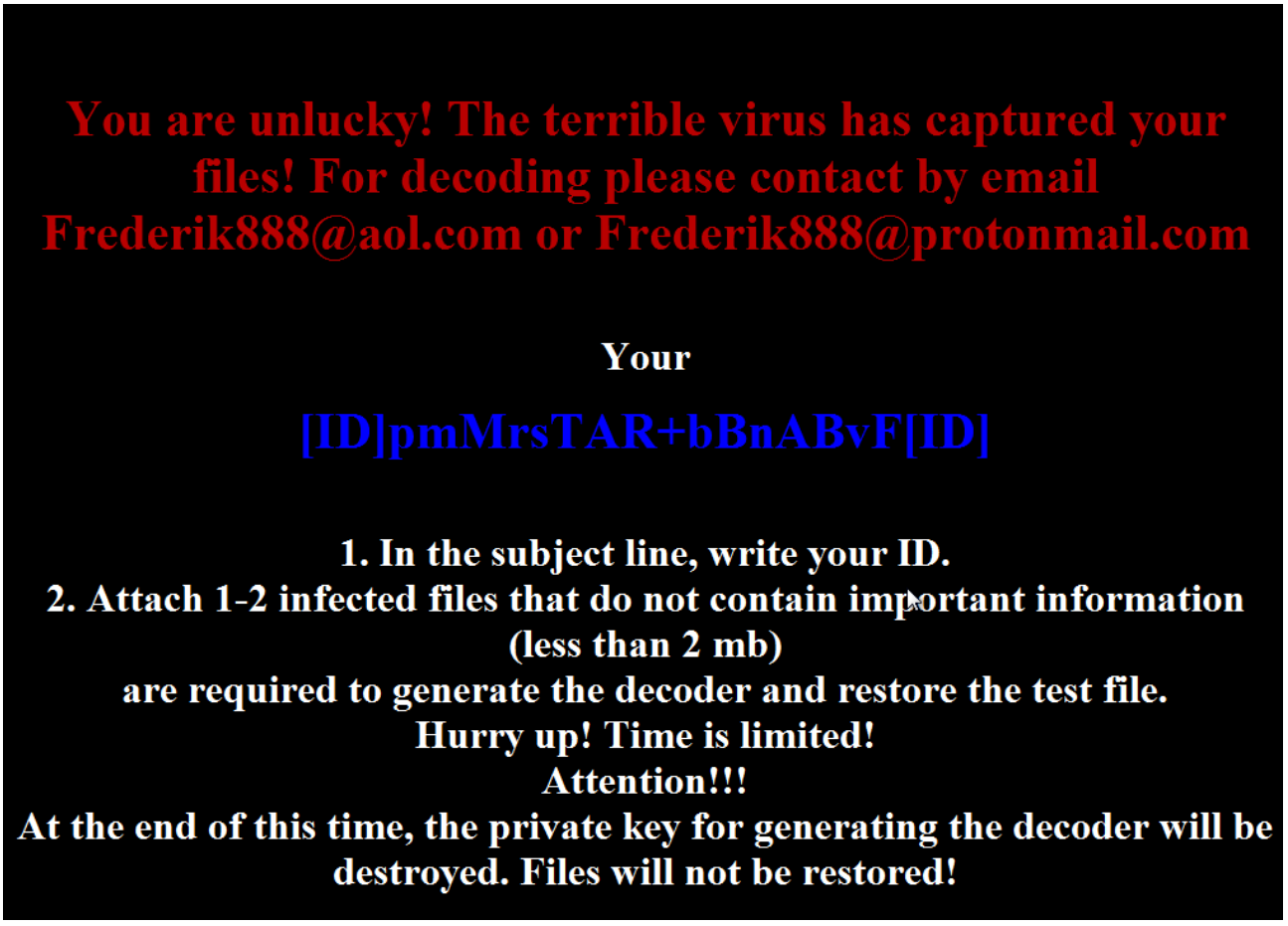
MrDec @ AnyRun | VirusTotal | HybridAnalysis --> `sha256` `a700f9ced75c4143da6c4d1e09d6778e84ff570ea7d297fc130a0844e56c96ad`

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

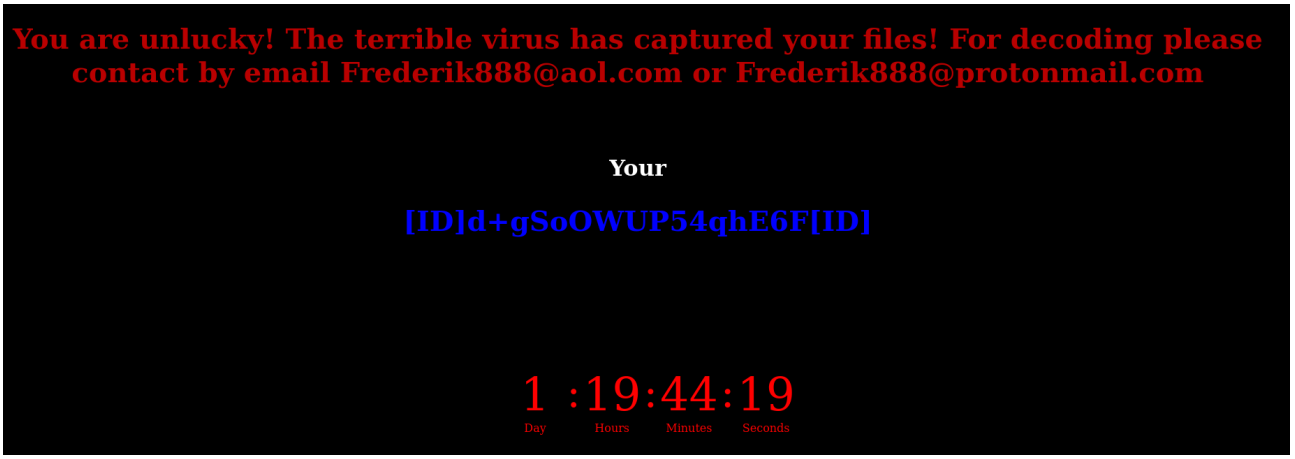




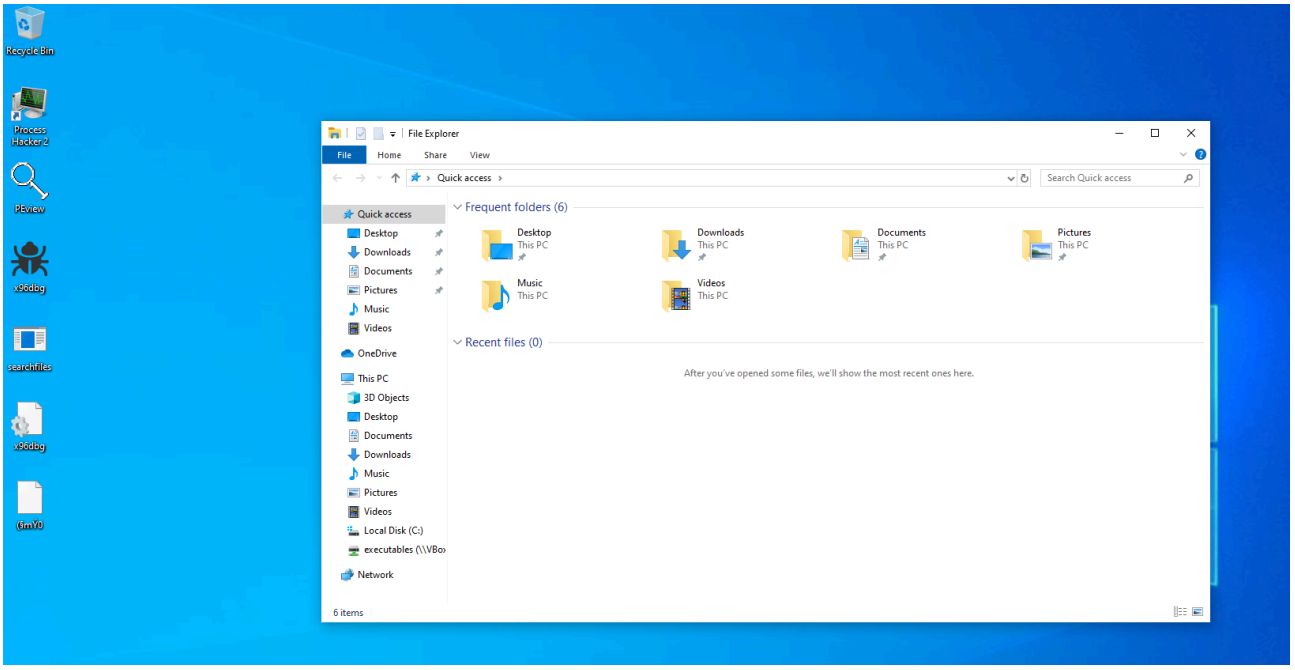
The Ransomnote is delivered via a *.hta* file. Like most other strains active in the last few month the criminals use two E-Mail addresses: a "primary" and a "backup". In this case they are using Protonmail and AOL which has been kind of a pattern for them (Tutanota is their third preferred service,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

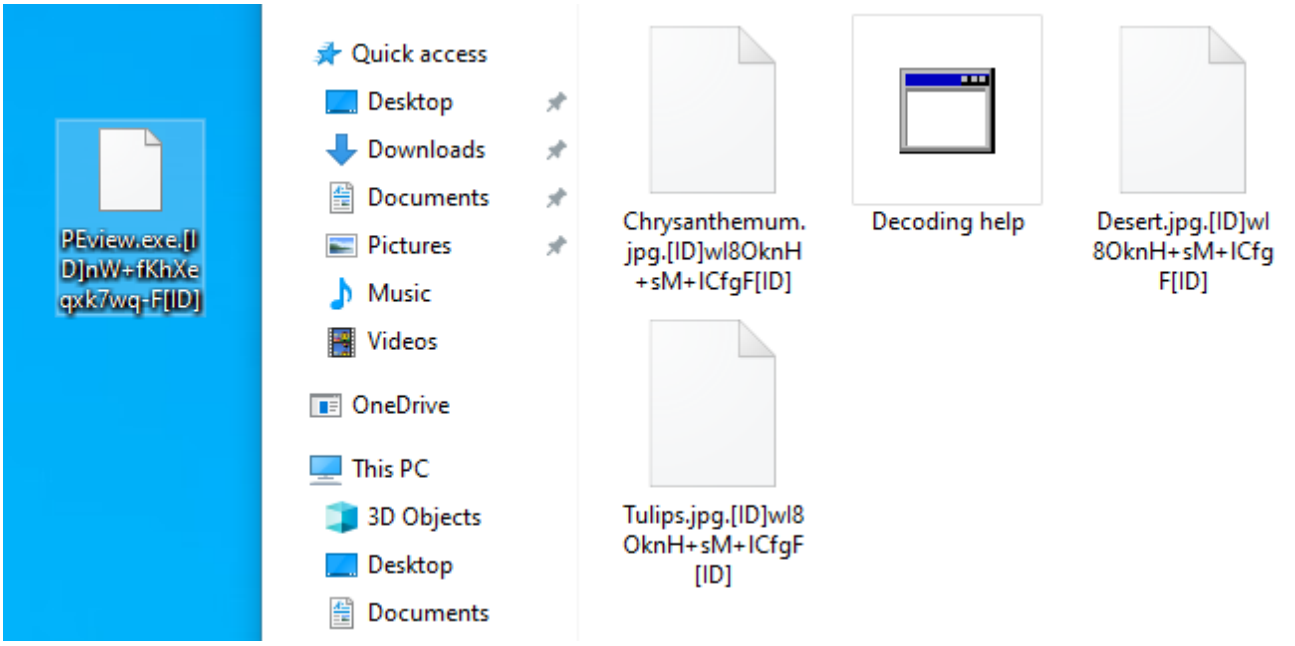


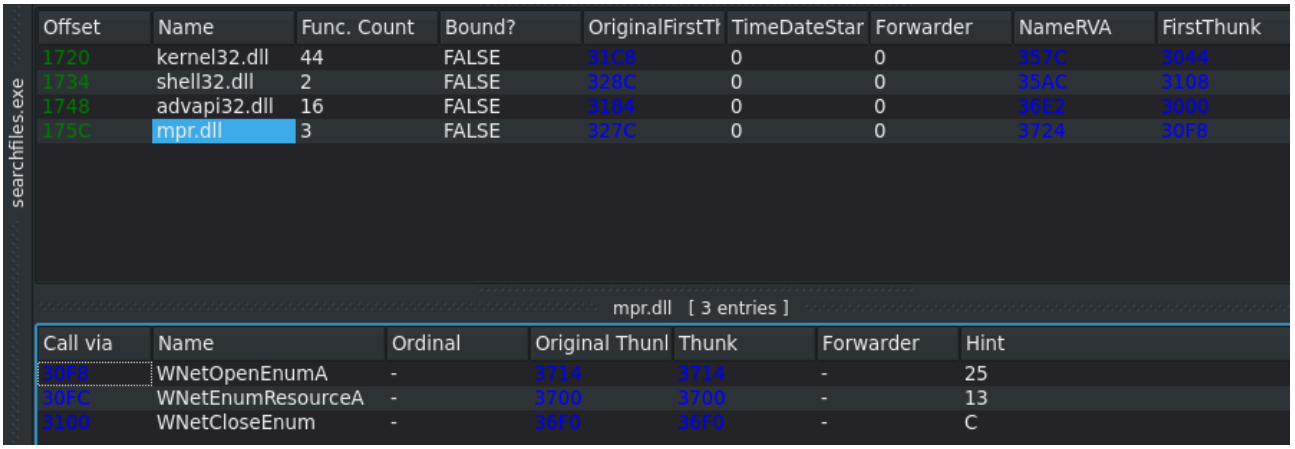
Opening the note in another browser (Chrome in this case) won't show the instructions but a countdown timer. The victim won't be able to see the timer in most cases because when using Internet Explorer because scrolling is disabled :D

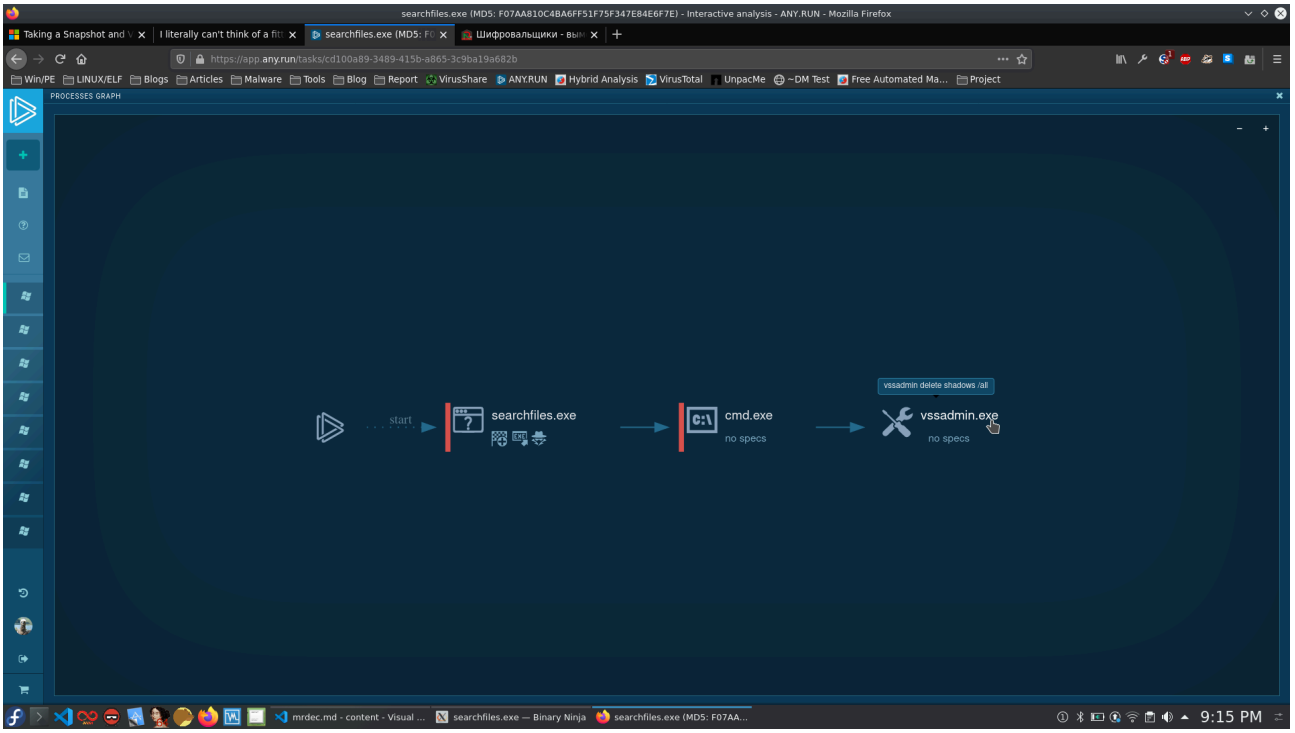


Ransomnote in Chrome

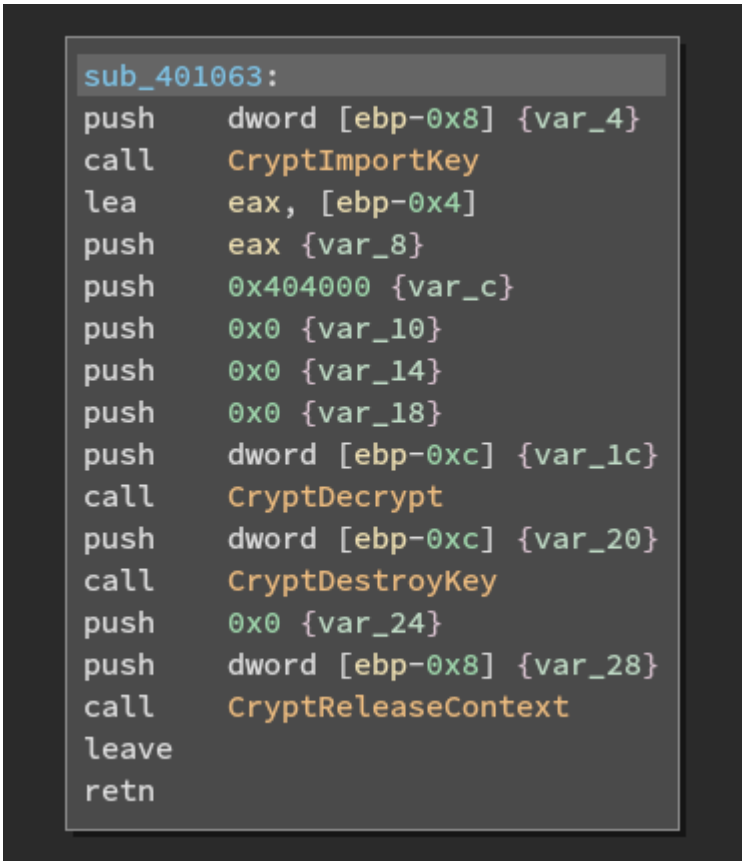

Recycle Bin
Process Hacker 2
PEview
x96dbg
searchfiles
x96dbg
6mY0
File Explorer
File
Home
Share
View
Quick access
Search Quick access
Frequent folders (6)
Desktop
This PC
Downloads
This PC
Documents
This PC
Pictures
This PC
Music
This PC
Videos
This PC
Recent files (0)
After you've opened some files, we'll show the most recent ones here.
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
executables (\\VBox
Network
6 items


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 Thunk Thunk Forwarder Hint
30F8 WNetOpenEnumA - 3714 3714 - 25
50FC WNetEnumResourceA - 3700 3700 - 13
3100 WNetCloseEnum - 36F0 36F0 - C

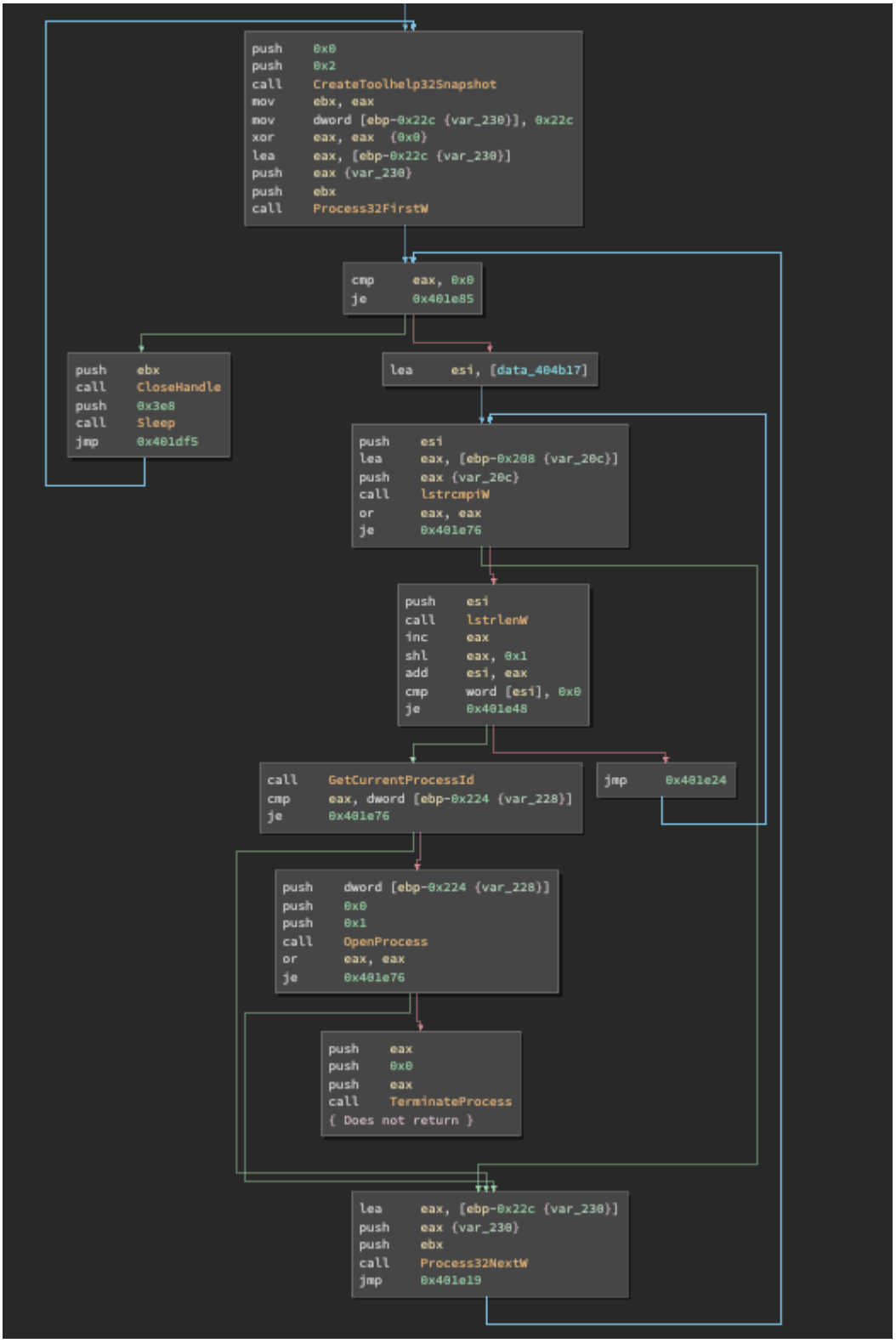

searchfiles.exe (MD5: F07AA810C4BA6FF51F75F347E84E6F7E) - Interactive analysis - ANY.RUN - Mozilla Firefox
PROCESSES GRAPH
start
searchfiles.exe
cmd.exe
no specs
vssadmin delete shadows /all
vssadmin.exe
no specs
9:15 PM


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
```

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



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 {var_68_2}
call    lstrcatA
push    eax {var_6c_2}
push    0x404ac8
push    0x1 {var_70_2}
push    0x0 {var_74_2}
push    0x404ae0
push    dword [ebp-0x20 {var_24}] {var_78_2}
call    RegSetValueExA
```

```
00404abb  28 a7 9d 6d dd     (..m.
00404ac0  30 00 b4 89 4d 06 a0 2a  0...M..*
00404ac8  df 9d 6b 8d d9 95 b4 e3  ..k.....
00404ad0  30 5c a2 28 80 6a 63 4c  0\.(.jcL
00404ad8  4f 50 cf d2 08 f4 9f 3b  OP.....;
00404ae0  dc bd 59 f3 70 44 ac 9a  ..Y.pD..
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+
```

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 (
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

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\ru
HKEY_CLASSES_ROOT\[ID]PFOBHpZYUnxnfV9F[ID]_auto_file\shell\open\DropTarget --> {FFE2A43C-56B9-4bf5-9A
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\ru
HKEY_CLASSES_ROOT\[ID]PFOBHpZYUnxnfV9F[ID]_auto_file\shell\print\DropTarget --> {60fd46de-f830-4894-a
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.[ID]PFOBHpZYUnxnfV9F[
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Explorer\FileExts\.[ID]PFOBHpZYUnxnfV9F[
```

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 Fr
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 no
```

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