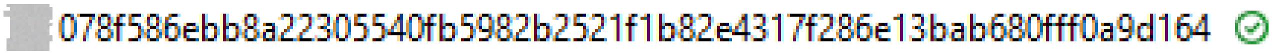
Malware Analysis: Mystery File

<u>Analysis Members</u>:
James Baumhardt, Brendon Werner, Ben Saunders, Brendan Kinder

---

STATIC ANALYSIS

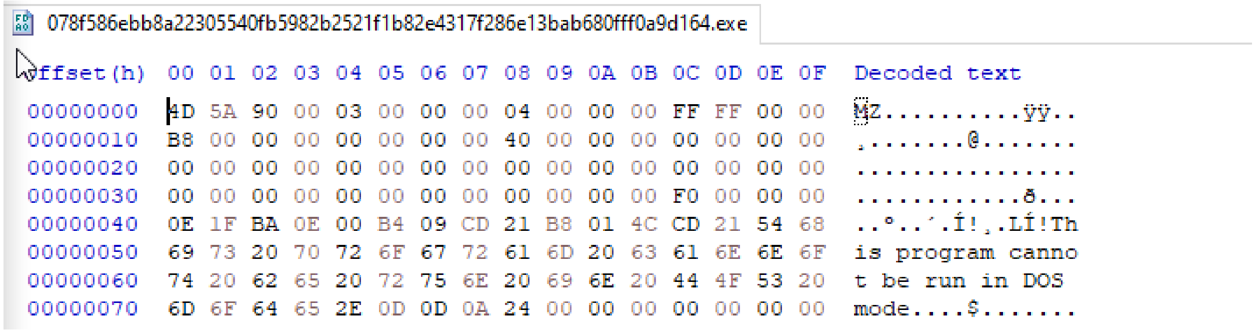
File preview:



078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164

Determine the file type:

File signature: exe

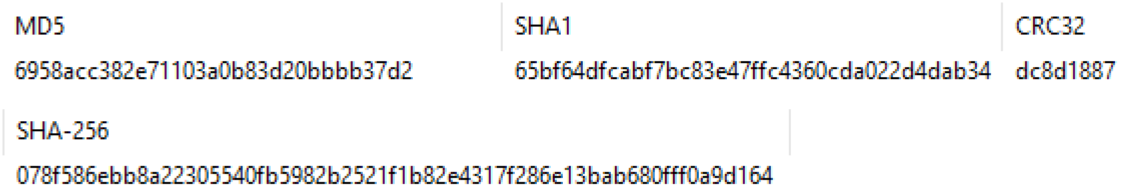


078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164.exe

```
Offset(h) 00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F  Decoded text

00000000  4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00  MZ..........ÿÿ..
00000010  B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00  ¸.......@.......
00000020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00000030  00 00 00 00 00 00 00 00 00 00 00 00 F0 00 00 00  ............ð...
00000040  0E 1F BA 0E 00 B4 09 CD 21 B8 01 4C CD 21 54 68  ..º..´.Í!¸.LÍ!Th
00000050  69 73 20 70 72 6F 67 72 61 6D 20 63 61 6E 6E 6F  is program canno
00000060  74 20 62 65 20 72 75 6E 20 69 6E 20 44 4F 53 20  t be run in DOS 
00000070  6D 6F 64 65 2E 0D 0D 0A 24 00 00 00 00 00 00 00  mode....$.......
```

Fingerprinting the malware:I was able to generate the hashes from the .exe file using the HashMyFiles Program.

The hash code in the name of the file is the SHA-256 hash code.

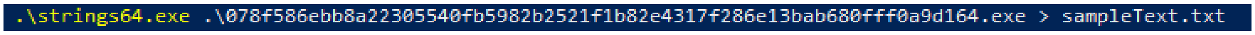


MD5	SHA1	CRC32
6958acc382e71103a0b83d20bbbb37d2	65bf64dfcabf7bc83e47ffc4360cda022d4dab34	dc8d1887

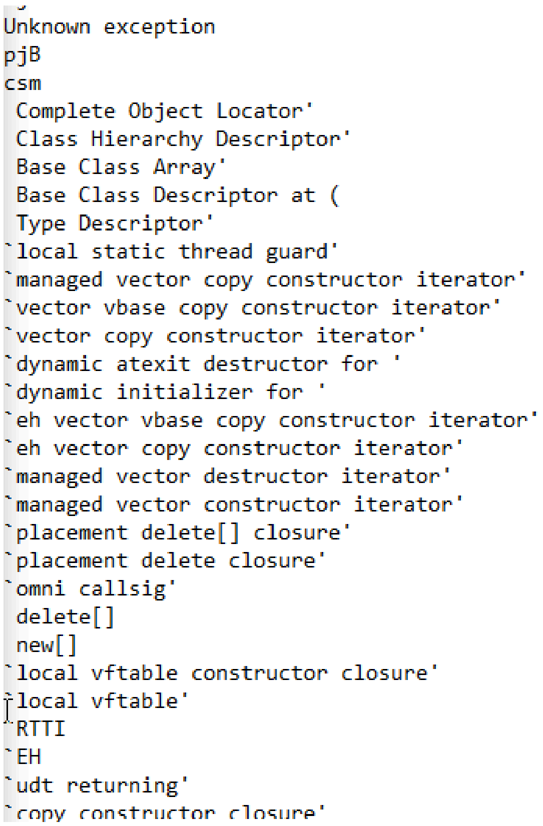
SHA-256
078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164

Extracting Strings:

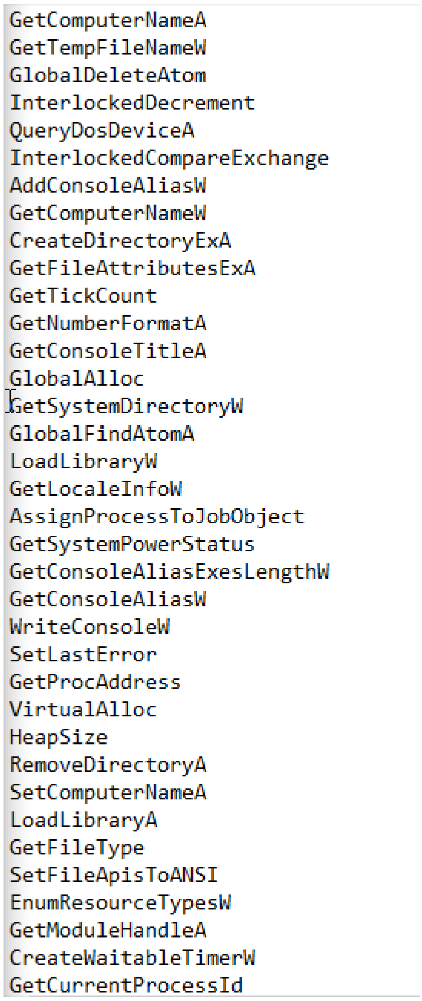
I used the Windows Strings64.exe analyzer to analyze the strings inside of the .exe file. I output the strings to a text file using Powershell.



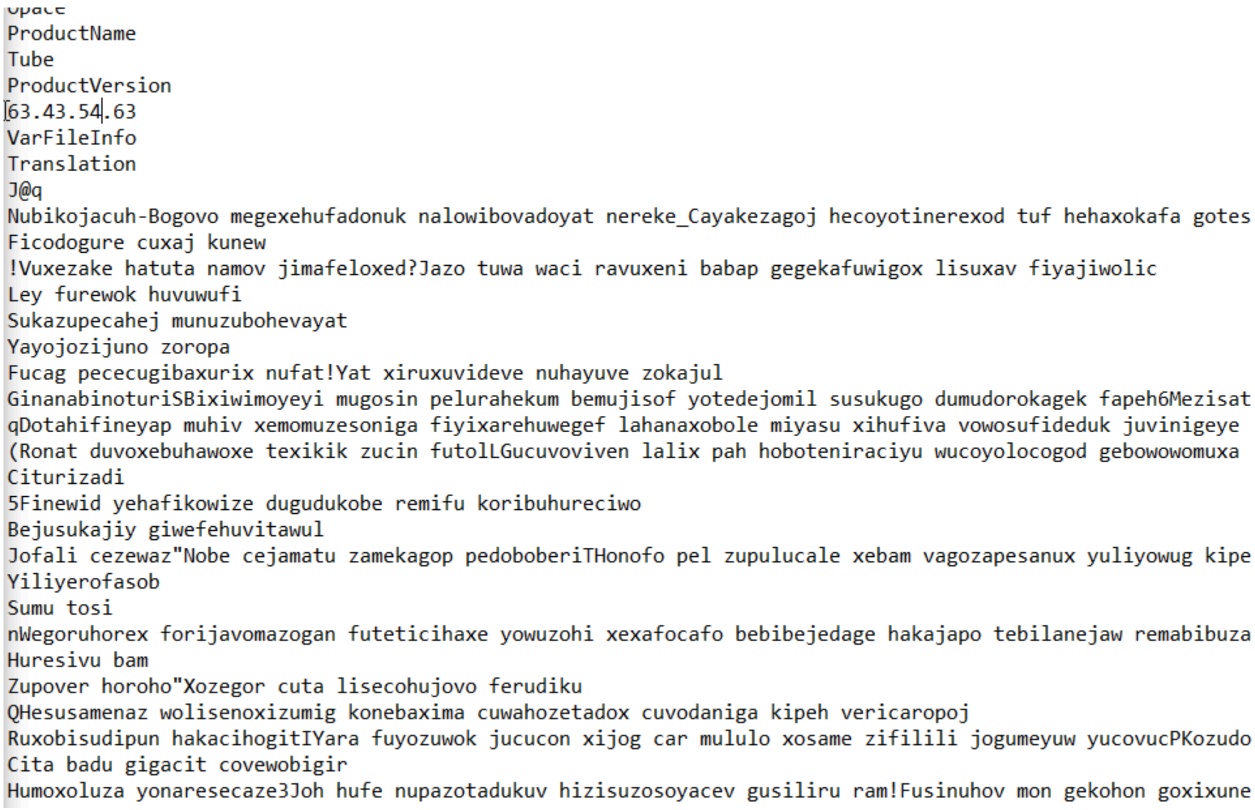
```
.\strings64.exe .\078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164.exe > sampleText.txt
```



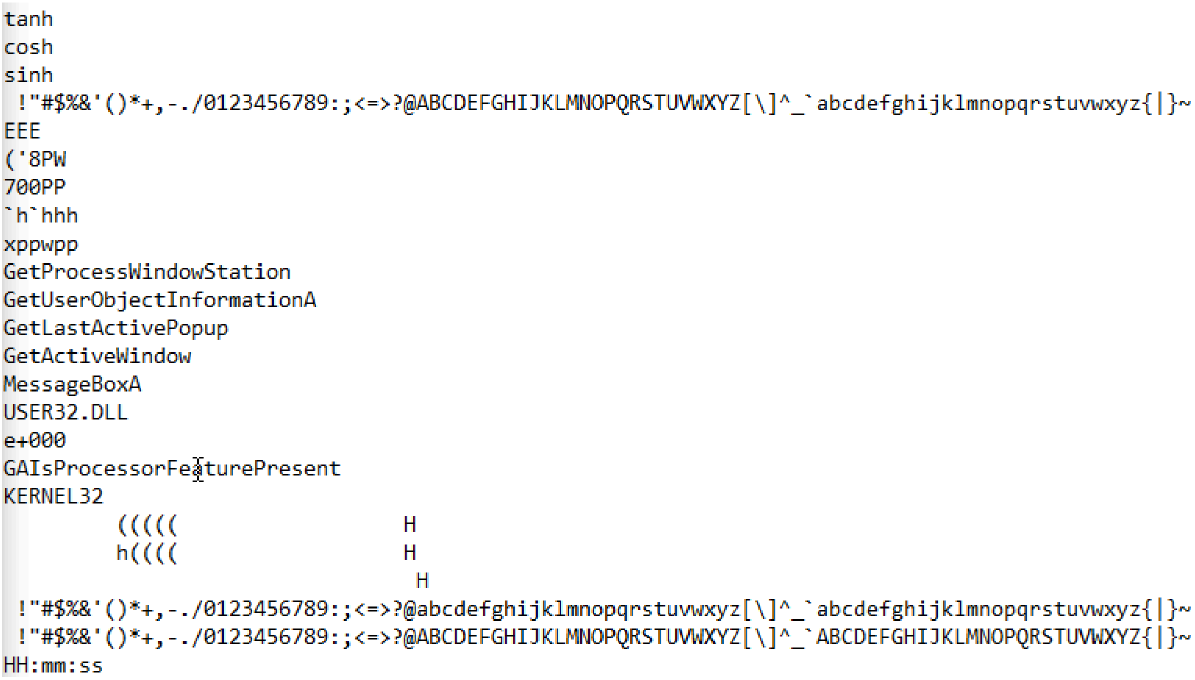
```
Unknown exception
pjB
csm
 Complete Object Locator'
 Class Hierarchy Descriptor'
 Base Class Array'
 Base Class Descriptor at (
 Type Descriptor'
`local static thread guard'
`managed vector copy constructor iterator'
`vector vbase copy constructor iterator'
`vector copy constructor iterator'
`dynamic atexit destructor for '
`dynamic initializer for '
`eh vector vbase copy constructor iterator'
`eh vector copy constructor iterator'
`managed vector destructor iterator'
`managed vector constructor iterator'
`placement delete[] closure'
`placement delete closure'
`omni callsig'
 delete[]
 new[]
`local vftable constructor closure'
`local vftable'
`RTTI
`EH
`udt returning'
`copy constructor closure'
```



```
GetComputerNameA
GetTempFileNameW
GlobalDeleteAtom
InterlockedDecrement
QueryDosDeviceA
InterlockedCompareExchange
AddConsoleAliasW
GetComputerNameW
CreateDirectoryExA
GetFileAttributesExA
GetTickCount
GetNumberFormatA
GetConsoleTitleA
GlobalAlloc
GetSystemDirectoryW
GlobalFindAtomA
LoadLibraryW
GetLocaleInfoW
AssignProcessToJobObject
GetSystemPowerStatus
GetConsoleAliasExesLengthW
GetConsoleAliasW
WriteConsoleW
SetLastError
GetProcAddress
VirtualAlloc
HeapSize
RemoveDirectoryA
SetComputerNameA
LoadLibraryA
GetFileType
SetFileApisToANSI
EnumResourceTypesW
GetModuleHandleA
CreateWaitableTimerW
GetCurrentProcessId
```

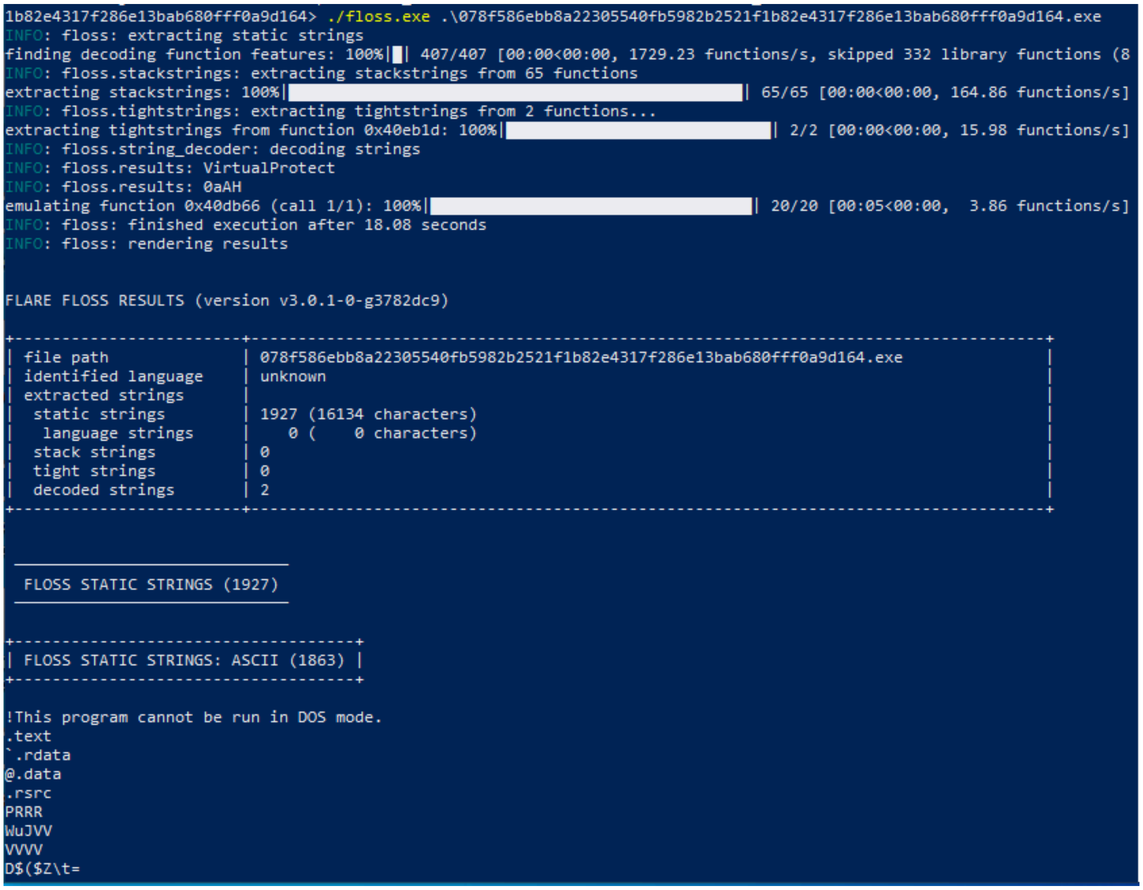


```
Space
ProductName
Tube
ProductVersion
63.43.54.63
VarFileInfo
Translation
J@q
Nubikojacuh-Bogovo megexehufadonuk nalowibovadoyat nereke_Cayakezagoj hecoyotinerexod tuf hehaxokafa gotes
Ficodogure cuxaj kunew
!Vuxezake hatuta namov jimafeloxed?Jazo tuwa waci ravuxeni babap gegekafuwigox lisuxav fiyajiwolic
Ley furewok huvuwufi
Sukazupecahej munuzubohevayat
Yayojozijuno zoropa
Fucag pececugibaxurix nufat!Yat xiruxuvideve nuhayuve zokajul
GinanabinoturiSBixiwimoyeyi mugosin pelurahekum bemujisof yotedejomil susukugo dumudorokagek fapeh6Mezisat
qDotahifineyap muhiv xemomuzesoniga fiyixarehuwegef lahanaxobole miyasu xihufiva vowosufideduk juvinigeye
(Ronat duvoxebuhawoxe texikik zucin futolLGucuvoviven lalix pah hoboteniraciyu wucoyolocogod gebowowomuxa
Citurizadi
5Finewid yehafikowize dugudukobe remifu koribuhureciwo
Bejusukajiy giwefehuvitawul
Jofali cezewaz"Nobe cejamatu zamekagop pedoboberiTHonofo pel zupulucale xebam vagozapesanux yuliyowug kipe
Yiliyerofasob
Sumu tosi
nWegoruhorex forijavomazogan futeticihaxe yowuzohi xexafocafo bebibejedage hakajapo tebilanejaw remabibuza
Huresivu bam
Zupover horoho"Xozegor cuta lisecohujovo ferudiku
QHesusamenaz wolisenoxizumig konebaxima cuwahozetadox cuvodaniga kipeh vericaropoj
Ruxobisudipun hakacihogitIYara fuyozuwok jucucon xijog car mululo xosame zifilili jogumeyuw yucovucPKozudo
Cita badu gigacit covewobigir
Humoxoluza yonaresecaze3Joh hufe nupazotadukuv hizisuzosoyacev gusiliru ram!Fusinuhov mon gekohon goxixune
```

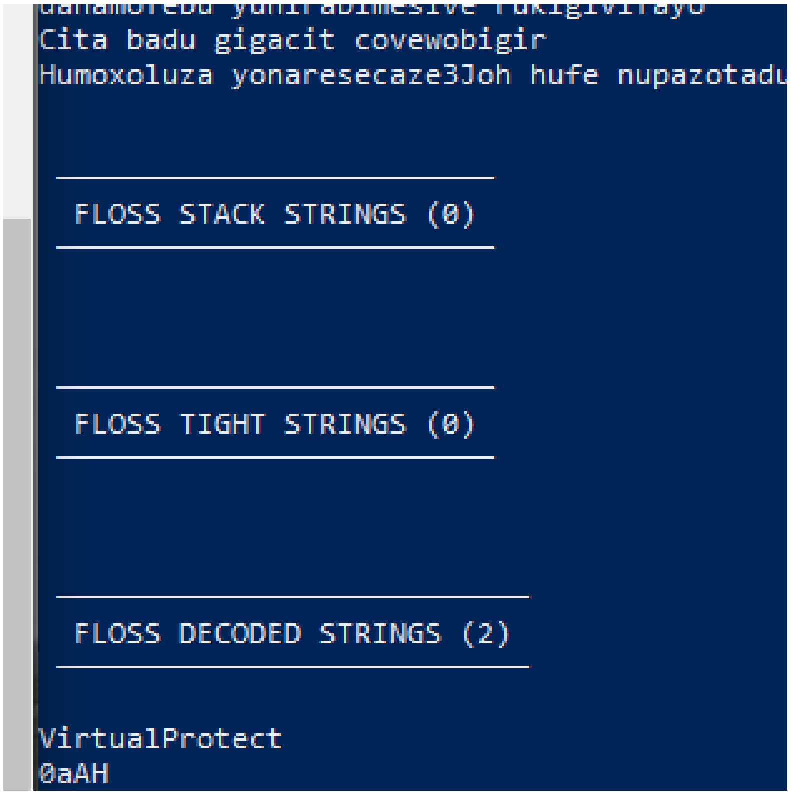


```
tanh
cosh
sinh
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
EEE
('8PW
700PP
`h`hhh
xppwpp
GetProcessWindowStation
GetUserObjectInformationA
GetLastActivePopup
GetActiveWindow
MessageBoxA
USER32.DLL
e+000
GAIsProcessorFeaturePresent
KERNEL32
         (((((                  H
         h((((                  H
                                 H
 !"#$%&'()*+,-./0123456789:;<=>?@abcdefghijklmnopqrstuvwxyz[\]^_`abcdefghijklmnopqrstuvwxyz{|}~
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`ABCDEFGHIJKLMNOPQRSTUVWXYZ{|}~
HH:mm:ss
```

FLOSS

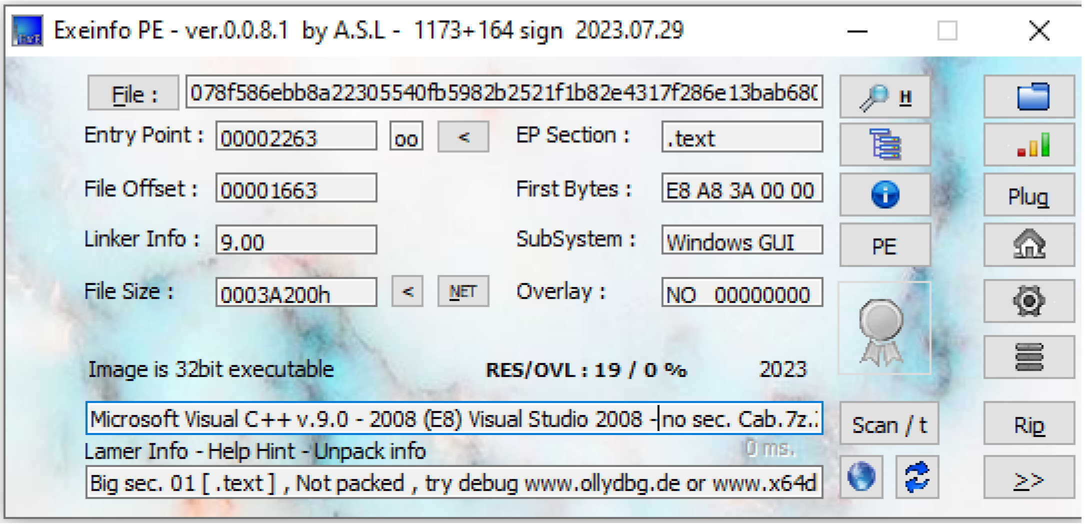


```
1b82e4317f286e13bab680fff0a9d164> ./floss.exe .\078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164.exe
INFO: floss: extracting static strings
finding decoding function features: 100%|█| 407/407 [00:00<00:00, 1729.23 functions/s, skipped 332 library functions (8
INFO: floss.stackstrings: extracting stackstrings from 65 functions
extracting stackstrings: 100%|████████████████████████████████████████| 65/65 [00:00<00:00, 164.86 functions/s]
INFO: floss.tightstrings: extracting tightstrings from 2 functions...
extracting tightstrings from function 0x40eb1d: 100%|███████████████████████| 2/2 [00:00<00:00, 15.98 functions/s]
INFO: floss.string_decoder: decoding strings
INFO: floss.results: VirtualProtect
INFO: floss.results: 0aAH
emulating function 0x40db66 (call 1/1): 100%|████████████████████████████| 20/20 [00:05<00:00,  3.86 functions/s]
INFO: floss: finished execution after 18.08 seconds
INFO: floss: rendering results


FLARE FLOSS RESULTS (version v3.0.1-0-g3782dc9)

+------------------------+------------------------------------------------------------------------------------+
| file path              | 078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164.exe               |
| identified language    | unknown                                                                            |
| extracted strings      |                                                                                    |
|  static strings        | 1927 (16134 characters)                                                            |
|   language strings     |    0 (    0 characters)                                                            |
|  stack strings         | 0                                                                                  |
|  tight strings         | 0                                                                                  |
|  decoded strings       | 2                                                                                  |
+------------------------+------------------------------------------------------------------------------------+


 ─────────────────────────────
  FLOSS STATIC STRINGS (1927)
 ─────────────────────────────

+-----------------------------------+
| FLOSS STATIC STRINGS: ASCII (1863) |
+-----------------------------------+

!This program cannot be run in DOS mode.
.text
`.rdata
@.data
.rsrc
PRRR
WuJVV
VVVV
D$($Z\t=
```



```
danamorebu yunirabimesive rukigivirayo
Cita badu gigacit covewobigir
Humoxoluza yonaresecaze3Joh hufe nupazotadu


 ─────────────────────────
  FLOSS STACK STRINGS (0)
 ─────────────────────────



 ─────────────────────────
  FLOSS TIGHT STRINGS (0)
 ─────────────────────────



 ───────────────────────────
  FLOSS DECODED STRINGS (2)
 ───────────────────────────


VirtualProtect
0aAH
```

Determining File obfuscation:
File is not obfuscated. We checked with ExeInfoPE.



Exeinfo PE - ver.0.0.8.1 by A.S.L - 1173+164 sign 2023.07.29

File : 078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab68

Entry Point : 00002263

EP Section : .text

File Offset : 00001663

First Bytes : E8 A8 3A 00 00

Linker Info : 9.00

SubSystem : Windows GUI

File Size : 0003A200h

Overlay : NO 00000000

Image is 32bit executable RES/OVL : 19 / 0 % 2023

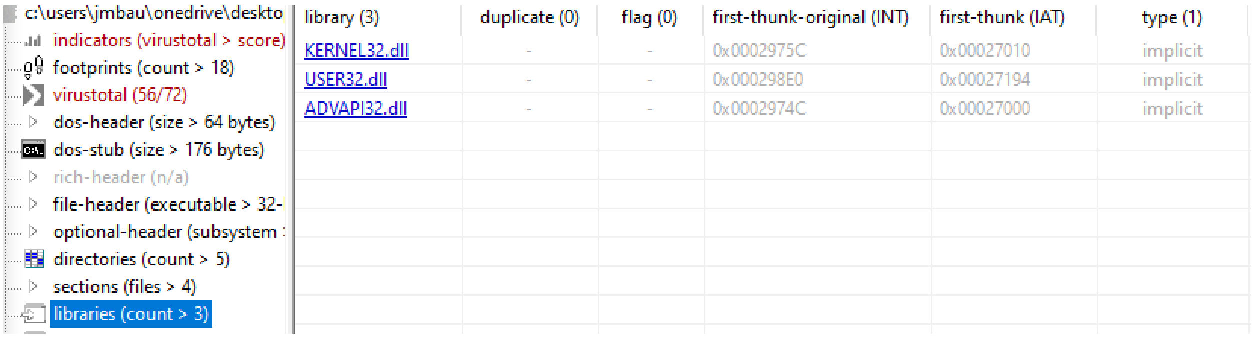
Microsoft Visual C++ v.9.0 - 2008 (E8) Visual Studio 2008 -|no sec. Cab.7z.:

Lamer Info - Help Hint - Unpack info 0 ms.

Big sec. 01 [.text] , Not packed , try debug www.ollydbg.de or www.x64d

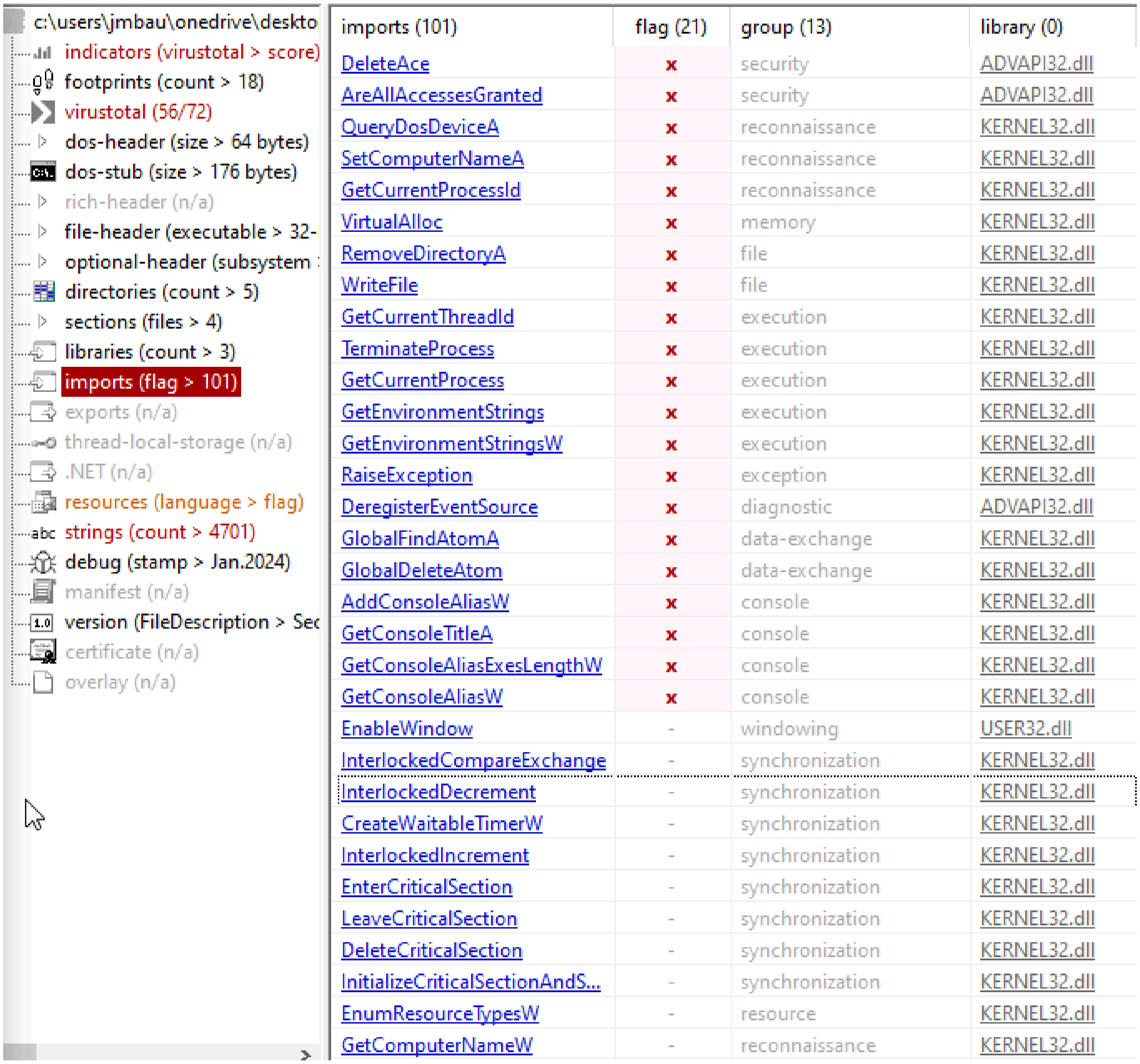
Inspecting PE header information:

Libraries:

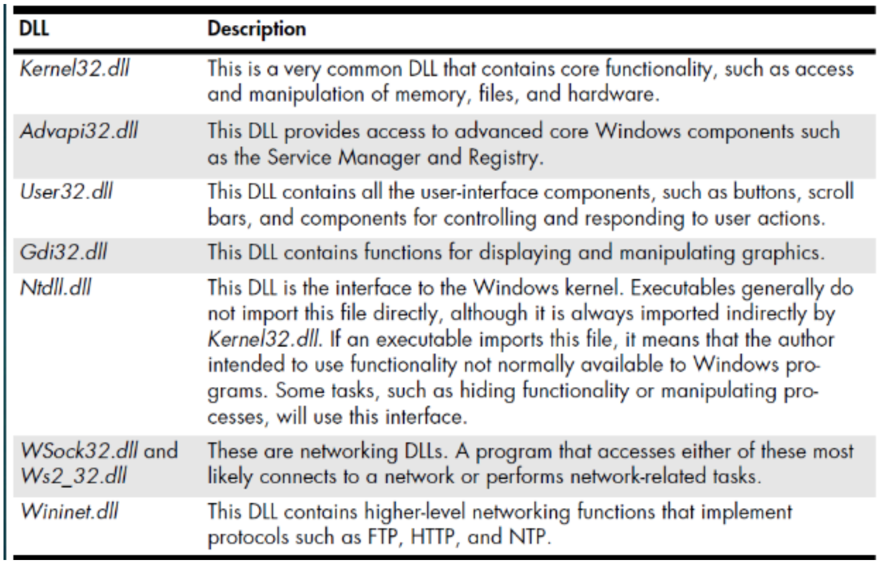

c:\users\jmbau\onedrive\deskto
indicators (virustotal > score)
footprints (count > 18)
virustotal (56/72)
dos-header (size > 64 bytes)
dos-stub (size > 176 bytes)
rich-header (n/a)
file-header (executable > 32-
optional-header (subsystem :
directories (count > 5)
sections (files > 4)
libraries (count > 3)

library (3)	duplicate (0)	flag (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)
KERNEL32.dll	-	-	0x0002975C	0x00027010	implicit
USER32.dll	-	-	0x000298E0	0x00027194	implicit
ADVAPI32.dll	-	-	0x0002974C	0x00027000	implicit

Imports:

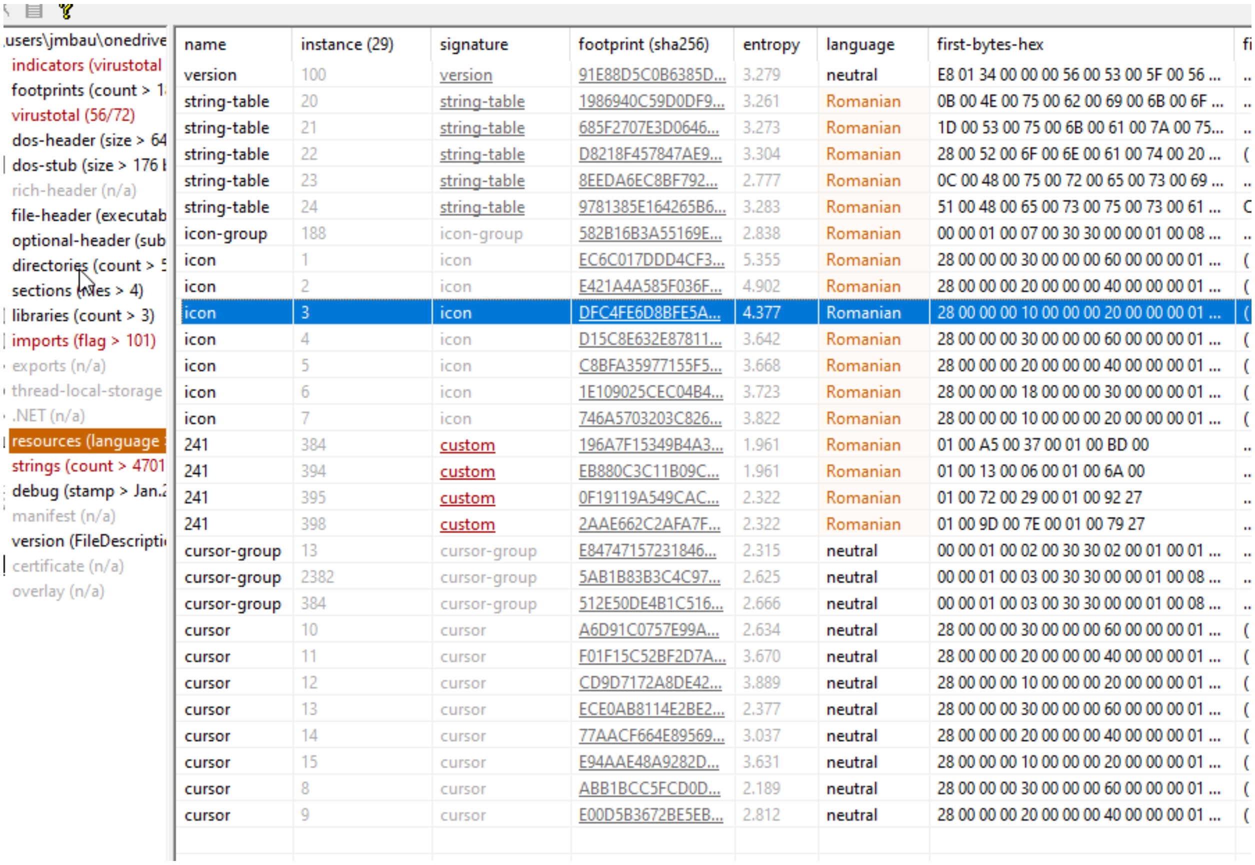

c:\users\jmbau\onedrive\deskto
indicators (virustotal > score)
footprints (count > 18)
virustotal (56/72)
dos-header (size > 64 bytes)
dos-stub (size > 176 bytes)
rich-header (n/a)
file-header (executable > 32-
optional-header (subsystem :
directories (count > 5)
sections (files > 4)
libraries (count > 3)
imports (flag > 101)
exports (n/a)
thread-local-storage (n/a)
.NET (n/a)
resources (language > flag)
strings (count > 4701)
debug (stamp > Jan.2024)
manifest (n/a)
version (FileDescription > Sec
certificate (n/a)
overlay (n/a)

imports (101)	flag (21)	group (13)	library (0)
DeleteAce	x	security	ADVAPI32.dll
AreAllAccessesGranted	x	security	ADVAPI32.dll
QueryDosDeviceA	x	reconnaissance	KERNEL32.dll
SetComputerNameA	x	reconnaissance	KERNEL32.dll
GetCurrentProcessId	x	reconnaissance	KERNEL32.dll
VirtualAlloc	x	memory	KERNEL32.dll
RemoveDirectoryA	x	file	KERNEL32.dll
WriteFile	x	file	KERNEL32.dll
GetCurrentThreadId	x	execution	KERNEL32.dll
TerminateProcess	x	execution	KERNEL32.dll
GetCurrentProcess	x	execution	KERNEL32.dll
GetEnvironmentStrings	x	execution	KERNEL32.dll
GetEnvironmentStringsW	x	execution	KERNEL32.dll
RaiseException	x	exception	KERNEL32.dll
DeregisterEventSource	x	diagnostic	ADVAPI32.dll
GlobalFindAtomA	x	data-exchange	KERNEL32.dll
GlobalDeleteAtom	x	data-exchange	KERNEL32.dll
AddConsoleAliasW	x	console	KERNEL32.dll
GetConsoleTitleA	x	console	KERNEL32.dll
GetConsoleAliasExesLengthW	x	console	KERNEL32.dll
GetConsoleAliasW	x	console	KERNEL32.dll
EnableWindow	-	windowing	USER32.dll
InterlockedCompareExchange	-	synchronization	KERNEL32.dll
InterlockedDecrement	-	synchronization	KERNEL32.dll
CreateWaitableTimerW	-	synchronization	KERNEL32.dll
InterlockedIncrement	-	synchronization	KERNEL32.dll
EnterCriticalSection	-	synchronization	KERNEL32.dll
LeaveCriticalSection	-	synchronization	KERNEL32.dll
DeleteCriticalSection	-	synchronization	KERNEL32.dll
InitializeCriticalSectionAndS...	-	synchronization	KERNEL32.dll
EnumResourceTypesW	-	resource	KERNEL32.dll
GetComputerNameW	-	reconnaissance	KERNEL32.dll



DLL	Description
Kernel32.dll	This is a very common DLL that contains core functionality, such as access and manipulation of memory, files, and hardware.
Advapi32.dll	This DLL provides access to advanced core Windows components such as the Service Manager and Registry.
User32.dll	This DLL contains all the user-interface components, such as buttons, scroll bars, and components for controlling and responding to user actions.
Gdi32.dll	This DLL contains functions for displaying and manipulating graphics.
Ntdll.dll	This DLL is the interface to the Windows kernel. Executables generally do not import this file directly, although it is always imported indirectly by *Kernel32.dll*. If an executable imports this file, it means that the author intended to use functionality not normally available to Windows programs. Some tasks, such as hiding functionality or manipulating processes, will use this interface.
WSock32.dll and *Ws2_32.dll*	These are networking DLLs. A program that accesses either of these most likely connects to a network or performs network-related tasks.
Wininet.dll	This DLL contains higher-level networking functions that implement protocols such as FTP, HTTP, and NTP.

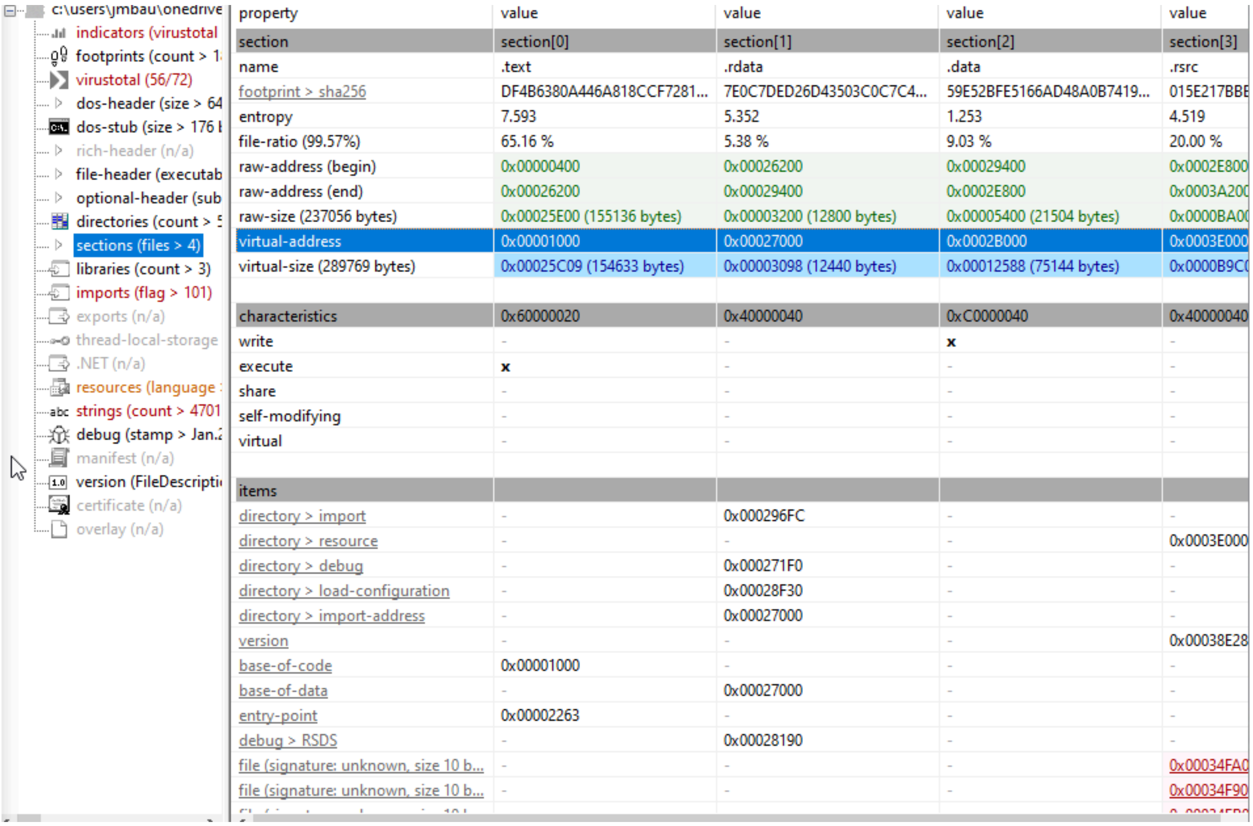
Language?



users\jmbau\onedrive
indicators (virustotal
footprints (count > 1
virustotal (56/72)
dos-header (size > 64
dos-stub (size > 176 I
rich-header (n/a)
file-header (executab
optional-header (sub
directories (count > 5
sections (files > 4)
libraries (count > 3)
imports (flag > 101)
exports (n/a)
thread-local-storage
.NET (n/a)
resources (language
strings (count > 4701
debug (stamp > Jan.2
manifest (n/a)
version (FileDescripti
certificate (n/a)
overlay (n/a)

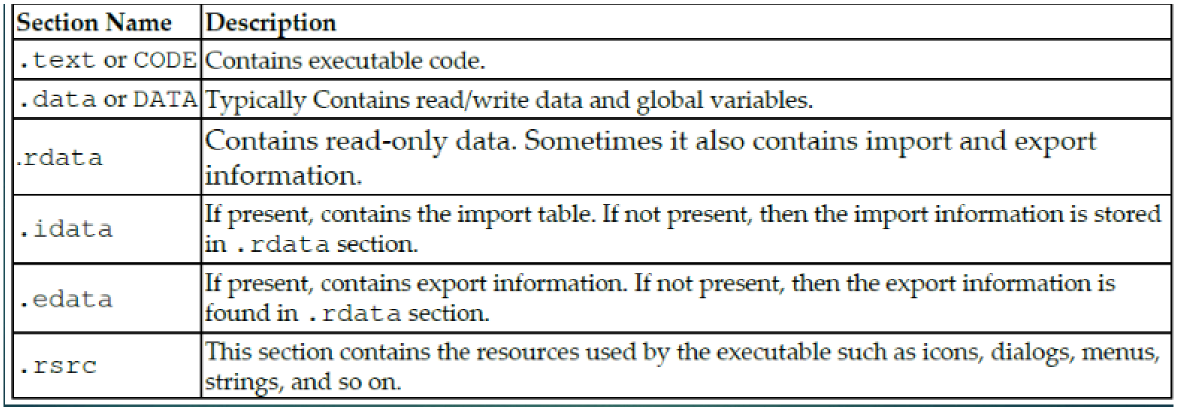
name	instance (29)	signature	footprint (sha256)	entropy	language	first-bytes-hex	fi
version	100	version	91E88D5C0B6385D...	3.279	neutral	E8 01 34 00 00 00 56 00 53 00 5F 00 56 ...	..
string-table	20	string-table	1986940C59D0DF9...	3.261	Romanian	0B 00 4E 00 75 00 62 00 69 00 6B 00 6F ...	..
string-table	21	string-table	685F2707E3D0646...	3.273	Romanian	1D 00 53 00 75 00 6B 00 61 00 7A 00 75...	..
string-table	22	string-table	D8218F457847AE9...	3.304	Romanian	28 00 52 00 6F 00 6E 00 61 00 74 00 20 ...	(
string-table	23	string-table	8EEDA6EC8BF792...	2.777	Romanian	0C 00 48 00 75 00 72 00 65 00 73 00 69 ...	..
string-table	24	string-table	9781385E164265B6...	3.283	Romanian	51 00 48 00 65 00 73 00 75 00 73 00 61 ...	C
icon-group	188	icon-group	582B16B3A55169E...	2.838	Romanian	00 00 01 00 07 00 30 30 00 00 01 00 08 ...	..
icon	1	icon	EC6C017DDD4CF3...	5.355	Romanian	28 00 00 00 30 00 00 00 60 00 00 00 01 ...	(
icon	2	icon	E421A4A585F036F...	4.902	Romanian	28 00 00 00 20 00 00 00 40 00 00 00 01 ...	(
icon	3	icon	DFC4FE6D8BFE5A...	4.377	Romanian	28 00 00 00 10 00 00 00 20 00 00 00 01 ...	(
icon	4	icon	D15C8E632E87811...	3.642	Romanian	28 00 00 00 30 00 00 00 60 00 00 00 01 ...	(
icon	5	icon	C8BFA35977155F5...	3.668	Romanian	28 00 00 00 20 00 00 00 40 00 00 00 01 ...	(
icon	6	icon	1E109025CEC04B4...	3.723	Romanian	28 00 00 00 18 00 00 00 30 00 00 00 01 ...	(
icon	7	icon	746A5703203C826...	3.822	Romanian	28 00 00 00 10 00 00 00 20 00 00 00 01 ...	(
241	384	custom	196A7F15349B4A3...	1.961	Romanian	01 00 A5 00 37 00 01 00 BD 00	..
241	394	custom	EB880C3C11B09C...	1.961	Romanian	01 00 13 00 06 00 01 00 6A 00	..
241	395	custom	0F19119A549CAC...	2.322	Romanian	01 00 72 00 29 00 01 00 92 27	..
241	398	custom	2AAE662C2AFA7F...	2.322	Romanian	01 00 9D 00 7E 00 01 00 79 27	..
cursor-group	13	cursor-group	E84747157231846...	2.315	neutral	00 00 01 00 02 00 30 30 02 00 01 00 01 ...	..
cursor-group	2382	cursor-group	5AB1B83B3C4C97...	2.625	neutral	00 00 01 00 03 00 30 30 00 00 01 00 08 ...	..
cursor-group	384	cursor-group	512E50DE4B1C516...	2.666	neutral	00 00 01 00 03 00 30 30 00 00 01 00 08 ...	..
cursor	10	cursor	A6D91C0757E99A...	2.634	neutral	28 00 00 00 30 00 00 00 60 00 00 00 01 ...	(
cursor	11	cursor	F01F15C52BF2D7A...	3.670	neutral	28 00 00 00 20 00 00 00 40 00 00 00 01 ...	(
cursor	12	cursor	CD9D7172A8DE42...	3.889	neutral	28 00 00 00 10 00 00 00 20 00 00 00 01 ...	(
cursor	13	cursor	ECE0AB8114E2BE2...	2.377	neutral	28 00 00 00 30 00 00 00 60 00 00 00 01 ...	(
cursor	14	cursor	77AACF664E89569...	3.037	neutral	28 00 00 00 20 00 00 00 40 00 00 00 01 ...	(
cursor	15	cursor	E94AAE48A9282D...	3.631	neutral	28 00 00 00 10 00 00 00 20 00 00 00 01 ...	(
cursor	8	cursor	ABB1BCC5FCD0D...	2.189	neutral	28 00 00 00 30 00 00 00 60 00 00 00 01 ...	(
cursor	9	cursor	E00D5B3672BE5EB...	2.812	neutral	28 00 00 00 20 00 00 00 40 00 00 00 01 ...	(

Sections:



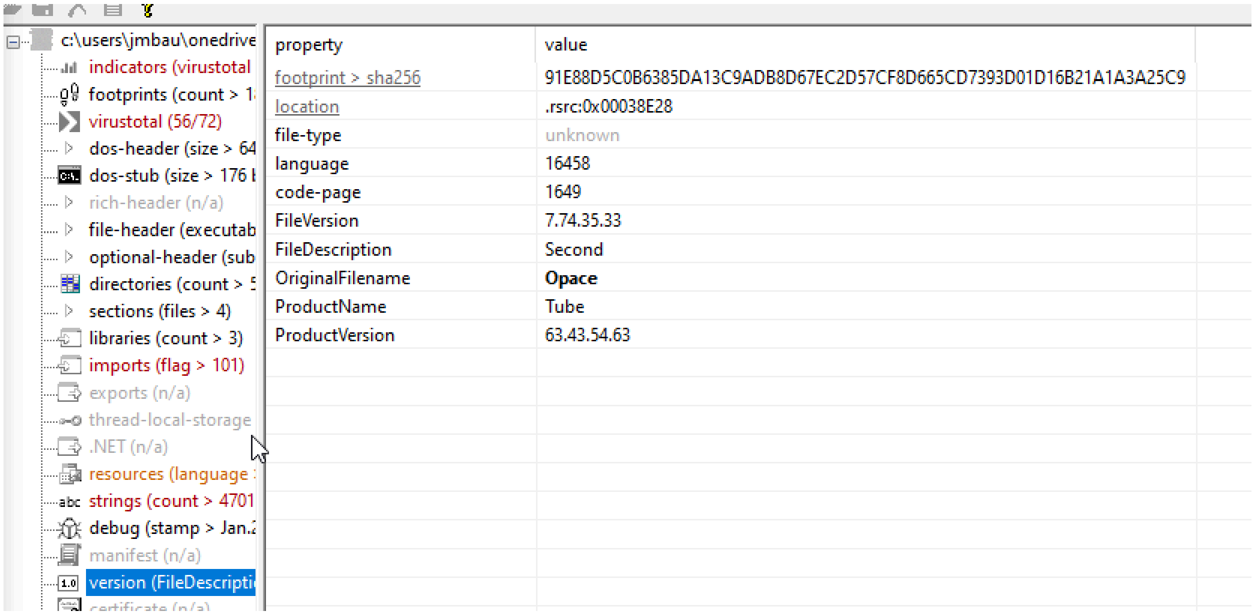
c:\users\jmbau\onedrive
- indicators (virustotal
- footprints (count > 1
- virustotal (56/72)
- dos-header (size > 64
- dos-stub (size > 176 l
- rich-header (n/a)
- file-header (executab
- optional-header (sub
- directories (count > 5
- sections (files > 4)
- libraries (count > 3)
- imports (flag > 101)
- exports (n/a)
- thread-local-storage
- .NET (n/a)
- resources (language
- strings (count > 4701
- debug (stamp > Jan.2
- manifest (n/a)
- version (FileDescripti
- certificate (n/a)
- overlay (n/a)

property	value	value	value	value
section	section[0]	section[1]	section[2]	section[3]
name	.text	.rdata	.data	.rsrc
footprint > sha256	DF4B6380A446A818CCF7281...	7E0C7DED26D43503C0C7C4...	59E52BFE5166AD48A0B7419...	015E217BBE
entropy	7.593	5.352	1.253	4.519
file-ratio (99.57%)	65.16 %	5.38 %	9.03 %	20.00 %
raw-address (begin)	0x00000400	0x00026200	0x00029400	0x0002E800
raw-address (end)	0x00026200	0x00029400	0x0002E800	0x0003A200
raw-size (237056 bytes)	0x00025E00 (155136 bytes)	0x00003200 (12800 bytes)	0x00005400 (21504 bytes)	0x0000BA00
virtual-address	0x00001000	0x00027000	0x0002B000	0x0003E000
virtual-size (289769 bytes)	0x00025C09 (154633 bytes)	0x00003098 (12440 bytes)	0x00012588 (75144 bytes)	0x0000B9C0
characteristics	0x60000020	0x40000040	0xC0000040	0x40000040
write	-	-	x	-
execute	x	-	-	-
share	-	-	-	-
self-modifying	-	-	-	-
virtual	-	-	-	-
items				
directory > import	-	0x000296FC	-	-
directory > resource	-	-	-	0x0003E000
directory > debug	-	0x000271F0	-	-
directory > load-configuration	-	0x00028F30	-	-
directory > import-address	-	0x00027000	-	-
version	-	-	-	0x00038E28
base-of-code	0x00001000	-	-	-
base-of-data	-	0x00027000	-	-
entry-point	0x00002263	-	-	-
debug > RSDS	-	0x00028190	-	-
file (signature: unknown, size 10 b...	-	-	-	0x00034FA0
file (signature: unknown, size 10 b...	-	-	-	0x00034F90



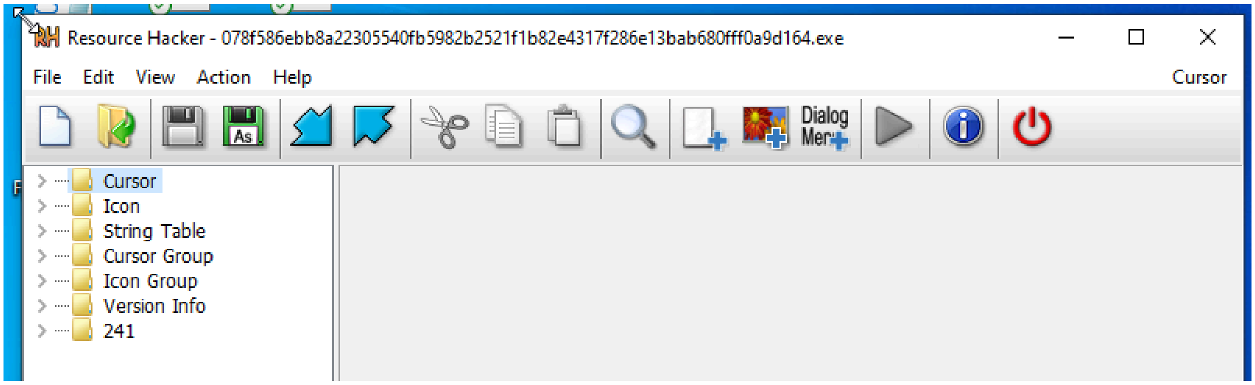
Section Name	Description
.text or CODE	Contains executable code.
.data or DATA	Typically Contains read/write data and global variables.
.rdata	Contains read-only data. Sometimes it also contains import and export information.
.idata	If present, contains the import table. If not present, then the import information is stored in .rdata section.
.edata	If present, contains export information. If not present, then the export information is found in .rdata section.
.rsrc	This section contains the resources used by the executable such as icons, dialogs, menus, strings, and so on.

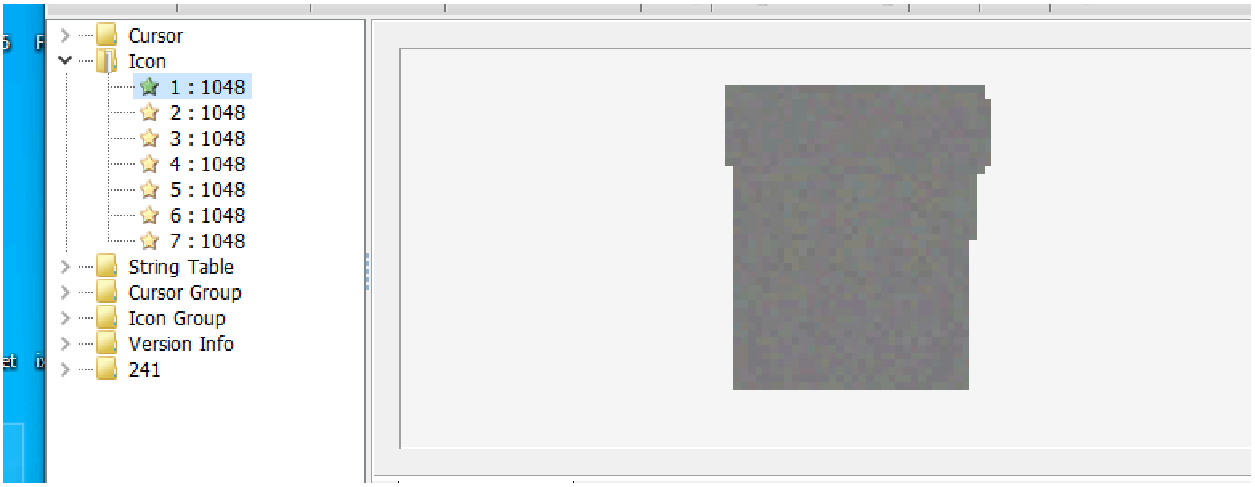
Filename:

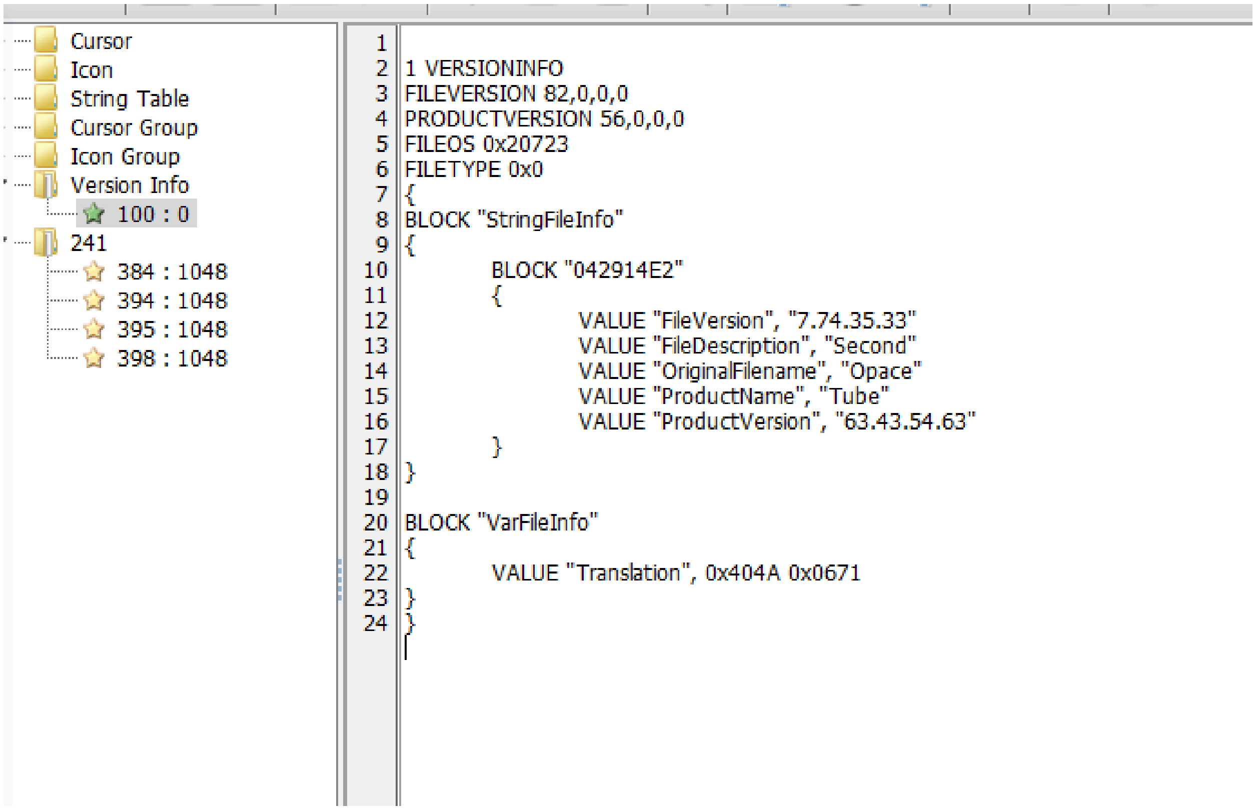


property	value
footprint > sha256	91E88D5C0B6385DA13C9ADB8D67EC2D57CF8D665CD7393D01D16B21A1A3A25C9
location	.rsrc:0x00038E28
file-type	unknown
language	16458
code-page	1649
FileVersion	7.74.35.33
FileDescription	Second
OriginalFilename	**Opace**
ProductName	Tube
ProductVersion	63.43.54.63

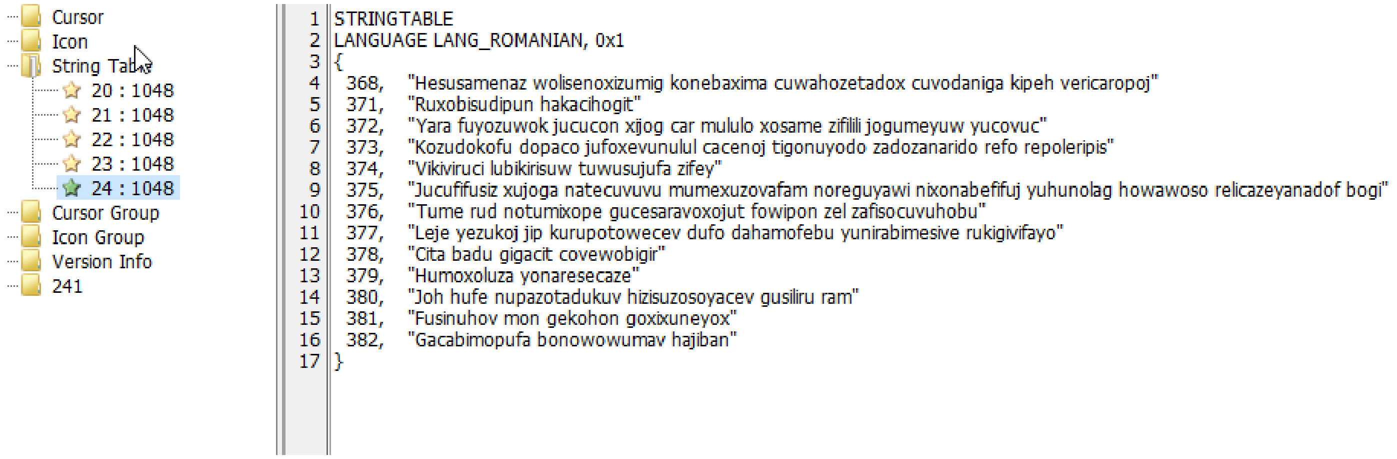
Recourse Hacker:


Resource Hacker - 078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164.exe





```

1 VERSIONINFO
FILEVERSION 82,0,0,0
PRODUCTVERSION 56,0,0,0
FILEOS 0x20723
FILETYPE 0x0
{
BLOCK "StringFileInfo"
{
	BLOCK "042914E2"
	{
		VALUE "FileVersion", "7.74.35.33"
		VALUE "FileDescription", "Second"
		VALUE "OriginalFilename", "Opace"
		VALUE "ProductName", "Tube"
		VALUE "ProductVersion", "63.43.54.63"
	}
}

BLOCK "VarFileInfo"
{
	VALUE "Translation", 0x404A 0x0671
}
}
```



```
STRINGTABLE
LANGUAGE LANG_ROMANIAN, 0x1
{
  368,    "Hesusamenaz wolisenoxizumig konebaxima cuwahozetadox cuvodaniga kipeh vericaropoj"
  371,    "Ruxobisudipun hakacihogit"
  372,    "Yara fuyozuwok jucucon xijog car mululo xosame zifilili jogumeyuw yucovuc"
  373,    "Kozudokofu dopaco jufoxevunulul cacenoj tigonuyodo zadozanarido refo repoleripis"
  374,    "Vikiviruci lubikirisuw tuwusujufa zifey"
  375,    "Jucufifusiz xujoga natecuvuvu mumexuzovafam noreguyawi nixonabefifuj yuhunolag howawoso relicazeyanadof bogi"
  376,    "Tume rud notumixope gucesaravoxojut fowipon zel zafisocuvuhobu"
  377,    "Leje yezukoj jip kurupotowecev dufo dahamofebu yunirabimesive rukigivifayo"
  378,    "Cita badu gigacit covewobigir"
  379,    "Humoxoluza yonaresecaze"
  380,    "Joh hufe nupazotadukuv hizisuzosoyacev gusiliru ram"
  381,    "Fusinuhov mon gekohon goxixuneyox"
  382,    "Gacabimopufa bonowowumav hajiban"
}
```

imphash, YARA, control flow graphs, opcodes

Compare and classify malware

DYNAMIC ANALYSIS