



# Malware Analysis

James Baumhardt, Brendon Werner, Ben Saunders, Brendan Kinder

# Static Analysis

File Preview:

 078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164 

# File Signature: exe

FD 078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164.exe

[illegible]

# 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
```

# Results of Extracting Strings:

```
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'
```

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

# Continued:

```
OpacE
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 fiyajiwoolic
Ley furewok huvuwufi
Sukazupecahej munuzubohevayat
Yayojozijuno zoropa
Fucag pececugibaxurix nufat!Yat xiruxuvideve nuhayuve zokajul
GinanabinoturiSBixiwimoyeyi mugosin pelurahekum bemujisof yotedejomil susukugo dumudorokagek fapeh6Mezizat
qDotahifineyap muhiv xemomuzesoniga fiyixarehuwegef lahanaxobole miyasu xihufiva vovosufideduk juvinigeye
(Ronat duvoxebuhawoxe texikik zucin futollGucuvoviven lalix pah hoboteniraciyu wucoyolocogod gebowowomuxa
Citurizadi
5Finewid yehafikowize dugudukobe remifu koribuhureciwo
Bejusukajiyi giwefehuvitawul
Jofali cezewaz"Nobe cejamatu zamekagop pedoboberiTonofo pel zupulucal 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 jucucun xijog car mululo xosame zifilili jogumeyuw yucovucPKozudo
Cita badu gigacit covewobigir
Humoxoluza yonaresecaze3Joh hufe nupazotadukuv hizisuzosoyacev gusiliru ram!Fusinuho mon gekohon goxixune
```

```
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
```



# Strings with 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
WuJV
VVVV
D$(Z\t=
```

## FLOSS STACK STRINGS (0)

## FLOSS TIGHT STRINGS (0)

## FLOSS DECODED STRINGS (2)

VirtualProtect  
0aAH



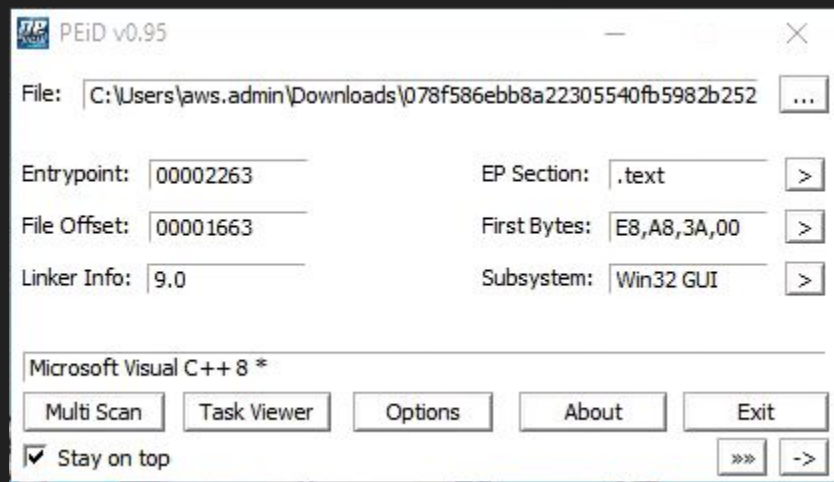
# Determining File obfuscation:

File is not obfuscated. We checked with ExeInfoPE.



# PEiD

We can confirm the same information using PEiD.



# Inspecting PE header information:

c:\users\jmbau\onedrive\desкто	library (3)	duplicate (0)	flag (0)	first-thunk-original (INT)	first-thunk (IAT)	type (1)
indicators (virustotal > score)	<a href="#">KERNEL32.dll</a>	-	-	0x0002975C	0x00027010	implicit
footprints (count > 18)	<a href="#">USER32.dll</a>	-	-	0x000298E0	0x00027194	implicit
virustotal (56/72)	<a href="#">ADVAPI32.dll</a>	-	-	0x0002974C	0x00027000	implicit
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)						

# PE Header Continued:

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

c:\users\jmbau\onedrive\deskte	imports (101)	flag (21)	group (13)	library (0)
indicators (virustotal > score)	<a href="#">DeleteAce</a>	x	security	ADVAPI32.dll
footprints (count > 18)	<a href="#">AreAllAccessesGranted</a>	x	security	ADVAPI32.dll
virustotal (56/72)	<a href="#">QueryDosDeviceA</a>	x	reconnaissance	KERNEL32.dll
dos-header (size > 64 bytes)	<a href="#">SetComputerNameA</a>	x	reconnaissance	KERNEL32.dll
dos-stub (size > 176 bytes)	<a href="#">GetCurrentProcessId</a>	x	reconnaissance	KERNEL32.dll
rich-header (n/a)	<a href="#">VirtualAlloc</a>	x	memory	KERNEL32.dll
file-header (executable > 32-	<a href="#">RemoveDirectoryA</a>	x	file	KERNEL32.dll
optional-header (subsystem :	<a href="#">WriteFile</a>	x	file	KERNEL32.dll
directories (count > 5)	<a href="#">GetCurrentThreadId</a>	x	execution	KERNEL32.dll
sections (files > 4)	<a href="#">TerminateProcess</a>	x	execution	KERNEL32.dll
libraries (count > 3)	<a href="#">GetCurrentProcess</a>	x	execution	KERNEL32.dll
imports (flag > 101)	<a href="#">GetEnvironmentStrings</a>	x	execution	KERNEL32.dll
exports (n/a)	<a href="#">GetEnvironmentStringsW</a>	x	execution	KERNEL32.dll
thread-local-storage (n/a)	<a href="#">RaiseException</a>	x	exception	KERNEL32.dll
.NET (n/a)	<a href="#">DeregisterEventSource</a>	x	diagnostic	ADVAPI32.dll
resources (language > flag)	<a href="#">GlobalFindAtomA</a>	x	data-exchange	KERNEL32.dll
strings (count > 4701)	<a href="#">GlobalDeleteAtom</a>	x	data-exchange	KERNEL32.dll
debug (stamp > Jan.2024)	<a href="#">AddConsoleAliasW</a>	x	console	KERNEL32.dll
manifest (n/a)	<a href="#">GetConsoleTitleA</a>	x	console	KERNEL32.dll
version (FileDescription > Sec	<a href="#">GetConsoleAliasExesLengthW</a>	x	console	KERNEL32.dll
certificate (n/a)	<a href="#">GetConsoleAliasW</a>	x	console	KERNEL32.dll
overlay (n/a)	<a href="#">EnableWindow</a>	-	windowing	USER32.dll
	<a href="#">InterlockedCompareExchange</a>	-	synchronization	KERNEL32.dll
	<a href="#">InterlockedDecrement</a>	-	synchronization	KERNEL32.dll
	<a href="#">CreateWaitableTimerW</a>	-	synchronization	KERNEL32.dll
	<a href="#">InterlockedIncrement</a>	-	synchronization	KERNEL32.dll
	<a href="#">EnterCriticalSection</a>	-	synchronization	KERNEL32.dll
	<a href="#">LeaveCriticalSection</a>	-	synchronization	KERNEL32.dll
	<a href="#">DeleteCriticalSection</a>	-	synchronization	KERNEL32.dll
	<a href="#">InitializeCriticalSectionAndS...</a>	-	synchronization	KERNEL32.dll
	<a href="#">EnumResourceTypesW</a>	-	resource	KERNEL32.dll
	<a href="#">GetComputerNameW</a>	-	reconnaissance	KERNEL32.dll

# Imphash

PEStudio:

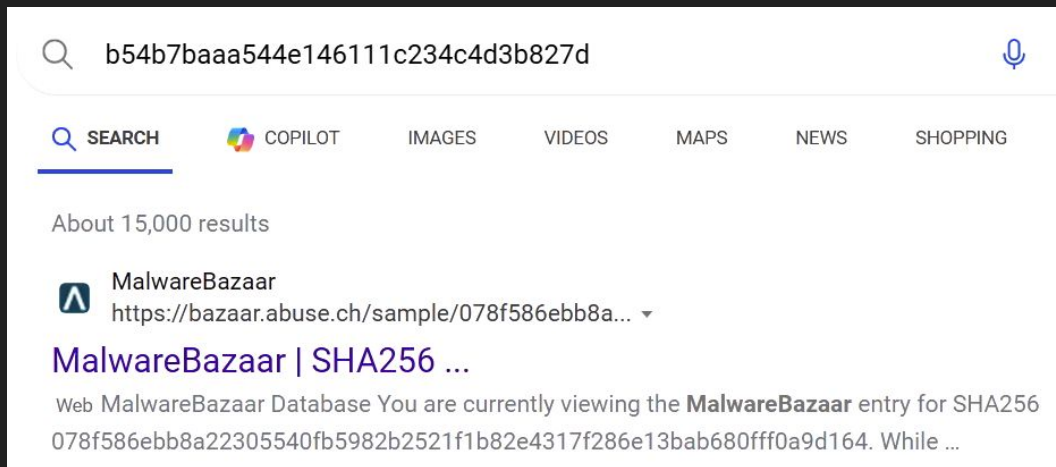
special	
<u>imphash &gt; md5</u>	<u><a href="#">B54B7BAAA544E146111C234C4D3B827D</a></u>

VirusTotal:

Imphash	b54b7baaa544e146111c234c4d3b827d
---------	----------------------------------

# Imphash 2

Found on Malware Bazaar:



SHA256 hash:

 078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164

imphash 

 b54b7baaa544e146111c234c4d3b827d (1 x RedLineStealer)



# Sections:

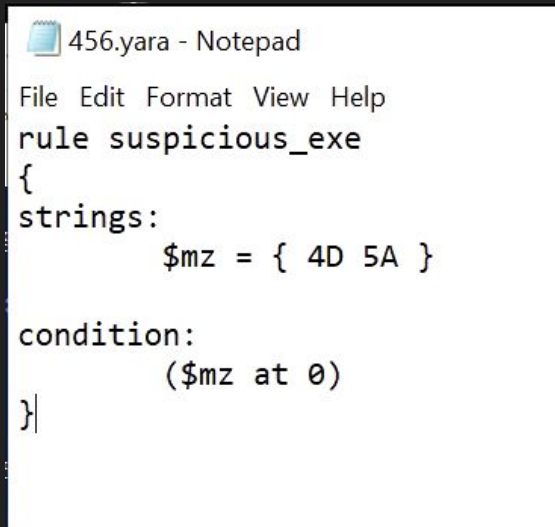
	property	value	value	value	value
	section	section[0]	section[1]	section[2]	section[3]
	name	.text	.rdata	.data	.rsrc
	footprint > sha256	DF4B6380A446A818CCF7281...	7E0C7DED26D43503C0C7C4...	59E52BFE5166AD48A0B7419...	015E217BBE...
	entropy	7.593	5.352	1.253	4.519
	file-ratio (99.57%)	65.16 %	5.38 %	9.03 %	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	-	-	-	-

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.

	0x000296FC	-	-
	-	-	0x0003E000
	0x000271F0	-	-
	0x00028F30	-	-
	0x00027000	-	-
	-	-	0x00038E28
	-	-	-
	0x00027000	-	-
	-	-	-
	0x00028190	-	-
	-	-	0x00034FA0
	-	-	0x00034F90
	-	-	0x00034F80



# YARA



```
456.yara - Notepad
File Edit Format View Help
rule suspicious_exe
{
strings:
    $mz = { 4D 5A }

condition:
    ($mz at 0)
}
```

```
PS C:\Users\aws.admin\Documents > yara -r 456.yara C:\Users\aws.admin\Downloads\Malware
suspicious_exe C:\Users\aws.admin\Downloads\Malware\078f586ebb8a22305540fb5982b2521f1b82e4317f286e13bab680fff0a9d164.exe
FLARE-VM 02/26/2024 15:30:08
```

# Filename:

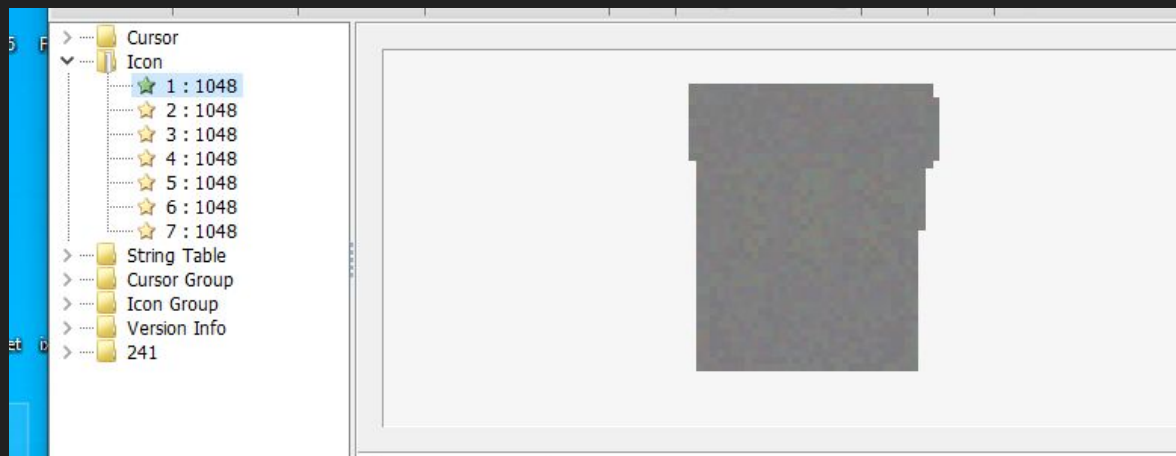
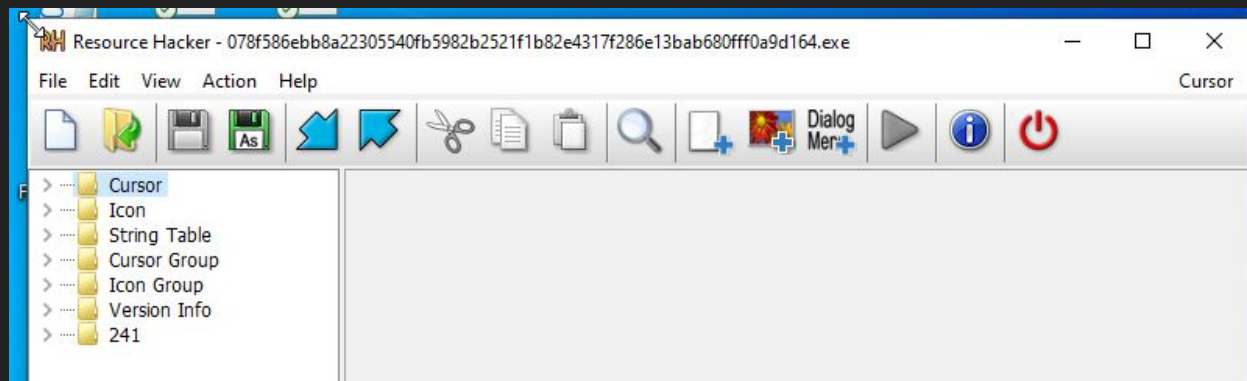
The screenshot displays the Windows File Explorer interface. The left sidebar shows the file's location at 'C:\Users\jmbau\onedrive' and a list of file properties. The right pane shows the details for the selected 'version' property, including the file version '7.74.35.33', file description 'Second', original filename 'Opace', product name 'Tube', and product version '63.43.54.63'.

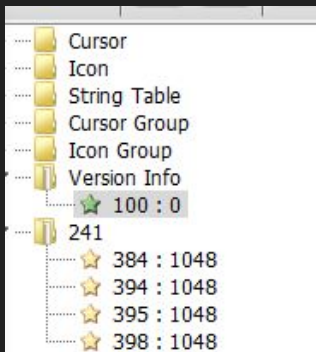
property	value
footprint > sha256	91E88D5C0B6385DA13C9ADB8D67EC2D57CF8D665CD7393D01D16B21A1A3A25C9
location	.rsrc:0x00038E28
file-type	unknown
language	16458
code-page	1649
FileVersion	7.74.35.33
FileDescription	Second
OriginalFilename	Opace
ProductName	Tube
ProductVersion	63.43.54.63

# Language?

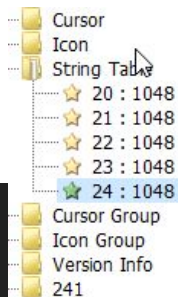
users\jmbau\onedrive	name	instance (29)	signature	footprint (sha256)	entropy	language	first-bytes-hex	f
indicators (virustotal	version	100	version	91E88D5C0B6385D...	3.279	neutral	E8 01 34 00 00 00 56 00 53 00 5F 00 56 ...	...
footprints (count > 1	string-table	20	string-table	1986940C59D0DDF9...	3.261	Romanian	08 00 4E 00 75 00 62 00 69 00 6B 00 6F ...	...
virustotal (56/72)	string-table	21	string-table	685F2707E3D0646...	3.273	Romanian	1D 00 53 00 75 00 6B 00 61 00 7A 00 75...	...
dos-header (size > 64	string-table	22	string-table	D8218F457847AE9...	3.304	Romanian	28 00 52 00 6F 00 6E 00 61 00 74 00 20 ...	(
dos-stub (size > 176	string-table	23	string-table	8EEDA6EC8BF792...	2.777	Romanian	0C 00 48 00 75 00 72 00 65 00 73 00 69 ...	...
rich-header (n/a)	string-table	24	string-table	9781385E164265B6...	3.283	Romanian	51 00 48 00 65 00 73 00 75 00 73 00 61 ...	C
file-header (executab	icon-group	188	icon-group	582B16B3A55169E...	2.838	Romanian	00 00 01 00 07 00 30 30 00 00 01 00 08 ...	...
optional-header (sub	icon	1	icon	EC6C017DDD4CF3...	5.355	Romanian	28 00 00 00 30 00 00 00 60 00 00 00 01 ...	(
directories (count > 5	icon	2	icon	E421A4A585F036F...	4.902	Romanian	28 00 00 00 20 00 00 00 40 00 00 00 01 ...	(
sections (files > 4)	icon	3	icon	DFC4FE6D8BFE5A...	4.377	Romanian	28 00 00 00 10 00 00 00 20 00 00 00 01 ...	(
libraries (count > 3)	icon	4	icon	D15C8E632E87811...	3.642	Romanian	28 00 00 00 30 00 00 00 60 00 00 00 01 ...	(
imports (flag > 101)	icon	5	icon	C8BFA35977155F5...	3.668	Romanian	28 00 00 00 20 00 00 00 40 00 00 00 01 ...	(
exports (n/a)	icon	6	icon	1E109025CEC04B4...	3.723	Romanian	28 00 00 00 18 00 00 00 30 00 00 00 01 ...	(
thread-local-storage	icon	7	icon	746A5703203C826...	3.822	Romanian	28 00 00 00 10 00 00 00 20 00 00 00 01 ...	(
.NET (n/a)	241	384	custom	196A7F15349B4A3...	1.961	Romanian	01 00 A5 00 37 00 01 00 BD 00	...
resources (language	241	394	custom	EB880C3C11B09C...	1.961	Romanian	01 00 13 00 06 00 01 00 6A 00	...
strings (count > 4701	241	395	custom	0F19119A549CAC...	2.322	Romanian	01 00 72 00 29 00 01 00 92 27	...
debug (stamp > Jan.2	241	398	custom	2AAE662C2AFA7F...	2.322	Romanian	01 00 9D 00 7E 00 01 00 79 27	...
manifest (n/a)	cursor-group	13	cursor-group	E84747157231846...	2.315	neutral	00 00 01 00 02 00 30 30 02 00 01 00 01 ...	...
version (FileDescripti	cursor-group	2382	cursor-group	5AB1B83B3C4C97...	2.625	neutral	00 00 01 00 03 00 30 30 00 00 01 00 08 ...	...
certificate (n/a)	cursor-group	384	cursor-group	512E50DE4B1C516...	2.666	neutral	00 00 01 00 03 00 30 30 00 00 01 00 08 ...	...
overlay (n/a)	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 ...	(

# Resource Hacker:





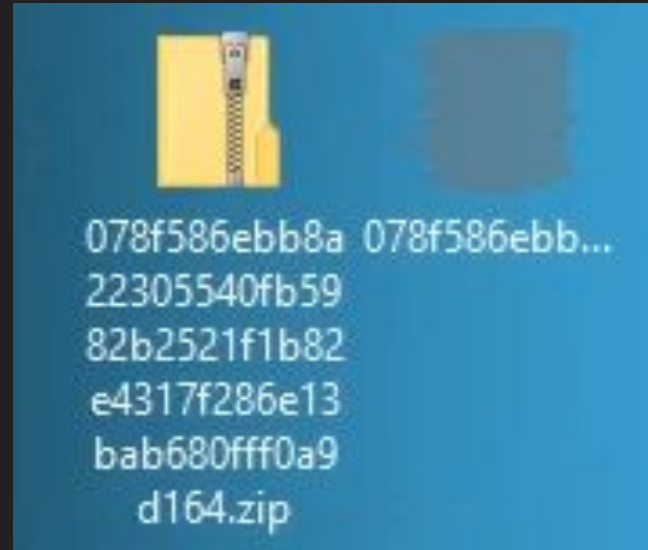
```
1
2 1 VERSIONINFO
3 FILEVERSION 82,0,0,0
4 PRODUCTVERSION 56,0,0,0
5 FILEOS 0x20723
6 FILETYPE 0x0
7 {
8 BLOCK "StringFileInfo"
9 {
10     BLOCK "042914E2"
11     {
12         VALUE "FileVersion", "7.74.35.33"
13         VALUE "FileDescription", "Second"
14         VALUE "OriginalFilename", "Opace"
15         VALUE "ProductName", "Tube"
16         VALUE "ProductVersion", "63.43.54.63"
17     }
18 }
19
20 BLOCK "VarFileInfo"
21 {
22     VALUE "Translation", 0x404A 0x0671
23 }
24 }
```



```
1 STRINGTABLE
2 LANGUAGE LANG_ROMANIAN, 0x1
3 {
4     368, "Hesusamenaz wolisenoxizumig konebaxima cuwahozetadox cuvodaniga kipeh vericaropoj"
5     371, "Ruxobisudipun hakachogit"
6     372, "Yara fuyoziwok jucucon xijog car mululo xosame zifili jogumeyuw yucovuc"
7     373, "Kozudokofu dopaco jufoxevunulul cacenoj tigonuyodo zadozanarido refo repoleripis"
8     374, "Vikiviruci lubikirisuw tuwusujufa zifey"
9     375, "Jucuffisuz xujoga natecuvuvu mumexuzovafam noreguyawi nixonabeffij yuhunolag howawoso relicazeyanadof bogi"
10    376, "Tume rud notumixope gucesaravoxojut fowipon zel zafisocuvuhobu"
11    377, "Leje yezukoj jip kurupotowecev dufo dahamofebu yunirabimesive rukigivifayo"
12    378, "Cita badu gigacit covewobigir"
13    379, "Humoxoluza yonaresecaze"
14    380, "Joh hufe nupazotadukuv hizisuzosoyacev gusiliru ram"
15    381, "Fusinhov mon gekohon goxixuneyox"
16    382, "Gacabimopufa bonowowumav hajiban"
17 }
```

# Dynamic Analysis:

I was able to unzip file and this is is the icon  
On the file.

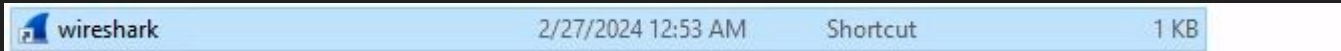


# Dynamic Analysis

I opened Wireshark before opening the malware.

The second I opened the file, my wireshark crashed and a bunch of alerts went off.

I still am not able to open wireshark. I'm not sure if the file is corrupt or not but I can't open it.






This screenshot shows that the file was modified today (the date at the time was 2/27/24)



# Dynamic

After opening the malware, I checked to see if other files were modified. I found these 3 files that were created on the drive.

The 2 “.sys” files are very large in size which raises an issue.

 DumpStack.log.tmp	2/27/2024 12:21 AM	TMP File	8 KB
 pagefile.sys	2/27/2024 12:21 AM	System file	1,310,720 KB
 swapfile.sys	2/27/2024 12:21 AM	System file	262,144 KB

I wasn't able to open a lot of the files on flare. My whole computer basically broke down and didn't work.

I believe some files were restricted access, i'm not sure if it was due to it being on a VM or if it was due to the malware.

Ran IDA for the file and these were  
The import files.

These are some of the files that  
Stood out to me.

Address	Ordin.	Name	Library
004270AC		GetStartupInfoA	KERNEL32
004270B0		GetModuleHandleW	KERNEL32
004270B4		TlsGetValue	KERNEL32
004270B8		TlsAlloc	KERNEL32
004270BC		TlsSetValue	KERNEL32
004270C0		TlsFree	KERNEL32
004270C4		InterlockedIncrement	KERNEL32
004270C8		GetCurrentThreadId	KERNEL32
004270CC		GetLastError	KERNEL32
004270D0		Sleep	KERNEL32
004270D4		ExitProcess	KERNEL32
004270D8		TerminateProcess	KERNEL32
004270DC		GetCurrentProcess	KERNEL32
004270E0		UnhandledExceptionFilter	KERNEL32
004270E4		SetUnhandledExceptionFilter	KERNEL32
004270E8		IsDebuggerPresent	KERNEL32
004270EC		EnterCriticalSection	KERNEL32
004270F0		LeaveCriticalSection	KERNEL32
004270F4		SetHandleCount	KERNEL32
004270F8		GetStdHandle	KERNEL32
004270FC		DeleteCriticalSection	KERNEL32
00427100		HeapFree	KERNEL32
00427104		SetFilePointer	KERNEL32
00427108		WriteFile	KERNEL32
0042710C		GetModuleFileNameA	KERNEL32
00427110		FreeEnvironmentStringsA	KERNEL32
00427114		GetEnvironmentStrings	KERNEL32
00427118		FreeEnvironmentStringsW	KERNEL32
0042711C		WideCharToMultiByte	KERNEL32
00427120		GetEnvironmentStringsW	KERNEL32
00427124		HeapCreate	KERNEL32
00427128		VirtualFree	KERNEL32
0042712C		QueryPerformanceCounter	KERNEL32
00427130		GetSystemTimeAsFileTime	KERNEL32
00427134		RaiseException	KERNEL32
00427138		GetCPInfo	KERNEL32
0042713C		GetACP	KERNEL32
00427140		GetOEMCP	KERNEL32
00427144		IsValidCodePage	KERNEL32
00427148		HeapAlloc	KERNEL32
0042714C		HeapReAlloc	KERNEL32
00427150		InitializeCriticalSectionAndSpinCount	KERNEL32
00427154		RtlUnwind	KERNEL32
00427158		ReadFile	KERNEL32
0042715C		SetStdHandle	KERNEL32
00427160		GetLocaleInfoA	KERNEL32
00427164		GetStringTypeA	KERNEL32
00427168		MultiByteToWideChar	KERNEL32
0042716C		GetStringTypeW	KERNEL32
00427170		LCMapStringA	KERNEL32
00427174		LCMapStringW	KERNEL32
00427178		GetConsoleCP	KERNEL32
0042717C		GetConsoleMode	KERNEL32
00427180		FlushFileBuffers	KERNEL32
00427184		WriteConsoleA	KERNEL32
00427188		GetConsoleOutputCP	KERNEL32
0042718C		CloseHandle	KERNEL32
00427194		EnableWindow	USER32
00427198		CharUpperBuffW	USER32

# Classify Malware:

Virus total:

56  
172

Community Score

56 security vendors and 3 sandboxes flagged this file as malicious

078f586ebb8a22305540fb5982b2521fb82e4317f286e13bab680fff0a9d164  
078f586ebb8a22305540fb5982b2521fb82e4317f286e13bab680fff0a9d164.exe

Size  
232.50 KB

Last Analysis Date  
3 days ago

EXE

peexe

spreader

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 7

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label trojan.ransomx/redline

Threat categories trojan ransomware

Family labels ransomx redline smokeloader

Security vendors' analysis ⓘ

Do you want to automate checks?

AhnLab-V3	! Trojan.Win.Generic.R635593	Alibaba	! Trojan:Win32/Redline.cee38f8d
ALYac	! Trojan.GenericKDZ.105667	Antiy-AVL	! Trojan/Win32.Kryptik
Arcabit	! Trojan.Generic.D19CC3	Avast	! Win32:RansomX-gen [Ransom]
AVG	! Win32:RansomX-gen [Ransom]	Avira (no cloud)	! TR/Crypt.Agent.vdwgl
BitDefender	! Trojan.GenericKDZ.105667	BitDefenderTheta	! Gen:NN.ZexaF.36744.oq0@aizFfnfG
Bkav Pro	! W32.AIDetectMalware	ClamAV	! Win.Packer.pkr_ce1a-9980177-0