

## STATIC ANALYSIS

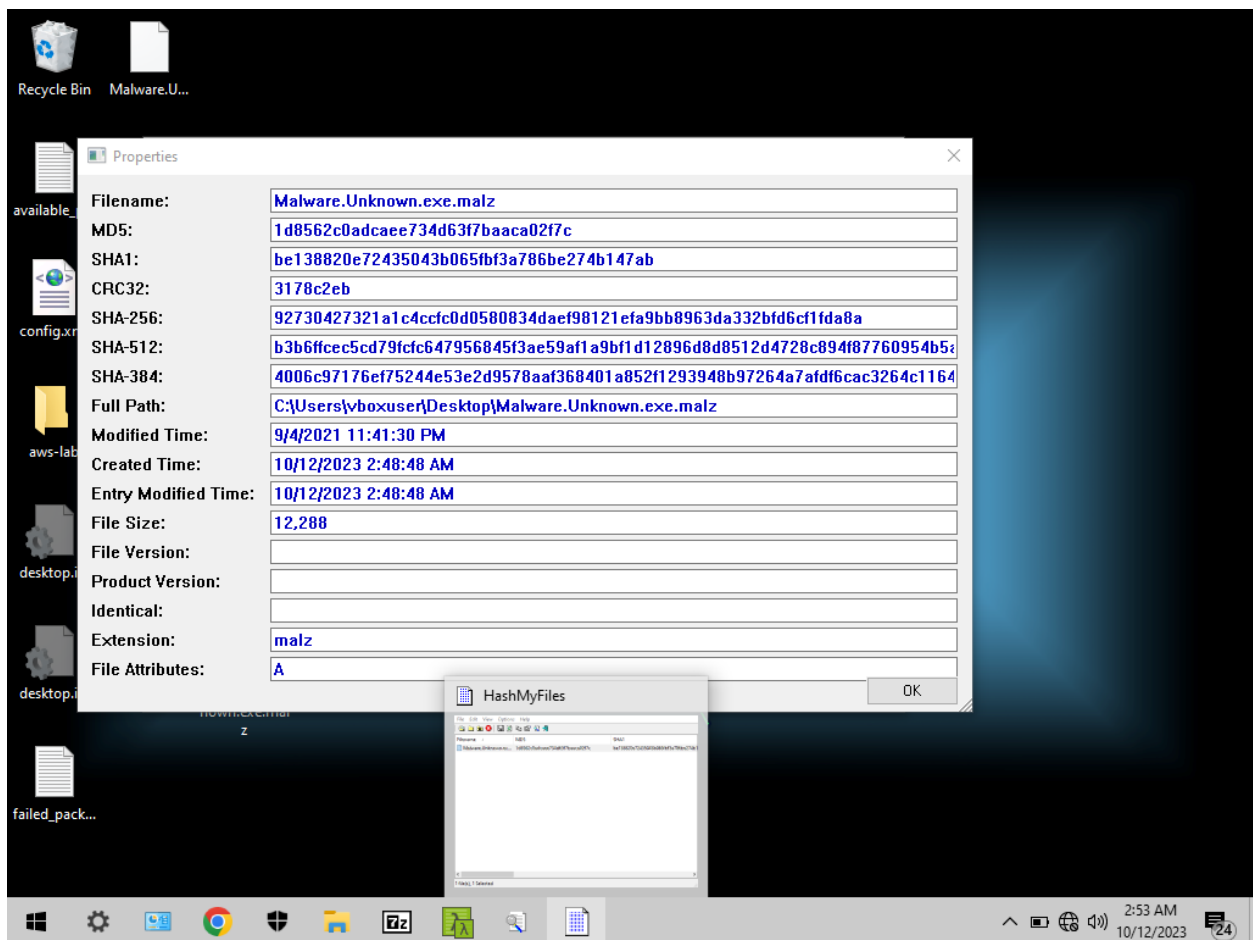
### Hashes Analysis:

Right click on the malware file and select HashMyFiles option and analyze the hash.

Copy the MD5 hash and run it on VirusTotal to know whether it is already been seen somewhere before.

### Important:

- SHA-256
- MD5

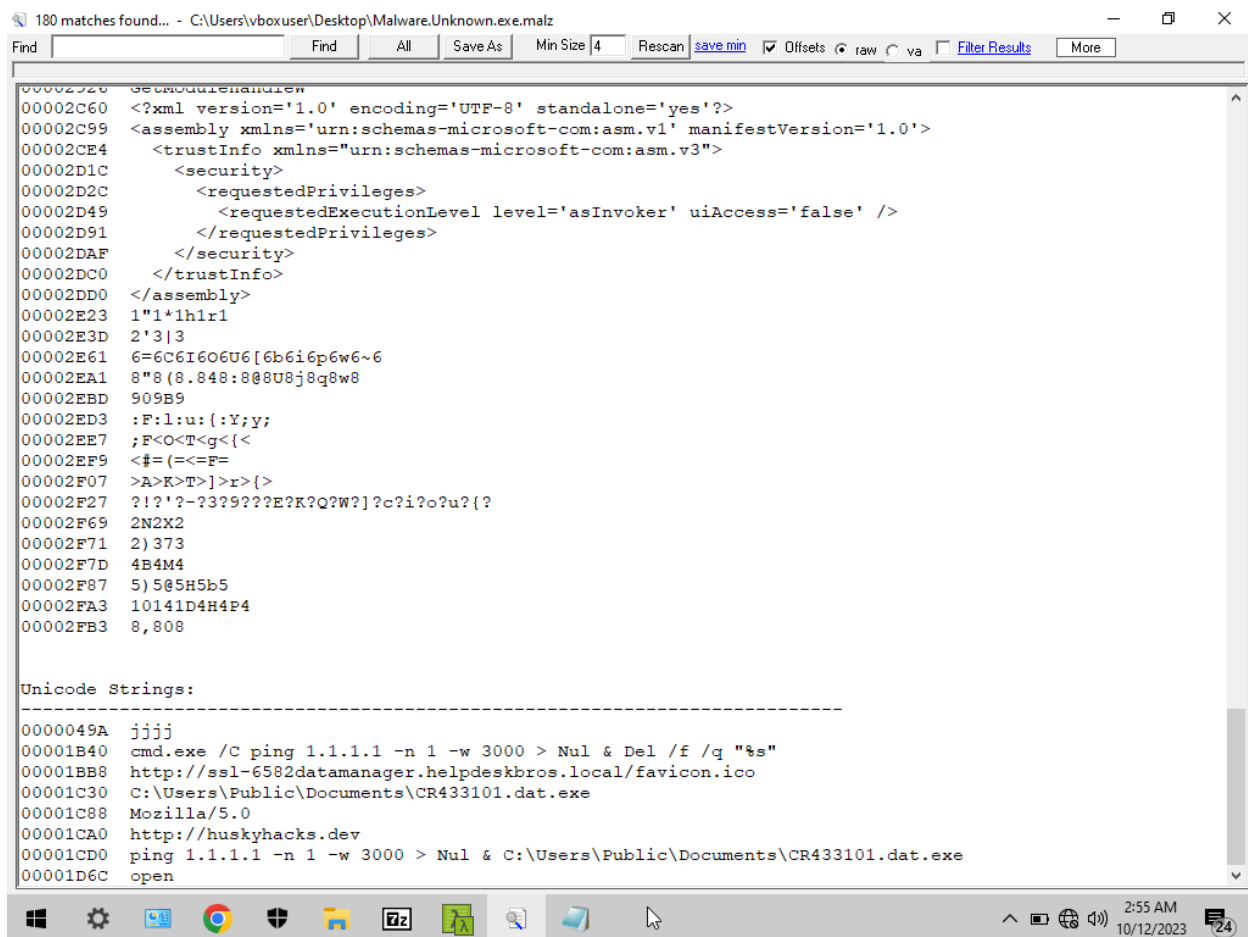


## String Analysis:

In simple language, a string is an array of characters.

Right click on the file and select strings. The list of strings will be visible look for evident strings that could help in analysis.

At the end, we get static unicode strings these are sometimes some of the most telling strings out of all.



```
180 matches found... - C:\Users\vboxuser\Desktop\Malware.Unknown.exe.malz
Find [ ] Find All Save As Min Size 4 Rescan save min Offsets raw va Filter Results More

00002920 GetModuleHandle
00002C60 <?xml version='1.0' encoding='UTF-8' standalone='yes'?>
00002C99 <assembly xmlns='urn:schemas-microsoft-com:asm.v1' manifestVersion='1.0'>
00002CE4 <trustInfo xmlns="urn:schemas-microsoft-com:asm.v3">
00002D1C <security>
00002D2C <requestedPrivileges>
00002D49 <requestedExecutionLevel level='asInvoker' uiAccess='false' />
00002D91 </requestedPrivileges>
00002DAF </security>
00002DC0 </trustInfo>
00002DD0 </assembly>
00002E23 1"1*1h1r1
00002E3D 2'3|3
00002E61 6=6C6I6O6U6[6b6i6p6w6~6
00002EA1 8"8 (8.848:8@8U8j8q8w8
00002EBD 909B9
00002ED3 :F:l:u:{:Y;y;
00002EE7 ;F<O<T<g<{<
00002EF9 <#=(=<F=
00002F07 >A>K>T>]>r>{>
00002F27 ?!'?'-?3?9???E?K?Q?W?]?c?i?o?u?{?
00002F69 2N2X2
00002F71 2)373
00002F7D 4B4M4
00002F87 5)5@5H5b5
00002FA3 10141D4H4F4
00002FB3 8,808

Unicode Strings:
-----
0000049A jjjj
00001B40 cmd.exe /C ping 1.1.1.1 -n 1 -w 3000 > Nul & Del /f /q "%s"
00001BB8 http://ssl-6582datamanager.helpdeskbro.local/favicon.ico
00001C30 C:\Users\Public\Documents\CR433101.dat.exe
00001C88 Mozilla/5.0
00001CA0 http://huskyhacks.dev
00001CD0 ping 1.1.1.1 -n 1 -w 3000 > Nul & C:\Users\Public\Documents\CR433101.dat.exe
00001D6C open
```

PEview:

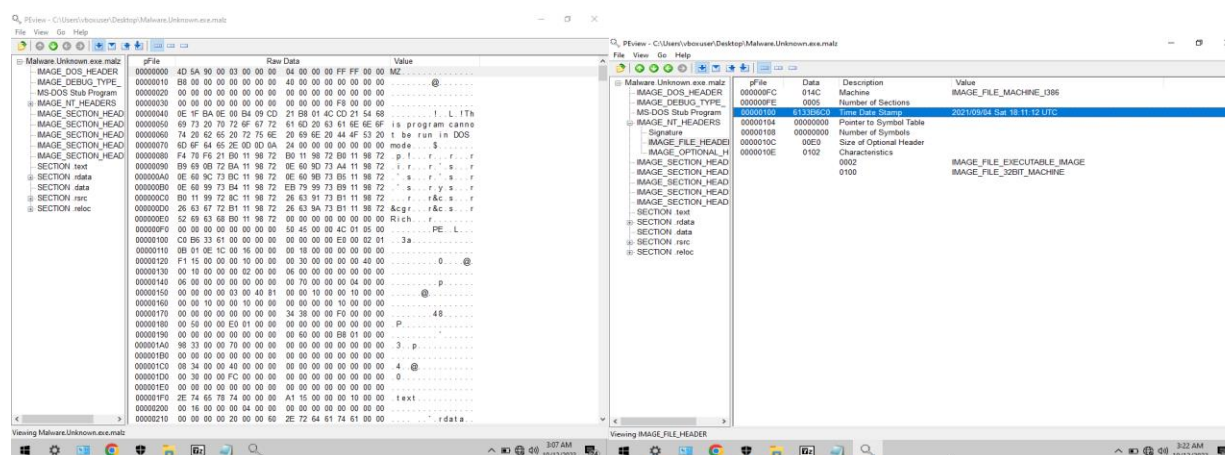
Now we will continue our analysis through PEView.

Open PEView and open the malware file. PEView gives us the idea of how a portable executable will look like.

Select IMAGE\_TIME\_HEADER in IMAGE\_NT\_HEADERS, you could see various details related to file such as Time Date Stamp.

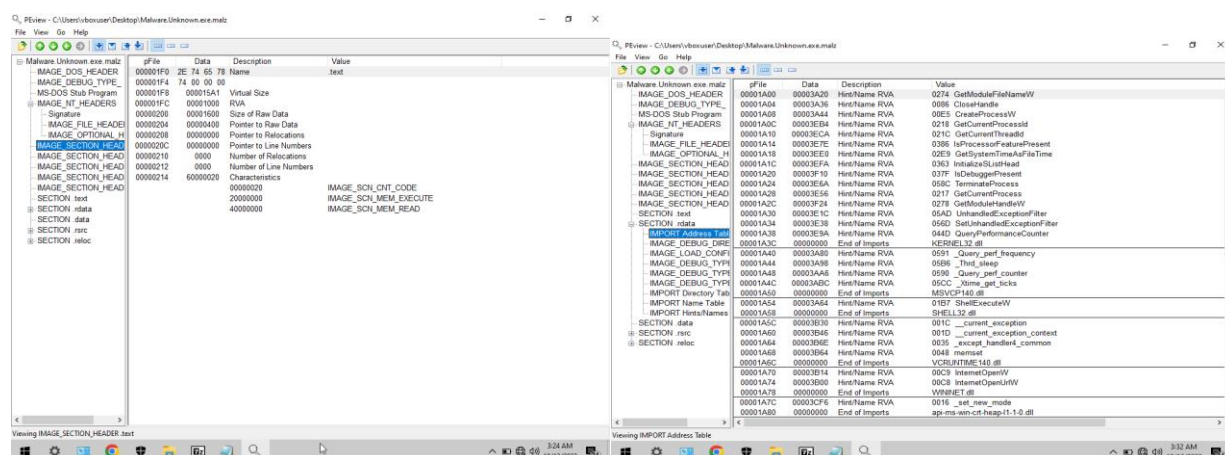
Select IMAGE\_SECTION\_HEADER.txt, compare the data of virtual size and size of raw data this gives us the information related to whether malware is packed or unpacked.

In SECTION .rdata select IMPORT Address Table, now you could see the API calls this portable executable is making note down the ones that are used in malicious activities.



(a) PE look

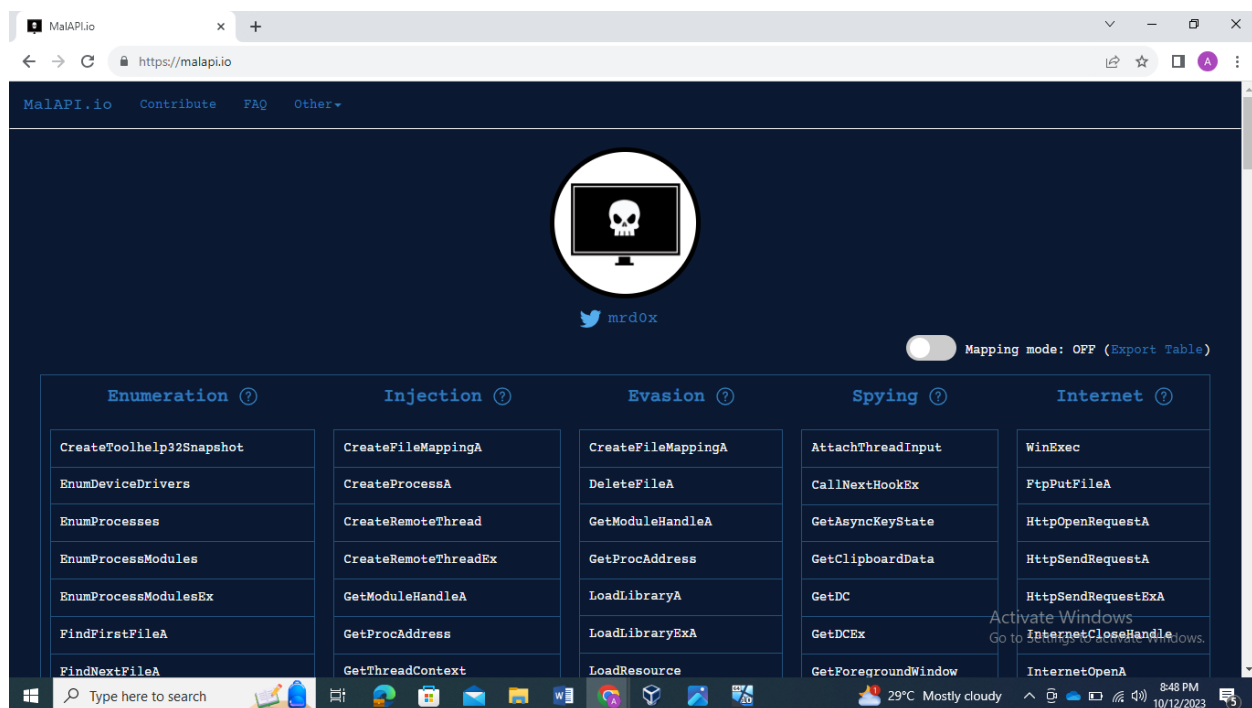
(b) Time Date Stamp



(c) Comparing raw data and virtual size to identify

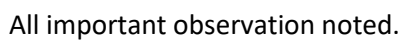
(d) Analysis of API calls

whether malware is packed or unpacked



A catalog of API calls that can be used maliciously. Malapi.io.

This catalog could help in analysis.



All important observation noted.

## Analysis through pestudio:

Open pestudio and open the portable executable file.

PEStudio is a specialized software tool that is used for analyzing and auditing Windows executable files, commonly known as PE files and these files include various Windows applications, system files, and dynamic link libraries (DLLs). PEStudio is often used for security and software analysis purposes.

The red cross in flag section indicate that the following is used or can be used by malware.

pestudio 9.55 - Malware Initial Assessment - www.winitron.com - [c:\users\vboxuser\desktop\malware.unknown.exe.malz]

file settings about

indicators (libraries > flag > name)

footprints (count > 12) \*

virustotal (error)

dos-header (size > 64 bytes)

dos-stub (size > 184 bytes)

rich-header (tooling > Visual Studio)

file-header (executable > 32-bit)

optional-header (subsystem > console)

directories (stamp > Sep.2021)

sections (count > 5)

libraries (flag > 2) \*

imports (flag > 52) \*

exports (n/a)

thread-local-storage (n/a)

.NET (n/a)

resources (signature > manifest)

strings (count > 255)

debug (streams > 3)

manifest (level > asinvoker)

version (n/a)

certificate (n/a)

overlay (n/a)

general	value
file > sha256	92730427321A1C4CFCF00580834DAEF98121EFA98B8963DA3328FD6CF1FDA8A
dos-stub > sha256	4725CA20ACEF29732DE0C97A64DFA4389EBB330100A772299C1502AE701405
dos-header > sha256	88B8D5B880DE11CB8B3547E427E8DFFFA0624E0668B8A5623E4308D019E4370
rich-header > sha256	7CC8B8D96391445204E763AB63E0DC78288D05752C7AC14772095C15A15037
section > text > sha256	F9A171BDAFFD854723EF795A546F38D03F48E3427E767F3E8E4F43AD44B0E2
section > .data > sha256	46DD5CADEF7D0106056D9054D34D59488C29E898DA5BCFDCFCF62302AFC488A8
section > .data > sha256	46BFF3F40F878A7E3EF3E898A3679C9608418D36012D999591DD1648586E3
section > .rsrc > sha256	75E650FC0D108F085CB909904D5CB598802B04F7C068E6C8622D0073AAC8F762
section > .reloc > sha256	7CFB7E58BC7AAAFD7E95DD894AE58432D887D38875996516887830E5A21FDBF
manifest > sha256	4BB79DCFA0A901F7D9EAC5AA0378AE92ACBA20C822E5DD14134F4421A3D8DF
debug > sha256	111E87F8B065A8BF6977382145FA95842145C79545CD4089E2418EDAF57B10

sha256: 92730427321A1C4CFCF00580834DAEF98121EFA98B8963DA3328FD6CF1FDA8A

cpu: 32-bit file-type: executable subsystem: console

pestudio 9.55 - Malware Initial Assessment - www.winitron.com - [c:\users\vboxuser\desktop\malware.unknown.exe.malz]

file settings about

library (11)	duplicate (0)	flag (2)	first-thunk-original (INT)	first-thunk (IAT)	type (1)	imports (52)
KERNEL32.dll	-	-	0x00003924	0x00003000	implicit	13
SHELL32.dll	-	-	0x00003978	0x00003054	implicit	1
MSVCP140.dll	-	-	0x00003964	0x00003040	implicit	4
urlmon.dll	-	×	0x00003A18	0x000030F4	implicit	1
WININET.dll	-	×	0x00003994	0x00003070	implicit	2
VCRUNTIME140.dll	-	-	0x00003A08	0x000030E4	implicit	4
api-ms-win-crt-h...	-	-	0x00003980	0x0000305C	implicit	3
api-ms-win-crt-h...	-	-	0x00003988	0x00003094	implicit	19
api-ms-win-crt-h...	-	-	0x00003980	0x0000308C	implicit	1
api-ms-win-crt-h...	-	-	0x000039A8	0x00003084	implicit	1
api-ms-win-crt-h...	-	-	0x000039A0	0x0000307C	implicit	1

sha256: 92730427321A1C4CFCF00580834DAEF98121EFA98B8963DA3328FD6CF1FDA8A

cpu: 32-bit file-type: executable subsystem: console

pestudio 9.55 - Malware Initial Assessment - www.winitor.com - [c:\users\vboxuser\desktop\malware.unknown.exe.malz]

file settings about

c:\users\vboxuser\desktop\malware.unknown.exe

indicators (libraries > flag > name)

footprints (count > 12) \*

virustotal (error)

dos-header (size > 64 bytes)

dos-stub (size > 184 bytes)

rich-header (tooling > Visual Studio)

file-header (executable > 32-bit)

optional-header (subsystem > console)

directories (stamp > Sep.2021)

sections (count > 5)

libraries (flag > 2) \*

imports (flag > 52) \*

exports (n/a)

thread-local-storage (n/a)

.NET (n/a)

resources (signature > manifest)

strings (count > 255)

debug (streams > 3)

manifest (level > asinvoker)

version (n/a)

certificate (n/a)

overlay (n/a)

imports (52)	flag (9)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (8)
InitializeStdThread	-	0x00003EFA	0x00003EFA	867 (0x0363)	synchroniz
GetCurrentProcessId	x	0x00003EB4	0x00003EB4	536 (0x0218)	reconnaiss
IsProcessorFeaturePresent	-	0x00003E7E	0x00003E7E	902 (0x0386)	reconnaiss
IsDebuggerPresent	-	0x00003F10	0x00003F10	895 (0x037F)	reconnaiss
QueryPerformanceCounter	-	0x00003E9A	0x00003E9A	1101 (0x044D)	reconnaiss
URLDownloadToFileW	x	0x00003ADE	0x00003ADE	116 (0x0074)	network
InternetOpenW	x	0x00003B14	0x00003B14	201 (0x00C9)	network
InternetOpenUrlW	x	0x00003B00	0x00003B00	200 (0x00C8)	network
memset	-	0x00003B64	0x00003B64	72 (0x0048)	memory
GetSystemTimeAsFileTime	-	0x00003EE0	0x00003EE0	745 (0x02E9)	file
CreateProcessW	x	0x00003A44	0x00003A44	229 (0x00E5)	execution
GetCurrentThreadId	x	0x00003ECA	0x00003ECA	540 (0x021C)	execution
TerminateProcess	x	0x00003E6A	0x00003E6A	1420 (0x058C)	execution
GetCurrentProcess	x	0x00003E56	0x00003E56	535 (0x0217)	execution
ShellExecuteW	x	0x00003A64	0x00003A64	439 (0x01B7)	execution
UnhandledExceptionFilter	-	0x00003E1C	0x00003E1C	1453 (0x05AD)	exception
SetUnhandledExceptionFilter	-	0x00003E38	0x00003E38	1389 (0x056D)	exception
GetModuleFileNameW	-	0x00003A20	0x00003A20	628 (0x0274)	dynamic-lib
GetModuleHandleW	-	0x00003F24	0x00003F24	632 (0x0278)	dynamic-lib
CloseHandle	-	0x00003A36	0x00003A36	134 (0x0086)	-
Query_perf_frequency	-	0x00003A80	0x00003A80	1425 (0x0591)	-
Thrd_sleep	-	0x00003A98	0x00003A98	1462 (0x05B6)	-
Query_perf_counter	-	0x00003AA6	0x00003AA6	1434 (0x0590)	-
Xtime_get_ticks	-	0x00003ABC	0x00003ABC	1484 (0x05C4)	-
current_exception	-	0x00003B30	0x00003B30	28 (0x001C)	-
current_exception_context	-	0x00003B46	0x00003B46	29 (0x001D)	-
except_handler4_common	-	0x00003B6E	0x00003B6E	53 (0x0035)	-
p_commode	-	0x00003D06	0x00003D06	1 (0x0001)	-
stdio_common_vswprintf	-	0x00003B9A	0x00003B9A	17 (0x0011)	-
set_fmode	-	0x00003C74	0x00003C74	84 (0x0054)	-
c_exit	-	0x00003CA8	0x00003CA8	22 (0x0016)	-

sha256: 92730427321A1C4CFC0D0580834DAEF98121EFA98B8963DA3328FD6CF1FDA8A

cpu: 32-bit file-type: executable subsystem: console

4:19 AM 10/12/2023

pestudio 9.55 - Malware Initial Assessment - www.winitor.com - [c:\users\vboxuser\desktop\malware.unknown.exe.malz]

file settings about

c:\users\vboxuser\desktop\malware.unknown.exe

encoding (2)

size (bytes)

location

flag (9)

label (67)

group (8)

tech

ascii	19	.rdata	-	import	synchronization	-
ascii	25	.rdata	-	import	reconnaissance	-
ascii	23	.rdata	-	import	reconnaissance	-
ascii	19	.rdata	x	import	reconnaissance	T10
ascii	17	.rdata	-	import	reconnaissance	T10
ascii	17	.rdata	x	import	network	-
ascii	15	.rdata	x	import	network	-
ascii	12	.rdata	x	import	network	-
ascii	10	.rdata	-	file	network	-
ascii	11	.rdata	-	file	network	-
ascii	6	.rdata	-	-	memory	-
ascii	23	.rdata	-	import	file	T11
ascii	13	.rdata	x	import	execution	T11
ascii	12	.rdata	x	import	execution	T11
ascii	17	.rdata	x	import	execution	T10
ascii	16	.rdata	x	import	execution	-
ascii	18	.rdata	x	import	execution	T10
ascii	24	.rdata	-	import	exception	-
ascii	27	.rdata	-	import	exception	-
ascii	17	.rdata	-	import	dynamic-library	-
ascii	15	.rdata	-	import	dynamic-library	-
unicode	59	.rdata	-	utility	-	T10
unicode	76	.rdata	-	utility	-	T10
unicode	4	.rdata	-	utility	-	-
unicode	11	.rdata	-	user-agent	-	-
unicode	21	.rdata	-	url-pattern	-	-
ascii	11	.rdata	-	import	-	-
ascii	11	.rdata	-	import	-	-
ascii	19	.rdata	-	import	-	-
ascii	16	.rdata	-	import	-	-

sha256: 92730427321A1C4CFC0D0580834DAEF98121EFA98B8963DA3328FD6CF1FDA8A

cpu: 32-bit file-type: executable subsystem: console

4:20 AM 10/12/2023

pestudio 9.55 - Malware Initial Assessment - www.winitor.com - [c:\users\vboxuser\desktop\malware.unknown.exe.malz]

file settings about

c:\users\vboxuser\desktop\malware.unknown.exe

indicators (libraries > flag > name)

footprints (count > 12) \*

dos-header (size > 64 bytes)

rich-header (tooling > Visual Studio)

file-header (executable > 32-bit)

optional-header (subsystem > console)

directories (stamp > Sep.2021)

sections (count > 5)

libraries (flag > 2) \*

imports (flag > 52) \*

exports (n/a)

thread-local-storage (n/a)

.NET (n/a)

resources (signature > manifest)

strings (count > 255)

debug (streams > 3)

manifest (level > asinvoker)

version (n/a)

certificate (n/a)

overlay (n/a)

	24)	detail	level
flag > name	OLE32 Extensions for Win32		1
flag > name	Internet Extensions for Win32 Library		1
flag > count	9		1
cksum	0x00000000		2
API	dynamic-library, execution, reconnaissance, file, synchronization, excep...		2
RI	http://ssl-6582datamanager.helpdeskbro.local/favicon.ico		2
RI	http://huskyhacks.dev		2
chnique	T1106, T1057, T1124, T1082, T1059, T1018		2
ppv	5.719		3
ature	Microsoft Visual C++		3
print	92730427321A1C4CCFC0D0580834DAEF98121EFA9B8B8963DA332BFD6CF...		3
er > checksum	12288 bytes		3
er > offset	0x729811B0		3
er > footprint	0x00000080		3
ing	7CCBB8D96391445204E763AB63E0DCA7B288D05752C74CE14772095C15...		3
protection	Visual Studio 2008		3
protection	data-execution-prevention (DEP) > ON		3
protection	control-flow-guard (CFG) > OFF		3
protection	address-space-layout-randomization (ASLR) > ON		3
streams	3		3
file-name	C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\Download...		3
protection	code-integrity (CI) > OFF		3
system	console		3
md5	F2D1B81B70ADF3F2DCC6D462AE64DC4		3

sha256: 92730427321A1C4CCFC0D0580834DAEF98121EFA9B8B8963DA332BFD6CF1FDA8A

cpu: 32-bit file-type: executable subsystem: console

4:15 AM 10/12/2023



Packed and unpacked malware refer to two different states of malicious software, where "packing" is a technique used by malware authors to obfuscate their code and make it more difficult to detect, while "unpacking" is the process of reversing this technique to reveal the original, malicious code.

The image shows a Windows desktop with a taskbar at the bottom. The active window is titled "Malware NotPacked.exe.malz" and displays a detailed analysis of the file. The window is divided into several panes. The top pane shows the raw data of the file, including sections like IMAGE\_DOS\_HEADER, IMAGE\_NT\_HEADERS, and various sections like .text, .data, and .rdata. The bottom pane shows the file's metadata, including its name, size, and various attributes like 'Is Executable', 'Is Portable', and 'Is 32-bit'. The bottom pane also shows the file's sections and their characteristics.

The top pane displays the raw data of the file, including sections like IMAGE\_DOS\_HEADER, IMAGE\_NT\_HEADERS, and various sections like .text, .data, and .rdata. The bottom pane shows the file's metadata, including its name, size, and various attributes like 'Is Executable', 'Is Portable', and 'Is 32-bit'. The bottom pane also shows the file's sections and their characteristics.

The bottom pane shows the file's metadata, including its name, size, and various attributes like 'Is Executable', 'Is Portable', and 'Is 32-bit'. The bottom pane also shows the file's sections and their characteristics.

Packed:

PEView - C:\Users\vbouser\Desktop\Malware.Packed.exe.malz

	pFile	Data	Description	Value
Malware Packed.exe.malz				
IMAGE_DOS_HEADER	0000BA3C	000188AC	Hint/Name RVA	0000 FreeSid
MS-DOS Stub Program	0000BA40	00000000	End of Imports	ADVAPI32.dll
IMAGE_NT_HEADERS	0000BA44	000188D4	Hint/Name RVA	0000 LoadLibraryA
Signature	0000BA48	000188B6	Hint/Name RVA	0000 ExitProcess
IMAGE_FILE_HEADER	0000BA4C	000188C4	Hint/Name RVA	0000 GetProcAddress
IMAGE_OPTIONAL_HEADER	0000BA50	000188E2	Hint/Name RVA	0000 VirtualProtect
IMAGE_SECTION_HEADER	0000BA54	00000000	End of Imports	KERNEL32.DLL
IMAGE_SECTION_HEADER	0000BA58	000188F2	Hint/Name RVA	0000 _job
IMAGE_SECTION_HEADER	0000BA5C	00000000	End of Imports	MSVCRT.dll
SECTION UPX0	0000BA60	000188F8	Hint/Name RVA	0000 WSARecv
SECTION UPX1	0000BA64	00000000	End of Imports	WS2_32.dll
SECTION .rsrc	0000BA68	8000006F	Ordinal	006F
IMAGE_RESOURCE_DIRECTORY	0000BA6C	00000000	End of Imports	WSOCK32.dll
IMAGE_RESOURCE_DIRECTORY				
IMAGE_RESOURCE_DIRECTORY				
IMAGE_RESOURCE_DIRECTORY				
VERSION 0001 0409				
IMPORT Directory Table				
IMPORT Address Table				
IMPORT DLL Names				
IMPORT Hints/Names				

Viewing IMPORT Address Table

PEView - C:\Users\vbouser\Desktop\Malware.Packed.exe.malz

	pFile	Data	Description	Value
Malware Packed.exe.malz				
IMAGE_DOS_HEADER	000001E0	55 50 58 30	Name	UPX0
MS-DOS Stub Program	000001E4	00 00 00 00		
IMAGE_NT_HEADERS	000001E8	0000C000	Virtual Size	
Signature	000001EC	00001000	RVA	
IMAGE_FILE_HEADER	000001F0	00000000	Size of Raw Data	
IMAGE_OPTIONAL_HEADER	000001F4	00000400	Pointer to Raw Data	
IMAGE_SECTION_HEADER	000001F8	00000000	Pointer to Relocations	
IMAGE_SECTION_HEADER	000001FC	00000000	Pointer to Line Numbers	
IMAGE_SECTION_HEADER	00000200	0000	Number of Relocations	
SECTION UPX0	00000202	0000	Number of Line Numbers	
SECTION UPX1	00000204	E0000080	Characteristics	
SECTION .rsrc				
				IMAGE_SCN_CNT_UNINITIALIZED_DATA
				IMAGE_SCN_MEM_EXECUTE
				IMAGE_SCN_MEM_READ
				IMAGE_SCN_MEM_WRITE

Viewing IMAGE\_SECTION\_HEADER UPX0