STATIC ANALYSIS

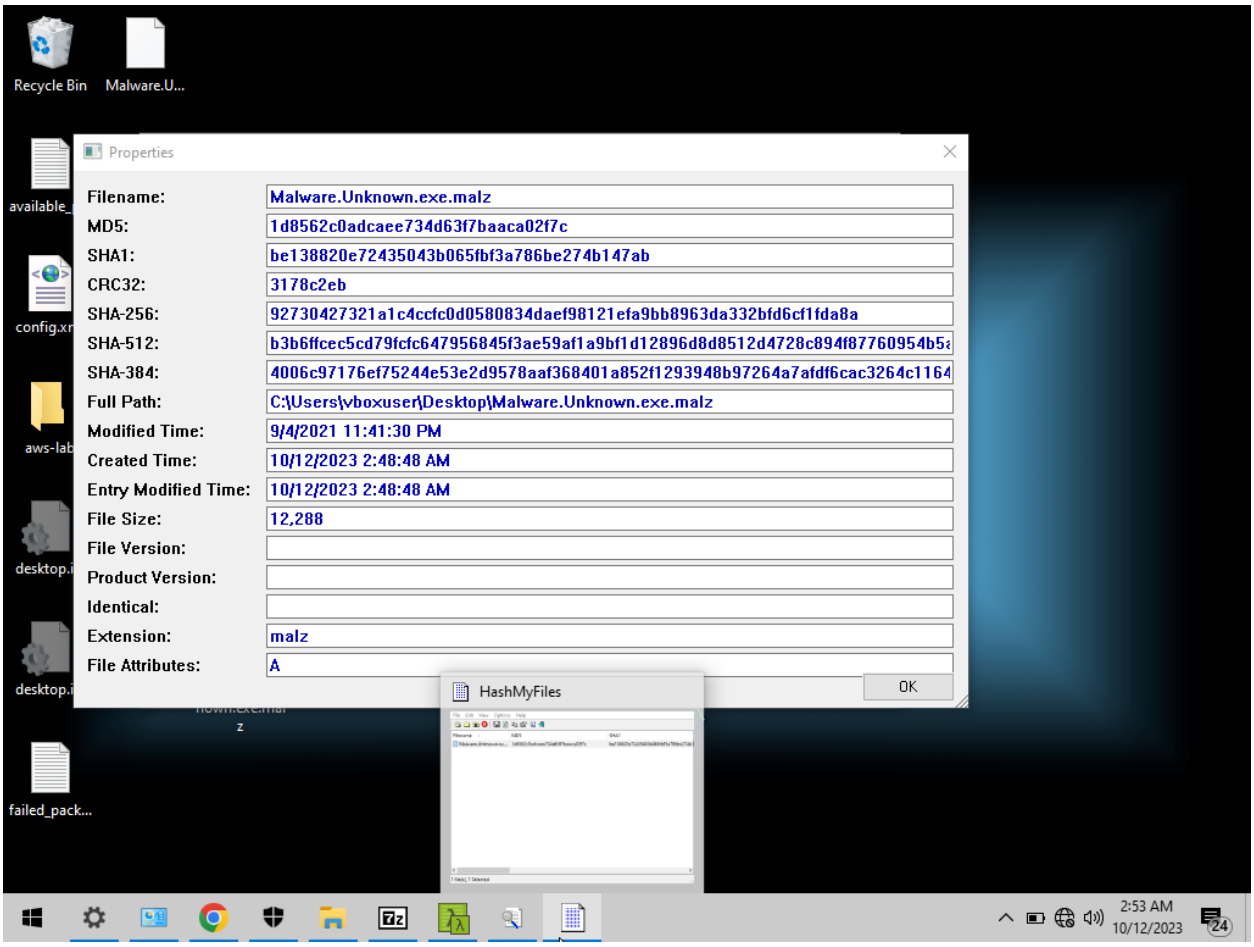
Hashes Analysis:

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

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

Important:

- SHA-256
- MD5

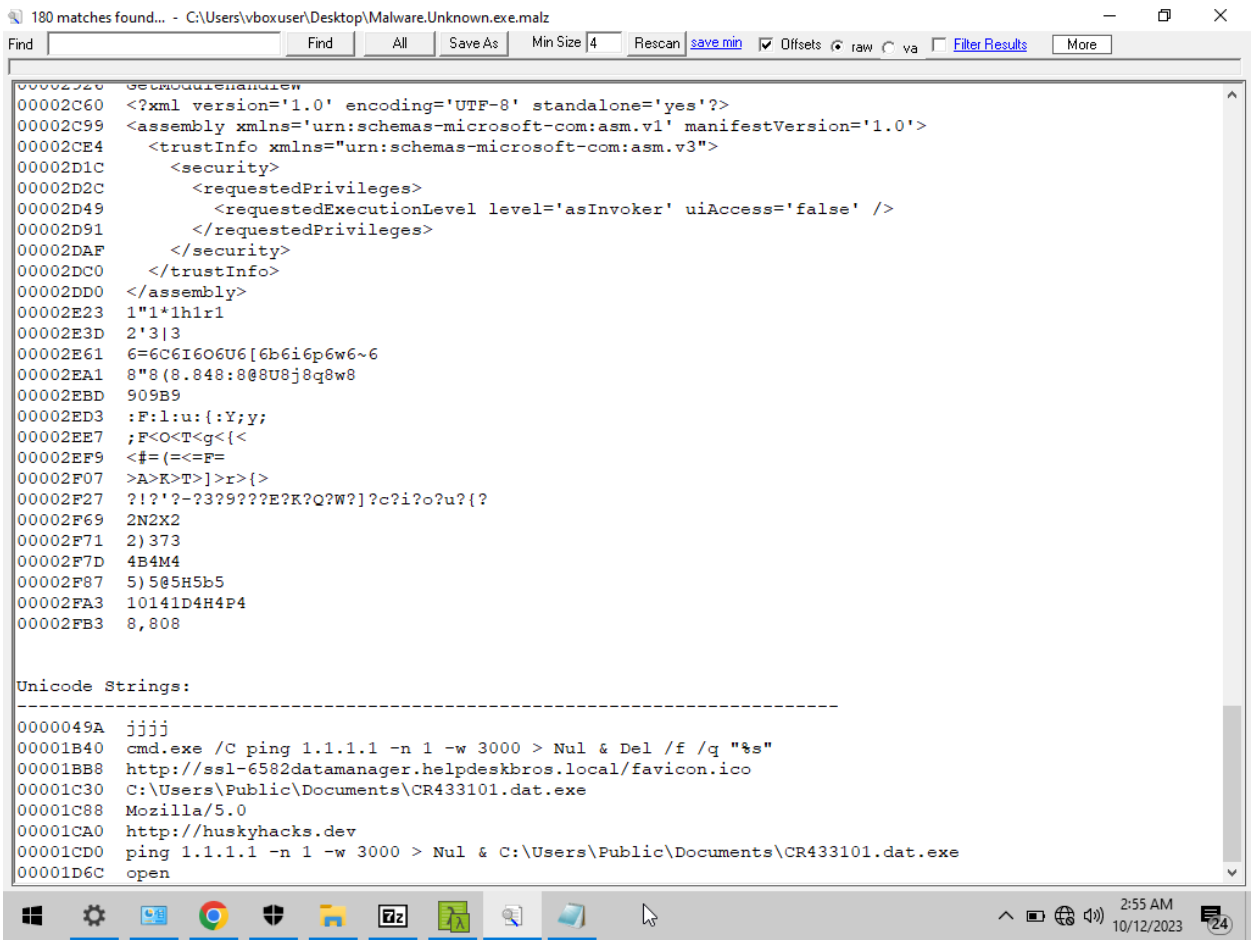


String Analysis:

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.



PEview:

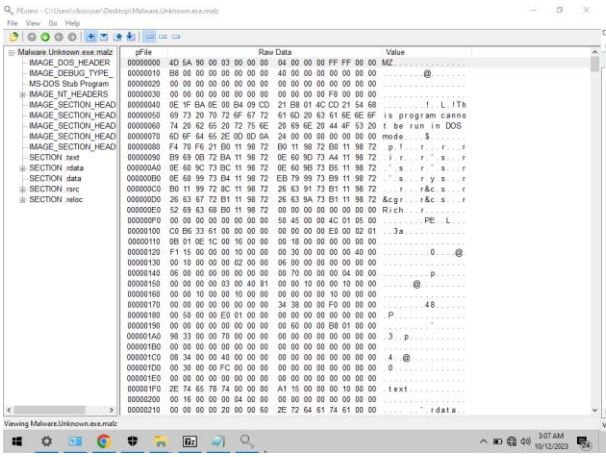
Now we will continue our analysis through PEview.

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

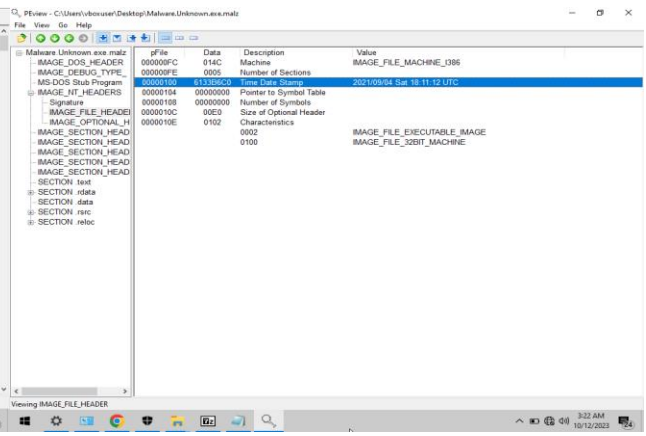
Select IMAGE_TIME_HEADER in IMAGE_NT_HEADERS, you could see various details related to file such as Time Date Stamp.

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.

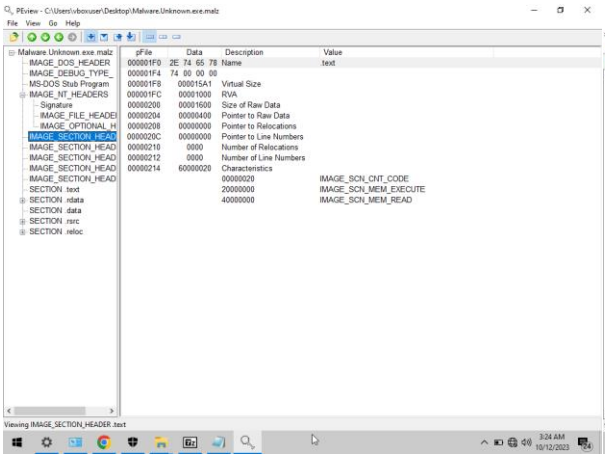
In SECTION .rdata select IMPORT Address Table, now you could see the API calls this portable executable is making note down the ones that are used in malicious activities.



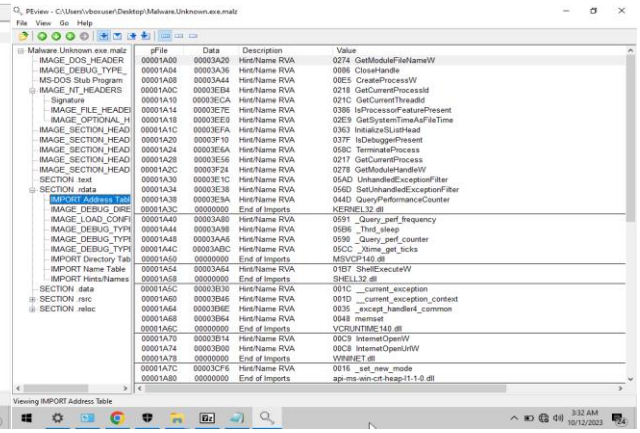
(a) PE look



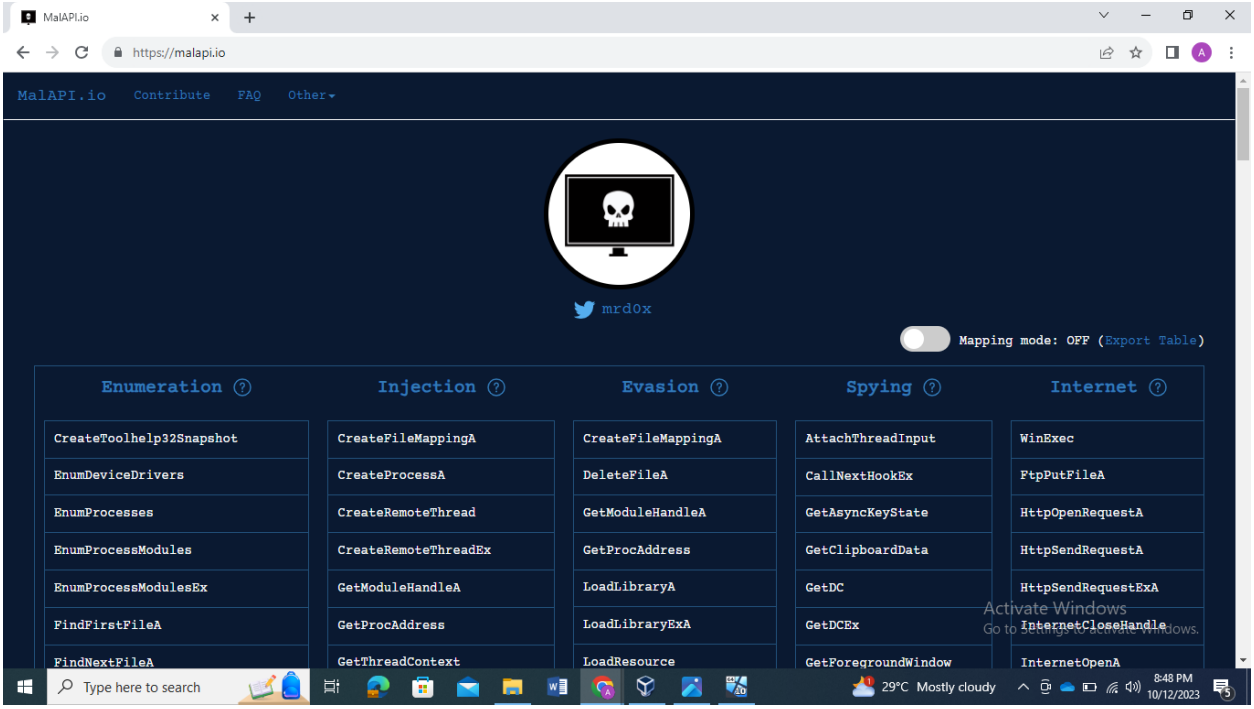
(b) Time Date Stamp



(c)Comparing raw data and virtual size to identify whether malware is packed or unpacked

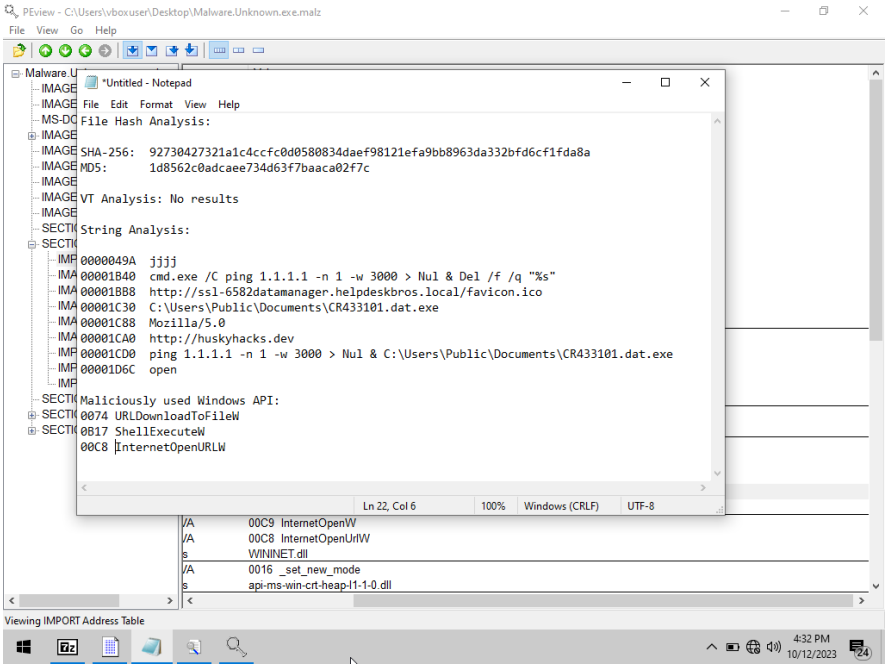


(d) Analysis of API calls



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

This catalog could help in analysis.



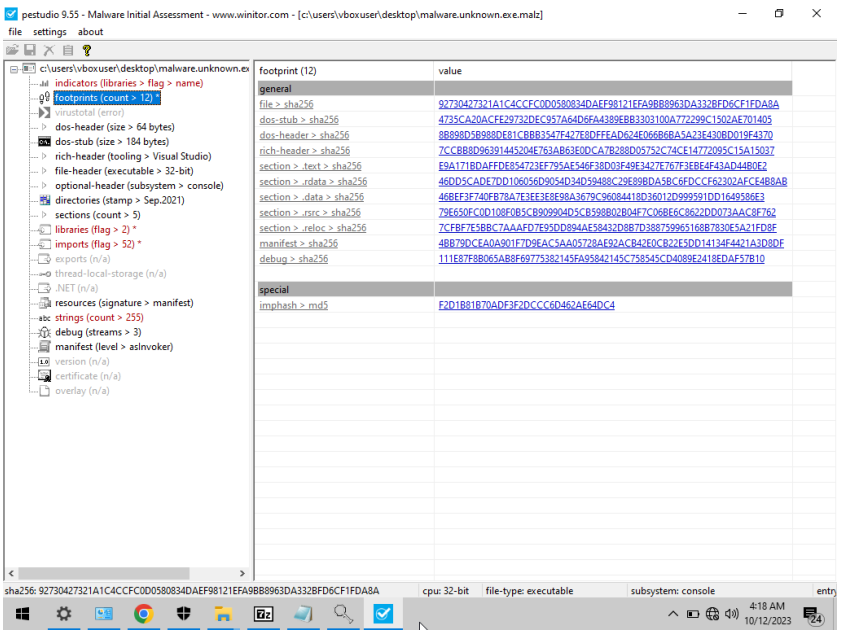
All important observation noted.

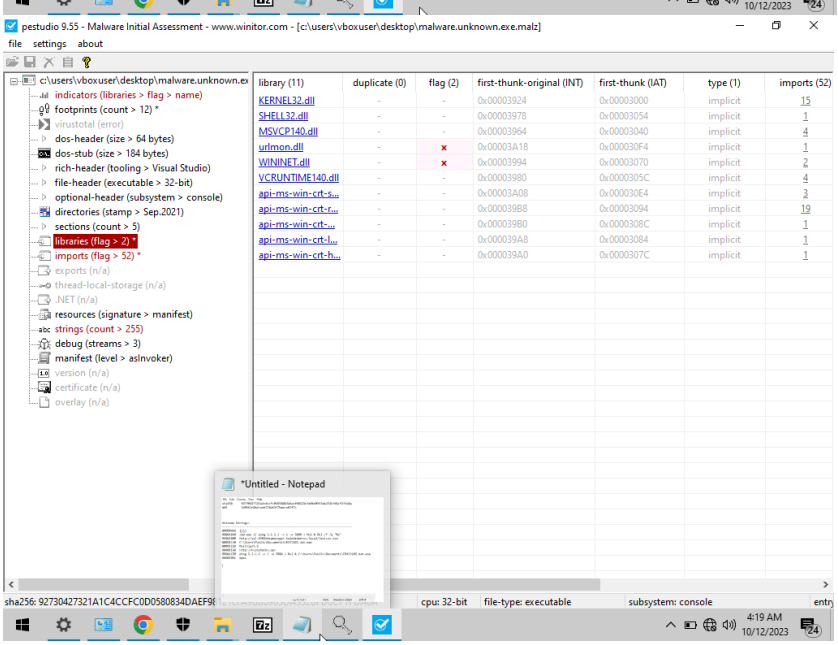
Analysis through pestudio:

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.winitor.com - [c:\users\vboxuser\desktop\malware.unknown.exe.malz]

file settings about

c:\users\vboxuser\desktop\malware.unknown.ex
- 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)
InitializeSListHead	-	0x00003EFA	0x00003EFA	867 (0x0363)	synchroniz
GetCurrentProcessId	×	0x00003EB4	0x00003EB4	536 (0x0218)	reconnaissa
IsProcessorFeaturePresent	-	0x00003E7E	0x00003E7E	902 (0x0386)	reconnaissa
IsDebuggerPresent	-	0x00003F10	0x00003F10	895 (0x037F)	reconnaissa
QueryPerformanceCounter	-	0x00003E9A	0x00003E9A	1101 (0x044D)	reconnaissa
URLDownloadToFileW	×	0x00003ADE	0x00003ADE	116 (0x0074)	network
InternetOpenW	×	0x00003B14	0x00003B14	201 (0x00C9)	network
InternetOpenUrlW	×	0x00003B00	0x00003B00	200 (0x00C8)	network
memset	-	0x00003B64	0x00003B64	72 (0x0048)	memory
GetSystemTimeAsFileTime	-	0x00003EE0	0x00003EE0	745 (0x02E9)	file
CreateProcessW	×	0x00003A44	0x00003A44	229 (0x00E5)	execution
GetCurrentThreadId	×	0x00003ECA	0x00003ECA	540 (0x021C)	execution
TerminateProcess	×	0x00003E6A	0x00003E6A	1420 (0x058C)	execution
GetCurrentProcess	×	0x00003E56	0x00003E56	535 (0x0217)	execution
ShellExecuteW	×	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	1424 (0x0590)	-
_Xtime_get_ticks	-	0x00003ABC	0x00003ABC	1484 (0x05CC)	-
__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: 92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A | cpu: 32-bit | file-type: executable | subsystem: console | entry

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.ex
- 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)

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	×	import	reconnaissance	T10
ascii	17	.rdata	-	import	reconnaissance	T10
ascii	17	.rdata	×	import	network	-
ascii	15	.rdata	×	import	network	-
ascii	12	.rdata	×	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	×	import	execution	T11
ascii	12	.rdata	×	import	execution	T11
ascii	17	.rdata	×	import	execution	T10
ascii	16	.rdata	×	import	execution	-
ascii	18	.rdata	×	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	21	.rdata	-	import	-	-
ascii	11	.rdata	-	import	-	-
ascii	19	.rdata	-	import	-	-
ascii	16	.rdata	-	import	-	-

sha256: 92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A | cpu: 32-bit | file-type: executable | subsystem: console | entry

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.ex
- 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)

(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
RL	http://ssl-6582datamanager.helpdeskbros.local/favicon.ico	2
RL	http://huskyhacks.dev	2
chnique	T1106, T1057, T1124, T1082, T1059, T1018	2
opy	5.719	3
ature	Microsoft Visual C++	3
print	92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF...	3
	12288 bytes	3
er > checksum	0x729811B0	3
er > offset	0x00000080	3
er > footprint	7CCBB8D96391445204E763AB63E0DCA7B288D05752C74CE14772095C15...	3
ing	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
ile-name	C:\Users\Matt\source\repos\HuskyHacks\PMAT-maldev\src\Download...	3
protection	code-integrity (CI) > OFF	3
ystem	console	3
md5	F2D1B81B70ADF3F2DCCC6D462AE64DC4	3

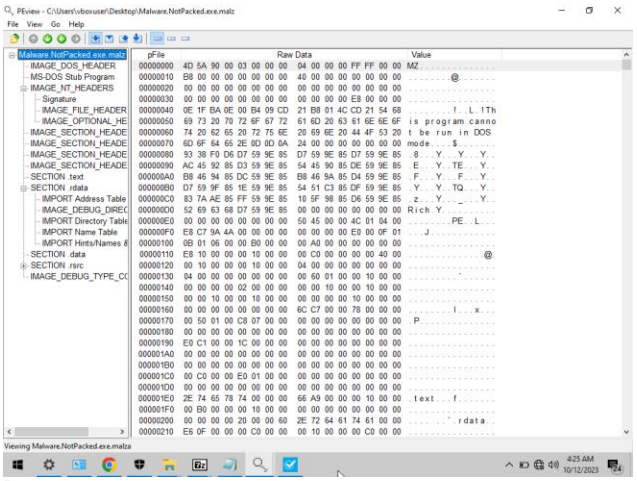
sha256: 92730427321A1C4CCFC0D0580834DAEF98121EFA9BB8963DA332BFD6CF1FDA8A | cpu: 32-bit | file-type: executable | subsystem: console | entr

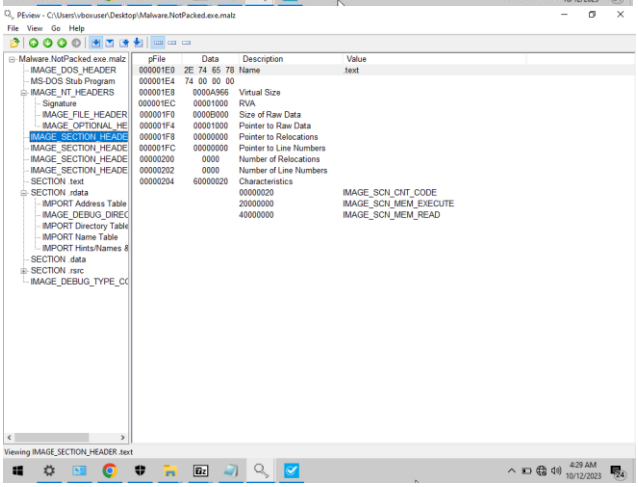
4:15 AM
10/12/2023

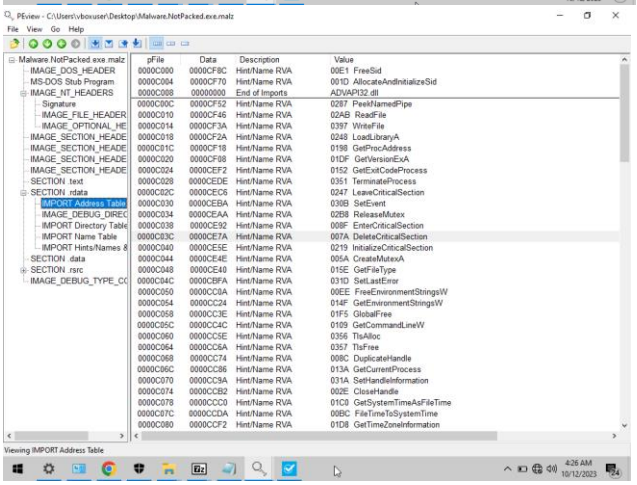
Difference in Packed and Unpacked Malware:

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.

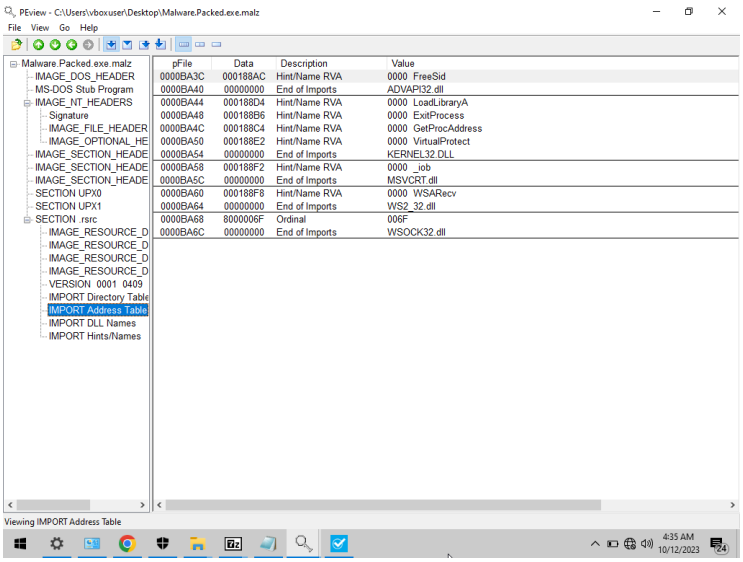
Unpacked:

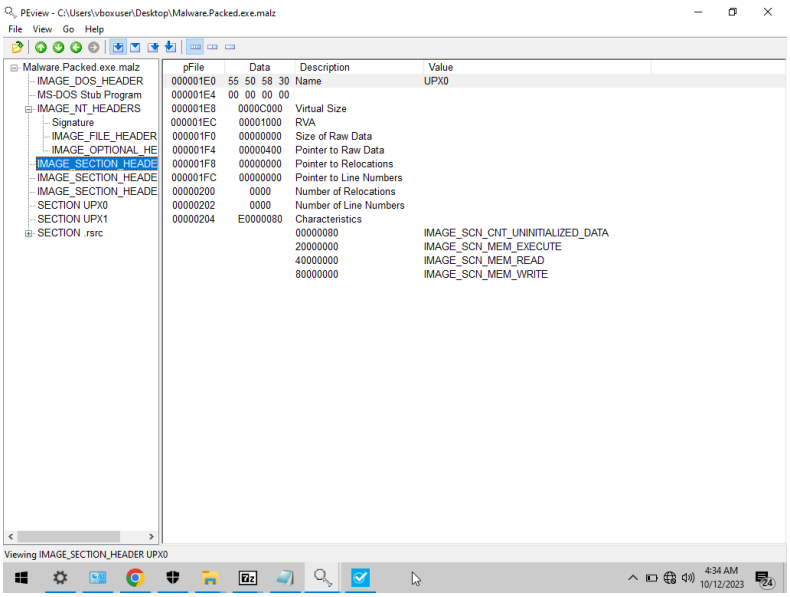






Packed:


PEview - C:\Users\vboxuser\Desktop\Malware.Packed.exe.malz
File View Go Help
Malware.Packed.exe.malz
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HE
IMAGE_SECTION_HEADE
IMAGE_SECTION_HEADE
IMAGE_SECTION_HEADE
SECTION UPX0
SECTION UPX1
SECTION .rsrc
IMAGE_RESOURCE_D
IMAGE_RESOURCE_D
IMAGE_RESOURCE_D
IMAGE_RESOURCE_D
VERSION 0001 0409
IMPORT Directory Table
IMPORT Address Table
IMPORT DLL Names
IMPORT Hints/Names
pFile Data Description Value
0000BA3C 000188AC Hint/Name RVA 0000 FreeSid
0000BA40 00000000 End of Imports ADVAPI32.dll
0000BA44 000188D4 Hint/Name RVA 0000 LoadLibraryA
0000BA48 000188B6 Hint/Name RVA 0000 ExitProcess
0000BA4C 000188C4 Hint/Name RVA 0000 GetProcAddress
0000BA50 000188E2 Hint/Name RVA 0000 VirtualProtect
0000BA54 00000000 End of Imports KERNEL32.DLL
0000BA58 000188F2 Hint/Name RVA 0000 _iob
0000BA5C 00000000 End of Imports MSVCRT.dll
0000BA60 000188F8 Hint/Name RVA 0000 WSARecv
0000BA64 00000000 End of Imports WS2_32.dll
0000BA68 8000006F Ordinal 006F
0000BA6C 00000000 End of Imports WSOCK32.dll
Viewing IMPORT Address Table
4:35 AM
10/12/2023


PEview - C:\Users\vboxuser\Desktop\Malware.Packed.exe.malz
File View Go Help
Malware.Packed.exe.malz
IMAGE_DOS_HEADER
MS-DOS Stub Program
IMAGE_NT_HEADERS
Signature
IMAGE_FILE_HEADER
IMAGE_OPTIONAL_HE
IMAGE_SECTION_HEADE
IMAGE_SECTION_HEADE
IMAGE_SECTION_HEADE
SECTION UPX0
SECTION UPX1
SECTION .rsrc
pFile Data Description Value
000001E0 55 50 58 30 Name UPX0
000001E4 00 00 00 00
000001E8 0000C000 Virtual Size
000001EC 00001000 RVA
000001F0 00000000 Size of Raw Data
000001F4 00000400 Pointer to Raw Data
000001F8 00000000 Pointer to Relocations
000001FC 00000000 Pointer to Line Numbers
00000200 0000 Number of Relocations
00000202 0000 Number of Line Numbers
00000204 E0000080 Characteristics
00000080 IMAGE_SCN_CNT_UNINITIALIZED_DATA
20000000 IMAGE_SCN_MEM_EXECUTE
40000000 IMAGE_SCN_MEM_READ
80000000 IMAGE_SCN_MEM_WRITE
Viewing IMAGE_SECTION_HEADER UPX0
4:34 AM
10/12/2023