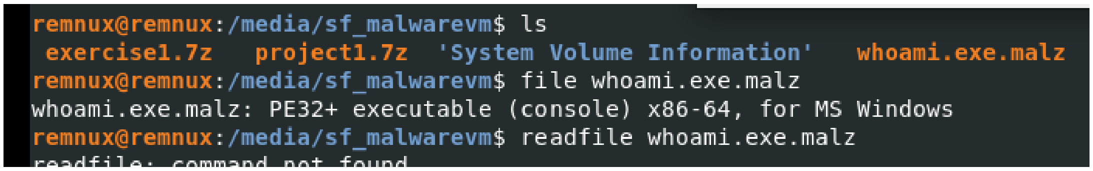
Project 1

CPSC 458-03 Fall 2024

Cassandra Guevara, Ryan Hellwege, Kyle Ho, Phu Lam, Wayne Muse

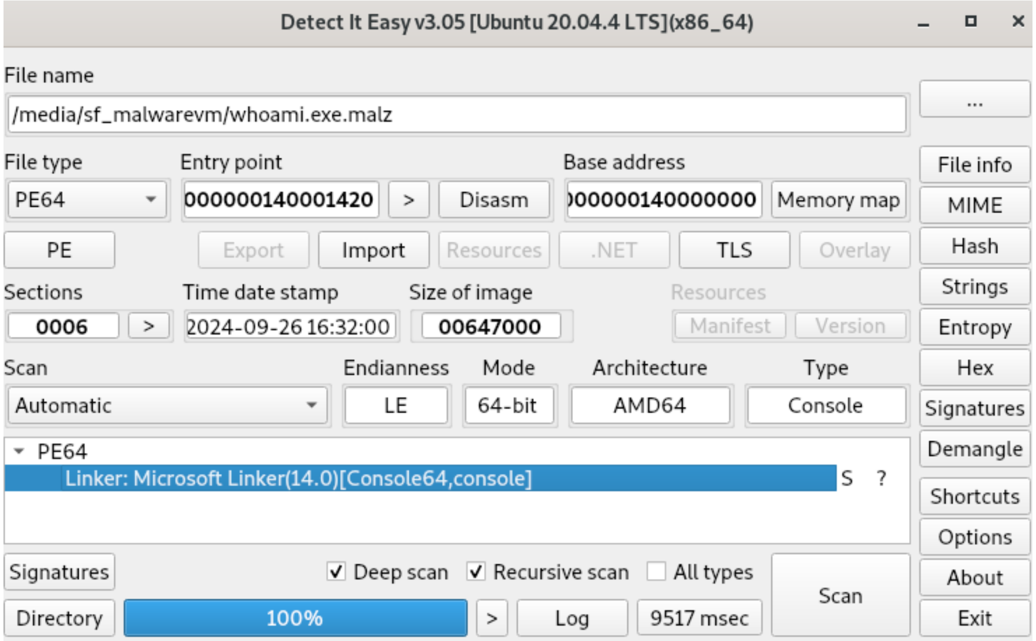
Static Analysis

1. Remnux
    a. File Type
        i. **Initial File Identification**
        ii. Command: file whoami.exe.malz
        iii. Result: whoami.exe.malz: PE32+ executable (console) x86-64, for MS Windows
        iv. Analysis: The file command identifies the file as a PE32+ executable, indicating that it is a Windows 64-bit binary.
        v. 

```
remnux@remnux:/media/sf_malwarevm$ ls
 exercise1.7z   project1.7z  'System Volume Information'   whoami.exe.malz
remnux@remnux:/media/sf_malwarevm$ file whoami.exe.malz
whoami.exe.malz: PE32+ executable (console) x86-64, for MS Windows
remnux@remnux:/media/sf_malwarevm$ readfile whoami.exe.malz
readfile: command not found
```

    b. Die
        i. Command: die whoami.exe.malz
        ii. Result: Linker: Microsoft Linker(14.0)[Console64,console]
        iii. Analysis: This shows how the file was built and compiled which can give clues about it’s development environment. 14.0 refers to Microsoft Linker which corresponds to Visual Studio 2015 and so that was used to compile the malware. Console 64 suggests it is an executable and runs in a command-line environment meaning it could be using command line to issue commands and interact with system files or malicious behavior.

iv.



Detect It Easy v3.05 [Ubuntu 20.04.4 LTS](x86_64)

File name: /media/sf_malwarevm/whoami.exe.malz

File type: PE64

Entry point: 000000140001420

Base address:)00000140000000

Sections: 0006

Time date stamp: 2024-09-26 16:32:00

Size of image: 00647000

Scan: Automatic

Endianness: LE

Mode: 64-bit

Architecture: AMD64

Type: Console

PE64
- Linker: Microsoft Linker(14.0)[Console64,console] S ?

☑ Deep scan ☑ Recursive scan □ All types

100%

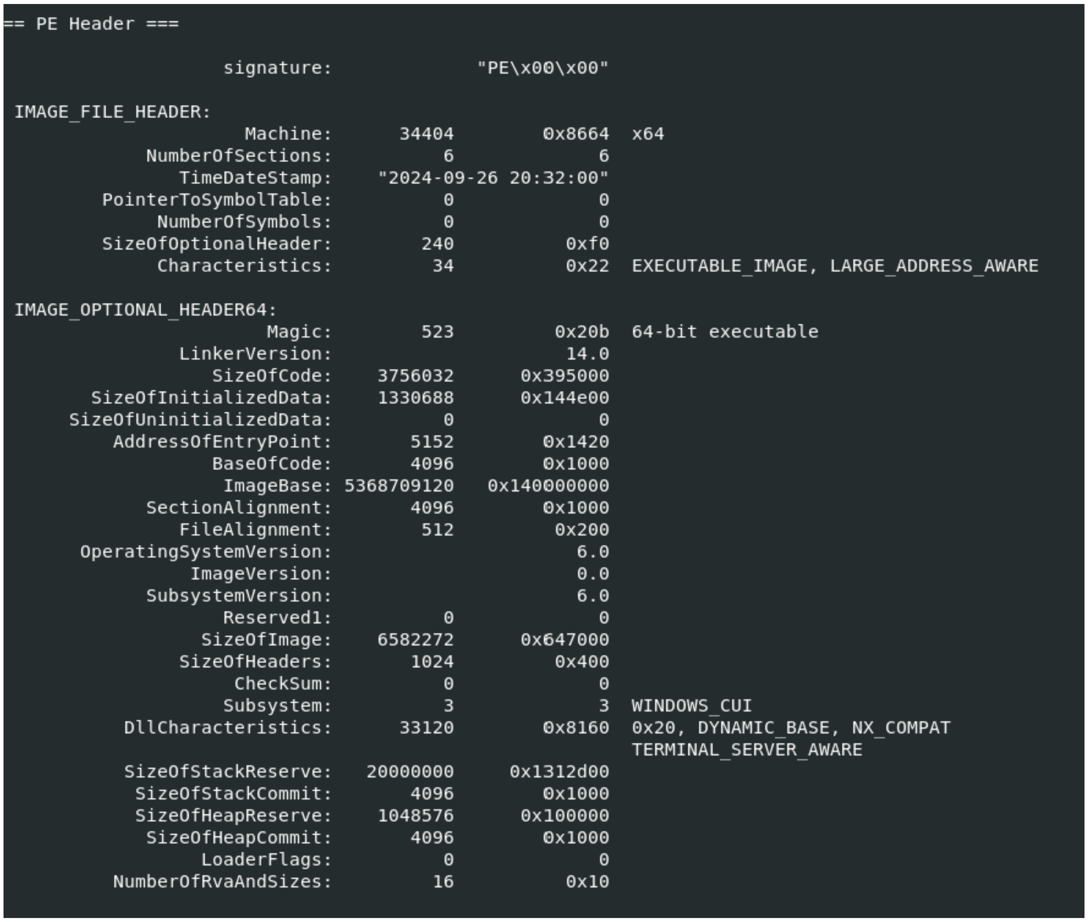
9517 msec

c. PeDump

i. Command: pedump whoami.exe.malz

ii. Result:

iii.

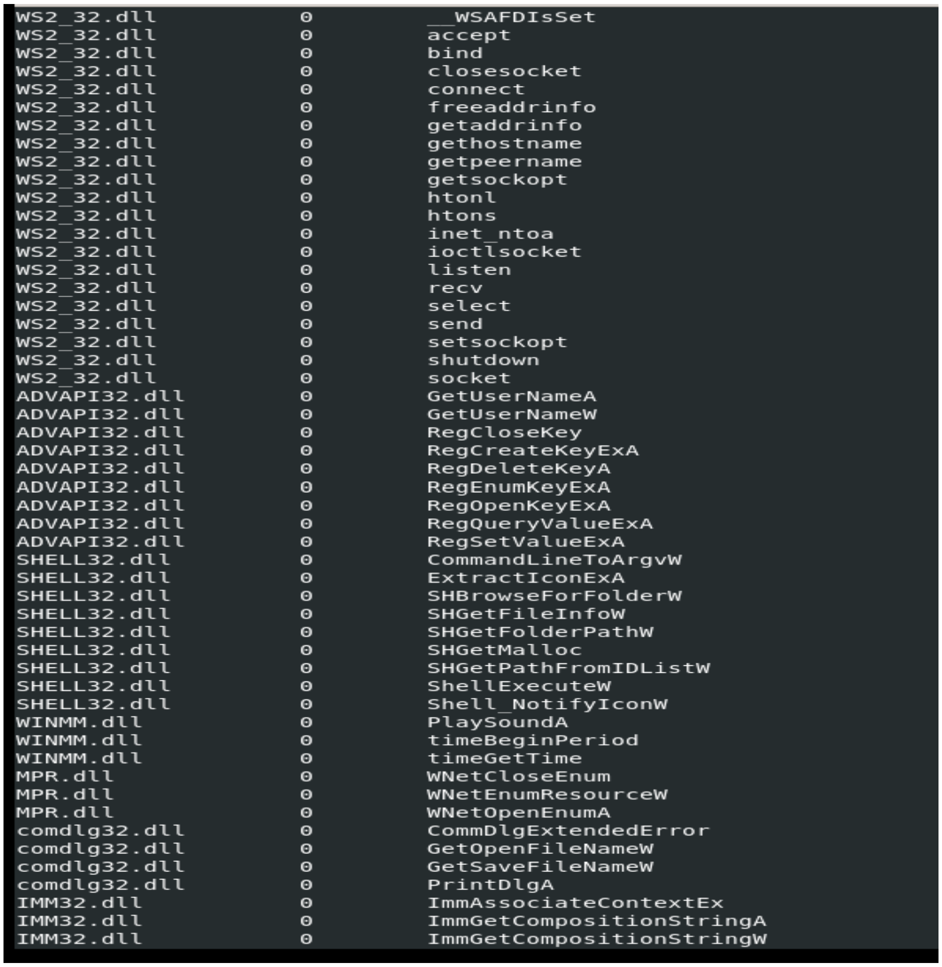


```
== PE Header ===

                    signature:             "PE\x00\x00"

 IMAGE_FILE_HEADER:
                      Machine:      34404        0x8664  x64
             NumberOfSections:          6             6
                TimeDateStamp:    "2024-09-26 20:32:00"
         PointerToSymbolTable:          0             0
              NumberOfSymbols:          0             0
         SizeOfOptionalHeader:        240          0xf0
              Characteristics:         34          0x22  EXECUTABLE_IMAGE, LARGE_ADDRESS_AWARE

 IMAGE_OPTIONAL_HEADER64:
                        Magic:        523         0x20b  64-bit executable
                LinkerVersion:                     14.0
                   SizeOfCode:    3756032      0x395000
        SizeOfInitializedData:    1330688      0x144e00
      SizeOfUninitializedData:          0             0
          AddressOfEntryPoint:       5152        0x1420
                   BaseOfCode:       4096        0x1000
                    ImageBase: 5368709120   0x140000000
             SectionAlignment:       4096        0x1000
                FileAlignment:        512         0x200
       OperatingSystemVersion:                      6.0
                 ImageVersion:                      0.0
             SubsystemVersion:                      6.0
                    Reserved1:          0             0
                  SizeOfImage:    6582272      0x647000
                SizeOfHeaders:       1024         0x400
                     CheckSum:          0             0
                    Subsystem:          3             3  WINDOWS_CUI
           DllCharacteristics:      33120        0x8160  0x20, DYNAMIC_BASE, NX_COMPAT
                                                         TERMINAL_SERVER_AWARE

           SizeOfStackReserve:   20000000     0x1312d00
            SizeOfStackCommit:       4096        0x1000
            SizeOfHeapReserve:    1048576      0x100000
             SizeOfHeapCommit:       4096        0x1000
                  LoaderFlags:          0             0
          NumberOfRvaAndSizes:         16          0x10
```

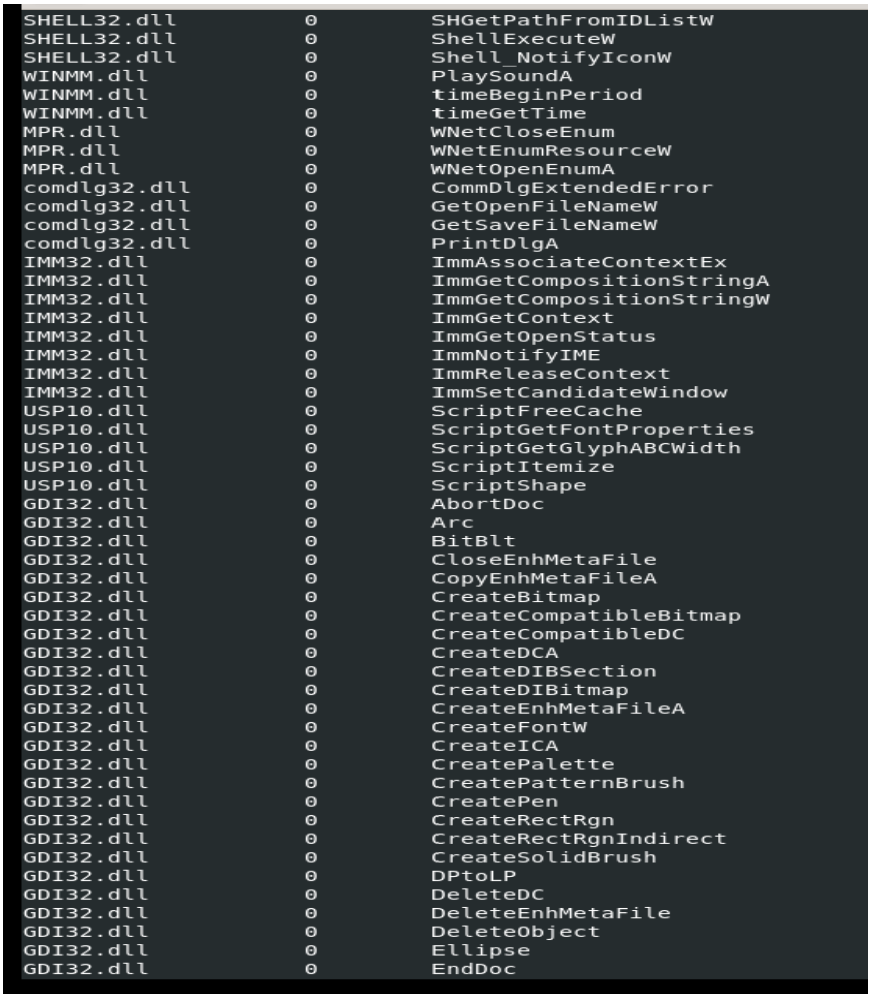
iv. **Findings**

1. PE header shows that the malware is a 64-bit windows console application with 6 sections and a compilation timestamp.

v.



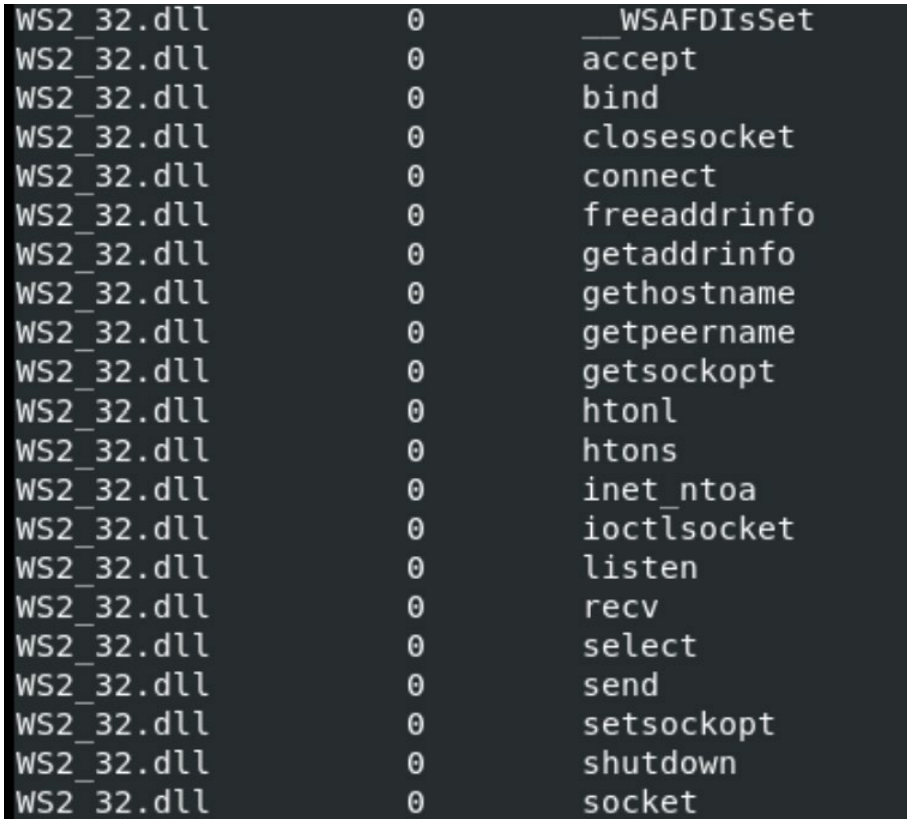
```
WS2_32.dll            0         __WSAFDIsSet
WS2_32.dll            0         accept
WS2_32.dll            0         bind
WS2_32.dll            0         closesocket
WS2_32.dll            0         connect
WS2_32.dll            0         freeaddrinfo
WS2_32.dll            0         getaddrinfo
WS2_32.dll            0         gethostname
WS2_32.dll            0         getpeername
WS2_32.dll            0         getsockopt
WS2_32.dll            0         htonl
WS2_32.dll            0         htons
WS2_32.dll            0         inet_ntoa
WS2_32.dll            0         ioctlsocket
WS2_32.dll            0         listen
WS2_32.dll            0         recv
WS2_32.dll            0         select
WS2_32.dll            0         send
WS2_32.dll            0         setsockopt
WS2_32.dll            0         shutdown
WS2_32.dll            0         socket
ADVAPI32.dll          0         GetUserNameA
ADVAPI32.dll          0         GetUserNameW
ADVAPI32.dll          0         RegCloseKey
ADVAPI32.dll          0         RegCreateKeyExA
ADVAPI32.dll          0         RegDeleteKeyA
ADVAPI32.dll          0         RegEnumKeyExA
ADVAPI32.dll          0         RegOpenKeyExA
ADVAPI32.dll          0         RegQueryValueExA
ADVAPI32.dll          0         RegSetValueExA
SHELL32.dll           0         CommandLineToArgvW
SHELL32.dll           0         ExtractIconExA
SHELL32.dll           0         SHBrowseForFolderW
SHELL32.dll           0         SHGetFileInfoW
SHELL32.dll           0         SHGetFolderPathW
SHELL32.dll           0         SHGetMalloc
SHELL32.dll           0         SHGetPathFromIDListW
SHELL32.dll           0         ShellExecuteW
SHELL32.dll           0         Shell_NotifyIconW
WINMM.dll             0         PlaySoundA
WINMM.dll             0         timeBeginPeriod
WINMM.dll             0         timeGetTime
MPR.dll               0         WNetCloseEnum
MPR.dll               0         WNetEnumResourceW
MPR.dll               0         WNetOpenEnumA
comdlg32.dll          0         CommDlgExtendedError
comdlg32.dll          0         GetOpenFileNameW
comdlg32.dll          0         GetSaveFileNameW
comdlg32.dll          0         PrintDlgA
IMM32.dll             0         ImmAssociateContextEx
IMM32.dll             0         ImmGetCompositionStringA
IMM32.dll             0         ImmGetCompositionStringW
```

vi. 

```
SHELL32.dll          0        SHGetPathFromIDListW
SHELL32.dll          0        ShellExecuteW
SHELL32.dll          0        Shell_NotifyIconW
WINMM.dll            0        PlaySoundA
WINMM.dll            0        timeBeginPeriod
WINMM.dll            0        timeGetTime
MPR.dll              0        WNetCloseEnum
MPR.dll              0        WNetEnumResourceW
MPR.dll              0        WNetOpenEnumA
comdlg32.dll         0        CommDlgExtendedError
comdlg32.dll         0        GetOpenFileNameW
comdlg32.dll         0        GetSaveFileNameW
comdlg32.dll         0        PrintDlgA
IMM32.dll            0        ImmAssociateContextEx
IMM32.dll            0        ImmGetCompositionStringA
IMM32.dll            0        ImmGetCompositionStringW
IMM32.dll            0        ImmGetContext
IMM32.dll            0        ImmGetOpenStatus
IMM32.dll            0        ImmNotifyIME
IMM32.dll            0        ImmReleaseContext
IMM32.dll            0        ImmSetCandidateWindow
USP10.dll            0        ScriptFreeCache
USP10.dll            0        ScriptGetFontProperties
USP10.dll            0        ScriptGetGlyphABCWidth
USP10.dll            0        ScriptItemize
USP10.dll            0        ScriptShape
GDI32.dll            0        AbortDoc
GDI32.dll            0        Arc
GDI32.dll            0        BitBlt
GDI32.dll            0        CloseEnhMetaFile
GDI32.dll            0        CopyEnhMetaFileA
GDI32.dll            0        CreateBitmap
GDI32.dll            0        CreateCompatibleBitmap
GDI32.dll            0        CreateCompatibleDC
GDI32.dll            0        CreateDCA
GDI32.dll            0        CreateDIBSection
GDI32.dll            0        CreateDIBitmap
GDI32.dll            0        CreateEnhMetaFileA
GDI32.dll            0        CreateFontW
GDI32.dll            0        CreateICA
GDI32.dll            0        CreatePalette
GDI32.dll            0        CreatePatternBrush
GDI32.dll            0        CreatePen
GDI32.dll            0        CreateRectRgn
GDI32.dll            0        CreateRectRgnIndirect
GDI32.dll            0        CreateSolidBrush
GDI32.dll            0        DPtoLP
GDI32.dll            0        DeleteDC
GDI32.dll            0        DeleteEnhMetaFile
GDI32.dll            0        DeleteObject
GDI32.dll            0        Ellipse
GDI32.dll            0        EndDoc
```

vii. Analysis:

1. **TimeDateStamp:** 2024-09-26 20:32:00 – The timestamp suggests when the file was compiled. This could be an indicator of when the malware was created or last modified.
2. **WS2_32.dll**

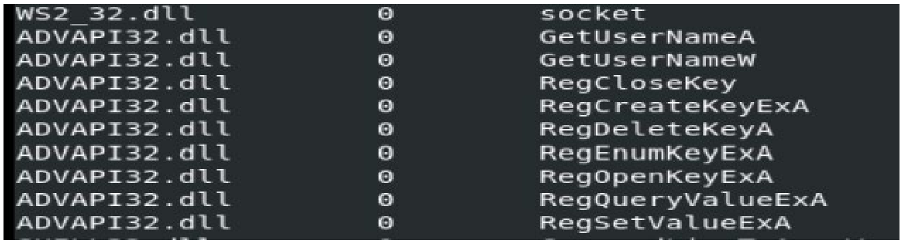
a. 

```
WS2_32.dll          0          __WSAFDIsSet
WS2_32.dll          0          accept
WS2_32.dll          0          bind
WS2_32.dll          0          closesocket
WS2_32.dll          0          connect
WS2_32.dll          0          freeaddrinfo
WS2_32.dll          0          getaddrinfo
WS2_32.dll          0          gethostname
WS2_32.dll          0          getpeername
WS2_32.dll          0          getsockopt
WS2_32.dll          0          htonl
WS2_32.dll          0          htons
WS2_32.dll          0          inet_ntoa
WS2_32.dll          0          ioctlsocket
WS2_32.dll          0          listen
WS2_32.dll          0          recv
WS2_32.dll          0          select
WS2_32.dll          0          send
WS2_32.dll          0          setsockopt
WS2_32.dll          0          shutdown
WS2_32.dll          0          socket
```

b. **Findings:**

   i. The malware imports several functions from the WS2.dll library for network communications. Key giveaways of these include socket, connect, recv, send, bind, and closesocket which suggests the malware can establish and manage network connections. These functions suggest that the malware likely connects to external systems which can allow attackers to control infected machines.

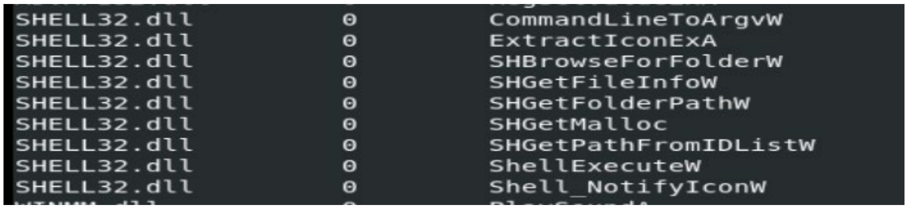
3. **ADVAPI32.dll**

a. 

```
WS2_32.dll          0          socket
ADVAPI32.dll        0          GetUserNameA
ADVAPI32.dll        0          GetUserNameW
ADVAPI32.dll        0          RegCloseKey
ADVAPI32.dll        0          RegCreateKeyExA
ADVAPI32.dll        0          RegDeleteKeyA
ADVAPI32.dll        0          RegEnumKeyExA
ADVAPI32.dll        0          RegOpenKeyExA
ADVAPI32.dll        0          RegQueryValueExA
ADVAPI32.dll        0          RegSetValueExA
```

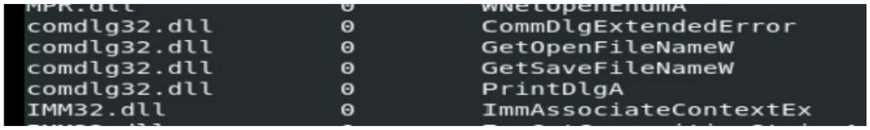
b. **Findings:**

   i. Functions like getUserNameA and W along with RegOpenKeyExA and RegSetValueExA indicate the malware interacts with user account information on Windows and may suggest gathering system/user data to make changes to the registry. This library gives malware access to Windows security functions which can allow the malware to gain more control over the system.

4. **SHELL32.dll**
   a. 

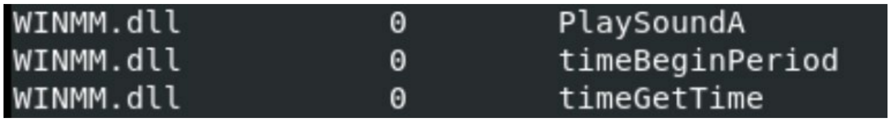
```
SHELL32.dll          0          CommandLineToArgvW
SHELL32.dll          0          ExtractIconExA
SHELL32.dll          0          SHBrowseForFolderW
SHELL32.dll          0          SHGetFileInfoW
SHELL32.dll          0          SHGetFolderPathW
SHELL32.dll          0          SHGetMalloc
SHELL32.dll          0          SHGetPathFromIDListW
SHELL32.dll          0          ShellExecuteW
SHELL32.dll          0          Shell_NotifyIconW
```

   b. **Findings:**
      i. Functions of CommandLineToArgvW, SHGetFileInfoW and ShellExecuteW show interactions with Windows shell which means executing commands, launching files, or even manipulating it.

5. **Comdlg32.dll**
   a. 

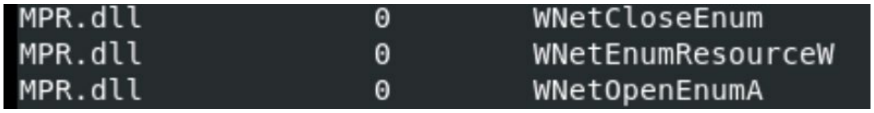
```
comdlg32.dll          0          CommDlgExtendedError
comdlg32.dll          0          GetOpenFileNameW
comdlg32.dll          0          GetSaveFileNameW
comdlg32.dll          0          PrintDlgA
IMM32.dll             0          ImmAssociateContextEx
```

   b. **Findings:**
      i. GetOpenFileNameW, GetSaveFileNameW, and PrintDlgA are used for file dialogs and print functions which suggest the malware may open/save files and intercept print functions.

6. **WINMM.dll**
   a. 

```
WINMM.dll          0          PlaySoundA
WINMM.dll          0          timeBeginPeriod
WINMM.dll          0          timeGetTime
```

   b. **Findings**
      i. These particular import functions are used for managing system time and suggests the malware might be capable of playing sound files and manipulating system timing.

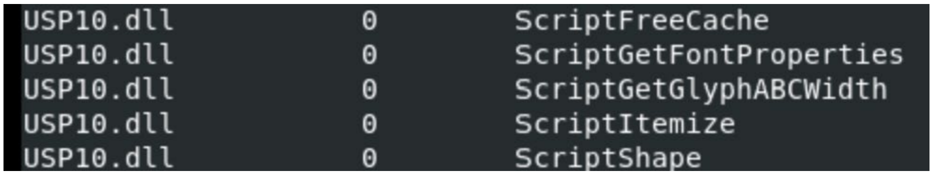
7. **MPR.dll**
   a. 

```
MPR.dll          0          WNetCloseEnum
MPR.dll          0          WNetEnumResourceW
MPR.dll          0          WNetOpenEnumA
```

   b. **Findings:**

        i. These functions are associated with network resource management and can suggest that the malware may be designed to explore network shares or access for spreading or collecting data.

8. **USP10.dll**

    a. 

```
USP10.dll          0          ScriptFreeCache
USP10.dll          0          ScriptGetFontProperties
USP10.dll          0          ScriptGetGlyphABCWidth
USP10.dll          0          ScriptItemize
USP10.dll          0          ScriptShape
```

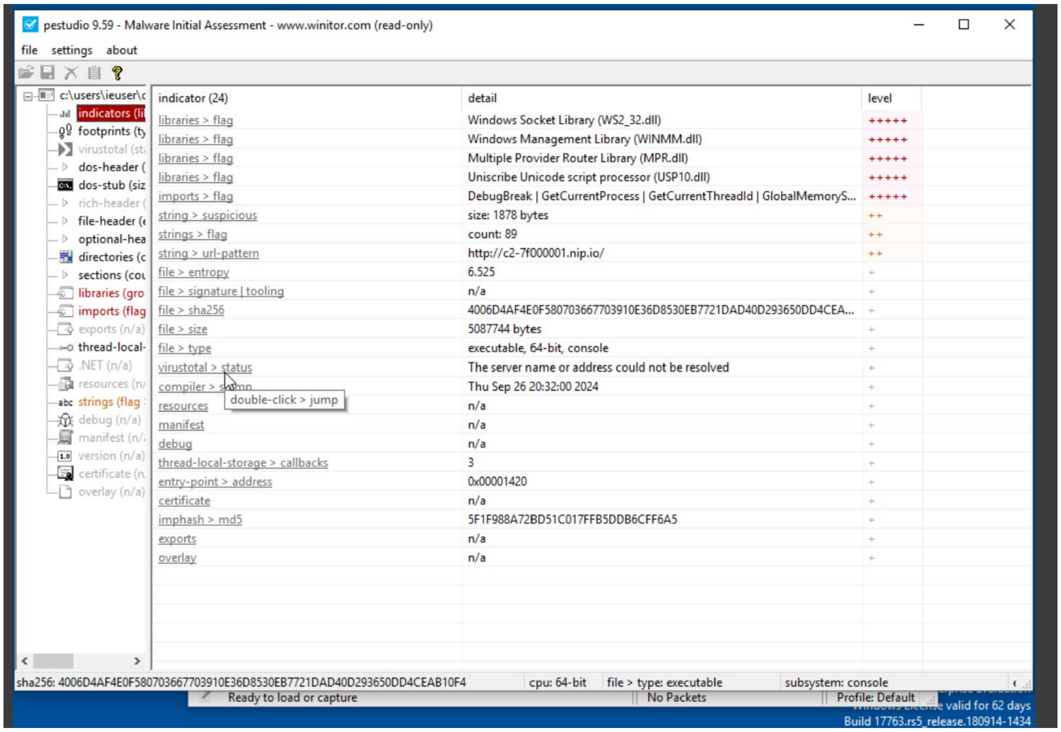
    b. **Findings:**

        i. These functions are related to a set of APIs for text shaping and rendering which handles text layout, font properties, and glyph shaping. This indicates that the malware might involve manipulation or rendering text to display fonts or characters.

2. Windows 10

    a. PeStudio

        i. **Indicators**

        ii. 

pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

indicator (24)	detail	level
libraries > flag	Windows Socket Library (WS2_32.dll)	+++++
libraries > flag	Windows Management Library (WINMM.dll)	+++++
libraries > flag	Multiple Provider Router Library (MPR.dll)	+++++
libraries > flag	Uniscribe Unicode script processor (USP10.dll)	+++++
imports > flag	DebugBreak | GetCurrentProcess | GetCurrentThreadId | GlobalMemoryS...	+++++
string > suspicious	size: 1878 bytes	++
strings > flag	count: 89	++
string > url-pattern	http://c2-7f000001.nip.io/	++
file > entropy	6.525	+
file > signature | tooling	n/a	+
file > sha256	4006D4AF4E0F580703667703910E36D8530EB7721DAD40D293650DD4CEA...	+
file > size	5087744 bytes	+
file > type	executable, 64-bit, console	+
virustotal > status	The server name or address could not be resolved	+
compiler > stamp	Thu Sep 26 20:32:00 2024	+
resources	n/a	+
manifest	n/a	+
debug	n/a	+
thread-local-storage > callbacks	3	+
entry-point > address	0x00001420	+
certificate	n/a	+
imphash > md5	5F1F988A72BD51C017FFB5DDB6CFF6A5	+
exports	n/a	+
overlay	n/a	+

sha256: 4006D4AF4E0F580703667703910E36D8530EB7721DAD40D293650DD4CEAB10F4 | cpu: 64-bit | file > type: executable | subsystem: console

Ready to load or capture | No Packets | Profile: Default

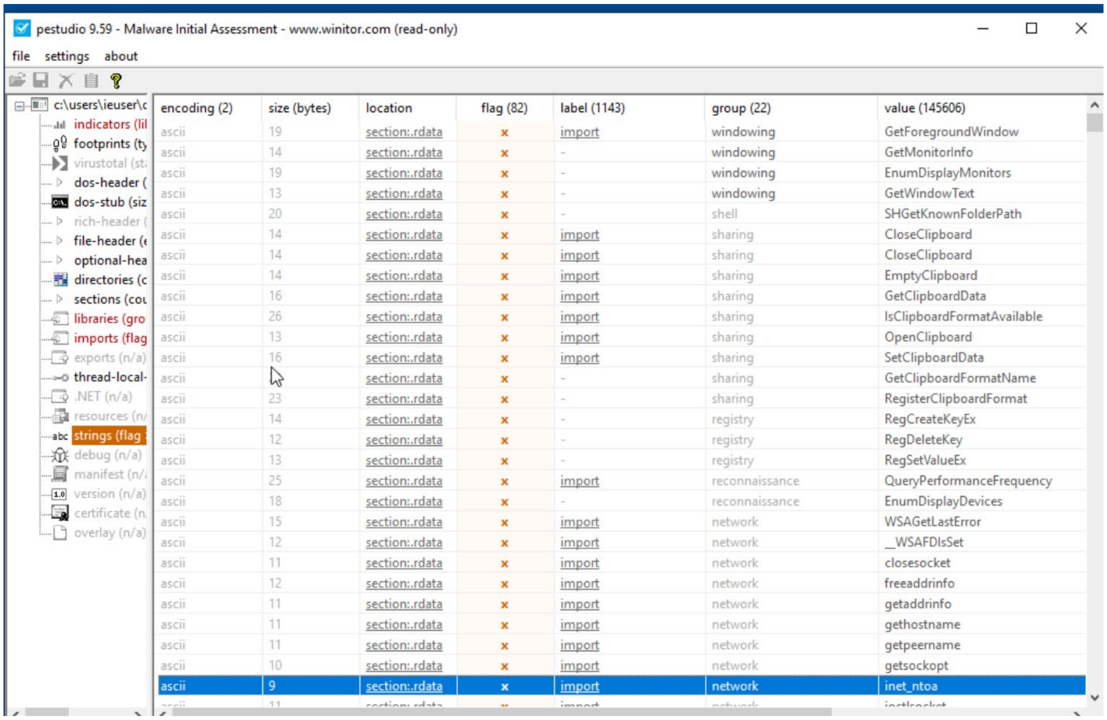
valid for 62 days
Build 17763.rs5_release.180914-1434

        iii. **Findings:**

            1. Several concerning indicators identified by the first five red flags denote high threat levels. The malware utilizes multiple

critical libraries including WS2_32.dll for network communication, WINMM.dll for multimedia function, and MPR.dll for network resource management. Additionally, there is a suspicious URL pattern http://c2-7f000001.nip.io/ that can indicate a C2 server communication and the file size of 1878 bytes and a total of 89 imports further reveal the compact and potentially efficient payload of this malware.

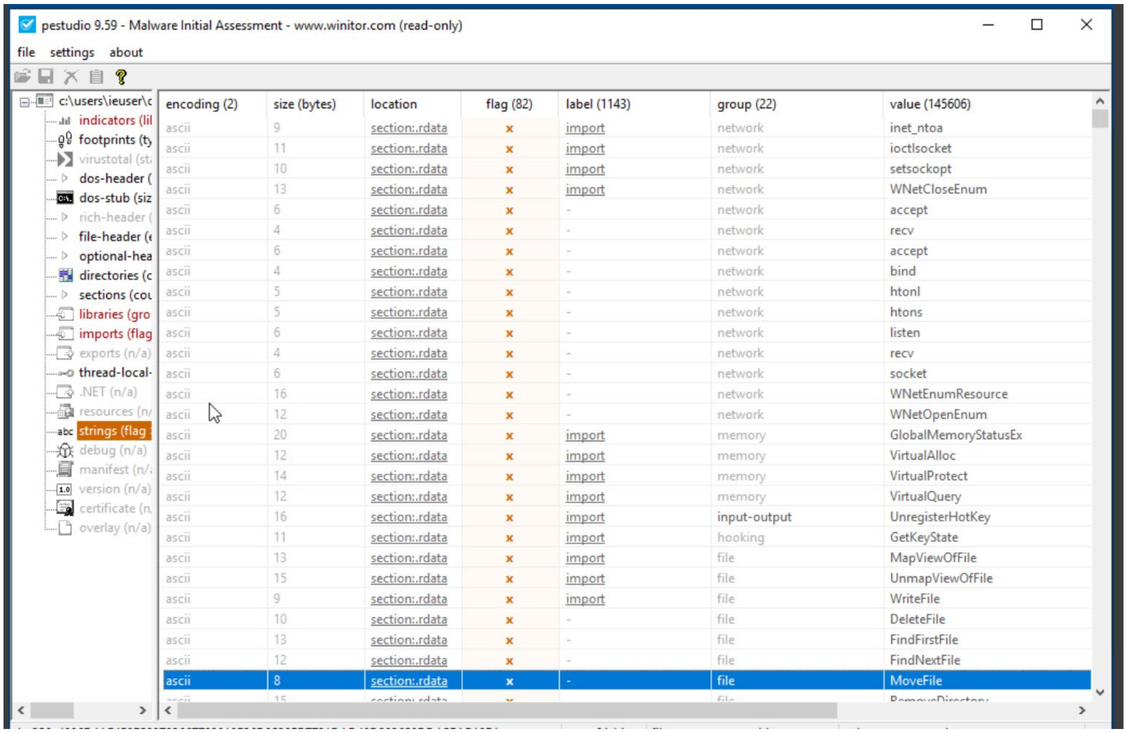
iv. **Strings**



encoding (2)	size (bytes)	location	flag (82)	label (1143)	group (22)	value (145606)
ascii	19	section:.rdata	x	import	windowing	GetForegroundWindow
ascii	14	section:.rdata	x	-	windowing	GetMonitorInfo
ascii	19	section:.rdata	x	-	windowing	EnumDisplayMonitors
ascii	13	section:.rdata	x	-	windowing	GetWindowText
ascii	20	section:.rdata	x	-	shell	SHGetKnownFolderPath
ascii	14	section:.rdata	x	import	sharing	CloseClipboard
ascii	14	section:.rdata	x	import	sharing	CloseClipboard
ascii	14	section:.rdata	x	import	sharing	EmptyClipboard
ascii	16	section:.rdata	x	import	sharing	GetClipboardData
ascii	26	section:.rdata	x	import	sharing	IsClipboardFormatAvailable
ascii	13	section:.rdata	x	import	sharing	OpenClipboard
ascii	16	section:.rdata	x	import	sharing	SetClipboardData
ascii		section:.rdata	x	-	sharing	GetClipboardFormatName
ascii	23	section:.rdata	x	-	sharing	RegisterClipboardFormat
ascii	14	section:.rdata	x	-	registry	RegCreateKeyEx
ascii	12	section:.rdata	x	-	registry	RegDeleteKey
ascii	13	section:.rdata	x	-	registry	RegSetValueEx
ascii	25	section:.rdata	x	import	reconnaissance	QueryPerformanceFrequency
ascii	18	section:.rdata	x	-	reconnaissance	EnumDisplayDevices
ascii	15	section:.rdata	x	import	network	WSAGetLastError
ascii	12	section:.rdata	x	import	network	__WSAFDIsSet
ascii	11	section:.rdata	x	import	network	closesocket
ascii	12	section:.rdata	x	import	network	freeaddrinfo
ascii	11	section:.rdata	x	import	network	getaddrinfo
ascii	11	section:.rdata	x	import	network	gethostname
ascii	11	section:.rdata	x	import	network	getpeername
ascii	10	section:.rdata	x	import	network	getsockopt
ascii	9	section:.rdata	x	import	network	inet_ntoa
ascii	11	section:.rdata	x	import	network	ioctlsocket

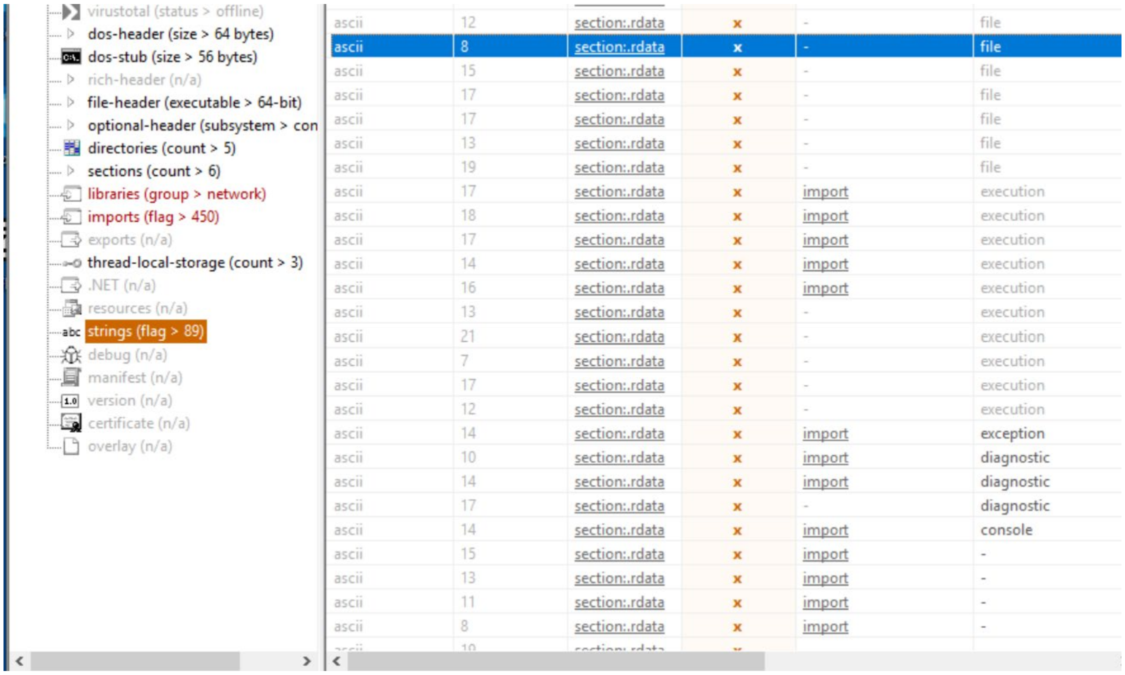
v.

vi.

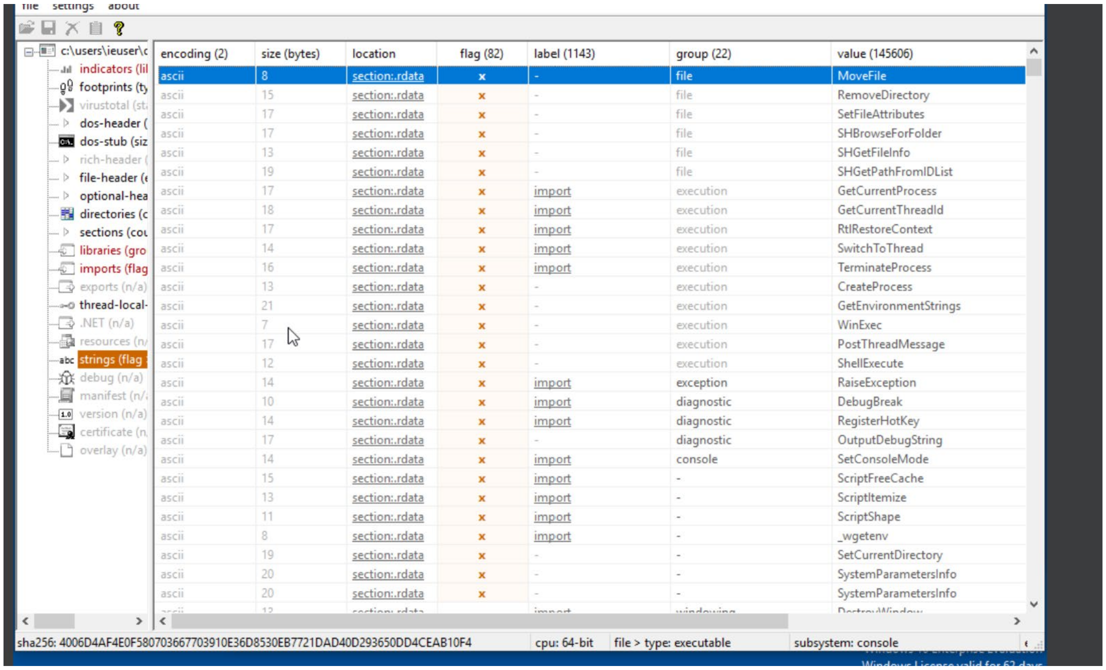


encoding (2)	size (bytes)	location	flag (82)	label (1143)	group (22)	value (145606)
ascii	9	section:.rdata	x	import	network	inet_ntoa
ascii	11	section:.rdata	x	import	network	ioctlsocket
ascii	10	section:.rdata	x	import	network	setsockopt
ascii	13	section:.rdata	x	import	network	WNetCloseEnum
ascii	6	section:.rdata	x	-	network	accept
ascii	4	section:.rdata	x	-	network	recv
ascii	6	section:.rdata	x	-	network	accept
ascii	4	section:.rdata	x	-	network	bind
ascii	5	section:.rdata	x	-	network	htonl
ascii	5	section:.rdata	x	-	network	htons
ascii	6	section:.rdata	x	-	network	listen
ascii	4	section:.rdata	x	-	network	recv
ascii	6	section:.rdata	x	-	network	socket
ascii	16	section:.rdata	x	-	network	WNetEnumResource
ascii	12	section:.rdata	x	-	network	WNetOpenEnum
ascii	20	section:.rdata	x	import	memory	GlobalMemoryStatusEx
ascii	12	section:.rdata	x	import	memory	VirtualAlloc
ascii	14	section:.rdata	x	import	memory	VirtualProtect
ascii	12	section:.rdata	x	import	memory	VirtualQuery
ascii	16	section:.rdata	x	import	input-output	UnregisterHotKey
ascii	11	section:.rdata	x	import	hooking	GetKeyState
ascii	13	section:.rdata	x	import	file	MapViewOfFile
ascii	15	section:.rdata	x	import	file	UnmapViewOfFile
ascii	9	section:.rdata	x	import	file	WriteFile
ascii	10	section:.rdata	x	-	file	DeleteFile
ascii	13	section:.rdata	x	-	file	FindFirstFile
ascii	12	section:.rdata	x	-	file	FindNextFile
ascii	8	section:.rdata	x	-	file	MoveFile

vii.


virustotal (status > offline)
dos-header (size > 64 bytes)
dos-stub (size > 56 bytes)
rich-header (n/a)
file-header (executable > 64-bit)
optional-header (subsystem > con
directories (count > 5)
sections (count > 6)
libraries (group > network)
imports (flag > 450)
exports (n/a)
thread-local-storage (count > 3)
.NET (n/a)
resources (n/a)
strings (flag > 89)
debug (n/a)
manifest (n/a)
version (n/a)
certificate (n/a)
overlay (n/a)

ascii	12	section:.rdata	x	-	file
ascii	8	section:.rdata	x	-	file
ascii	15	section:.rdata	x	-	file
ascii	17	section:.rdata	x	-	file
ascii	17	section:.rdata	x	-	file
ascii	13	section:.rdata	x	-	file
ascii	19	section:.rdata	x	-	file
ascii	17	section:.rdata	x	import	execution
ascii	18	section:.rdata	x	import	execution
ascii	17	section:.rdata	x	import	execution
ascii	14	section:.rdata	x	import	execution
ascii	16	section:.rdata	x	import	execution
ascii	13	section:.rdata	x	-	execution
ascii	21	section:.rdata	x	-	execution
ascii	7	section:.rdata	x	-	execution
ascii	17	section:.rdata	x	-	execution
ascii	12	section:.rdata	x	-	execution
ascii	14	section:.rdata	x	import	exception
ascii	10	section:.rdata	x	import	diagnostic
ascii	14	section:.rdata	x	import	diagnostic
ascii	17	section:.rdata	x	-	diagnostic
ascii	14	section:.rdata	x	import	console
ascii	15	section:.rdata	x	import	-
ascii	13	section:.rdata	x	import	-
ascii	11	section:.rdata	x	import	-
ascii	8	section:.rdata	x	import	-

viii. 

encoding (2)	size (bytes)	location	flag (82)	label (1143)	group (22)	value (145606)
ascii	8	section:.rdata	x	-	file	MoveFile
ascii	15	section:.rdata	x	-	file	RemoveDirectory
ascii	17	section:.rdata	x	-	file	SetFileAttributes
ascii	17	section:.rdata	x	-	file	SHBrowseForFolder
ascii	13	section:.rdata	x	-	file	SHGetFileInfo
ascii	19	section:.rdata	x	-	file	SHGetPathFromIDList
ascii	17	section:.rdata	x	import	execution	GetCurrentProcess
ascii	18	section:.rdata	x	import	execution	GetCurrentThreadId
ascii	17	section:.rdata	x	import	execution	RtlRestoreContext
ascii	14	section:.rdata	x	import	execution	SwitchToThread
ascii	16	section:.rdata	x	import	execution	TerminateProcess
ascii	13	section:.rdata	x	-	execution	CreateProcess
ascii	21	section:.rdata	x	-	execution	GetEnvironmentStrings
ascii	7	section:.rdata	x	-	execution	WinExec
ascii	17	section:.rdata	x	-	execution	PostThreadMessage
ascii	12	section:.rdata	x	-	execution	ShellExecute
ascii	14	section:.rdata	x	import	exception	RaiseException
ascii	10	section:.rdata	x	import	diagnostic	DebugBreak
ascii	14	section:.rdata	x	import	diagnostic	RegisterHotKey
ascii	17	section:.rdata	x	-	diagnostic	OutputDebugString
ascii	14	section:.rdata	x	import	console	SetConsoleMode
ascii	15	section:.rdata	x	import	-	ScriptFreeCache
ascii	13	section:.rdata	x	import	-	ScriptItemize
ascii	11	section:.rdata	x	import	-	ScriptShape
ascii	8	section:.rdata	x	import	-	_wgetenv
ascii	19	section:.rdata	x	-	-	SetCurrentDirectory
ascii	20	section:.rdata	x	-	-	SystemParametersInfo
ascii	20	section:.rdata	x	-	-	SystemParametersInfo

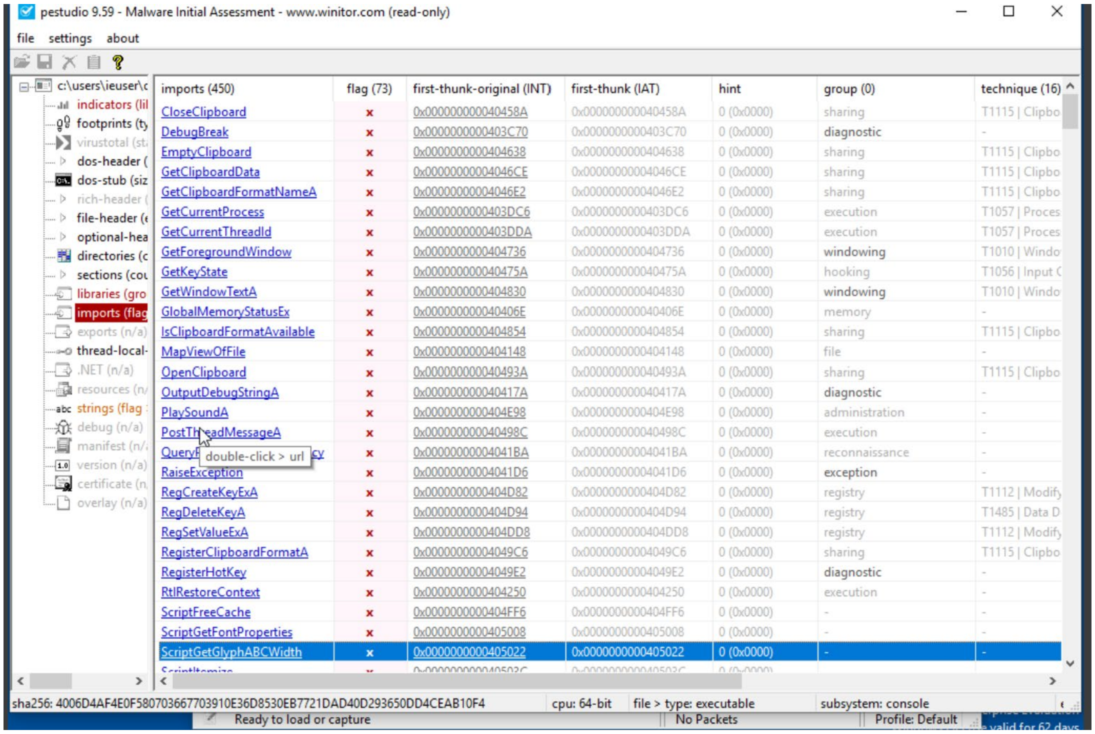
sha256: 4006D4AF4E0F580703667703910E36D8530EB7721DAD40D293650DD4CEAB10F4 | cpu: 64-bit | file > type: executable | subsystem: console

ix. Findings:

1. Some peculiar import statements emphasize the malware’s reliance on key Windows functions. Like openclipboard, getclipboarddata, and setclipboarddata imply a potential clipboard or data exfiltration. The inclusion of getaddrinfo, closesocket, freeaddrinfo allows the malware to perform network communications possibly for data reconnaissance and manipulation. These functions suggest that the malware might intercept sensitive data copied by the user such as passwords.

x. Imports

xi.

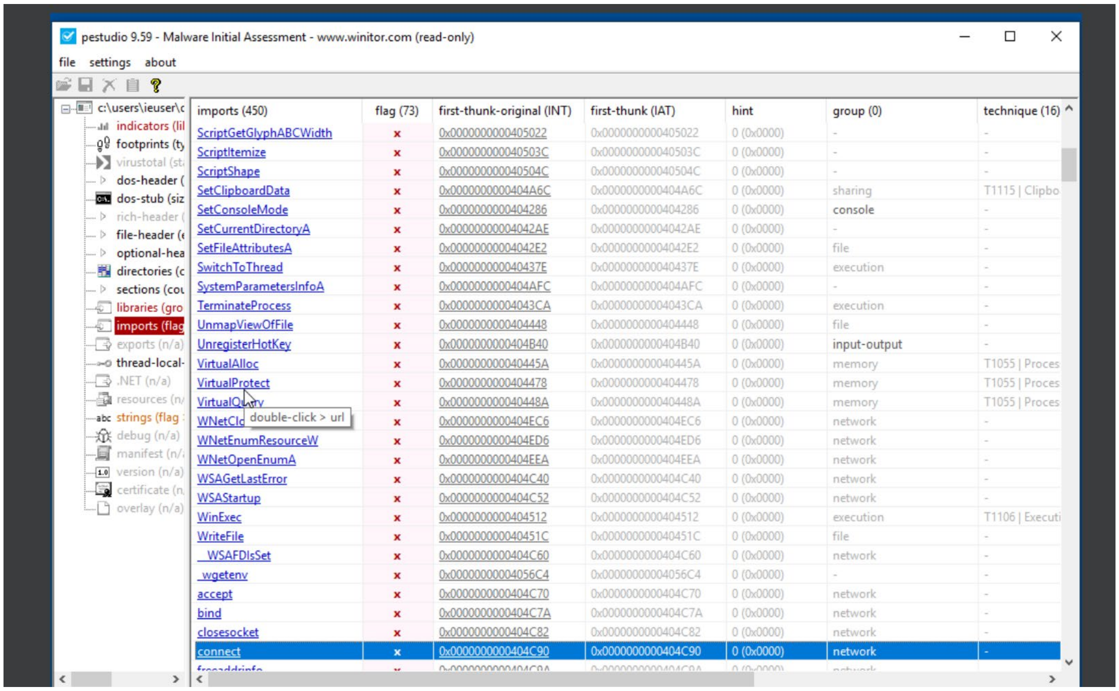


imports (450)	flag (73)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (0)	technique (16)
CloseClipboard	x	0x000000000040458A	0x000000000040458A	0 (0x0000)	sharing	T1115 | Clipbo
DebugBreak	x	0x0000000000403C70	0x0000000000403C70	0 (0x0000)	diagnostic	-
EmptyClipboard	x	0x0000000000404638	0x0000000000404638	0 (0x0000)	sharing	T1115 | Clipbo
GetClipboardData	x	0x00000000004046CE	0x00000000004046CE	0 (0x0000)	sharing	T1115 | Clipbo
GetClipboardFormatNameA	x	0x00000000004046E2	0x00000000004046E2	0 (0x0000)	sharing	T1115 | Clipbo
GetCurrentProcess	x	0x0000000000403DC6	0x0000000000403DC6	0 (0x0000)	execution	T1057 | Proces
GetCurrentThreadId	x	0x0000000000403DDA	0x0000000000403DDA	0 (0x0000)	execution	T1057 | Proces
GetForegroundWindow	x	0x0000000000404736	0x0000000000404736	0 (0x0000)	windowing	T1010 | Windo
GetKeyState	x	0x000000000040475A	0x000000000040475A	0 (0x0000)	hooking	T1056 | Input C
GetWindowTextA	x	0x0000000000404830	0x0000000000404830	0 (0x0000)	windowing	T1010 | Windo
GlobalMemoryStatusEx	x	0x000000000040406E	0x000000000040406E	0 (0x0000)	memory	-
IsClipboardFormatAvailable	x	0x0000000000404854	0x0000000000404854	0 (0x0000)	sharing	T1115 | Clipbo
MapViewOfFile	x	0x0000000000404148	0x0000000000404148	0 (0x0000)	file	-
OpenClipboard	x	0x000000000040493A	0x000000000040493A	0 (0x0000)	sharing	T1115 | Clipbo
OutputDebugStringA	x	0x000000000040417A	0x000000000040417A	0 (0x0000)	diagnostic	-
PlaySoundA	x	0x0000000000404E98	0x0000000000404E98	0 (0x0000)	administration	-
PostThreadMessageA	x	0x000000000040498C	0x000000000040498C	0 (0x0000)	execution	-
QueryP cy	x	0x00000000004041BA	0x00000000004041BA	0 (0x0000)	reconnaissance	-
RaiseException	x	0x00000000004041D6	0x00000000004041D6	0 (0x0000)	exception	-
RegCreateKeyExA	x	0x0000000000404D82	0x0000000000404D82	0 (0x0000)	registry	T1112 | Modify
RegDeleteKeyA	x	0x0000000000404D94	0x0000000000404D94	0 (0x0000)	registry	T1485 | Data D
RegSetValueExA	x	0x0000000000404DD8	0x0000000000404DD8	0 (0x0000)	registry	T1112 | Modify
RegisterClipboardFormatA	x	0x00000000004049C6	0x00000000004049C6	0 (0x0000)	sharing	T1115 | Clipbo
RegisterHotKey	x	0x00000000004049E2	0x00000000004049E2	0 (0x0000)	diagnostic	-
RtlRestoreContext	x	0x0000000000404250	0x0000000000404250	0 (0x0000)	execution	-
ScriptFreeCache	x	0x0000000000404FF6	0x0000000000404FF6	0 (0x0000)	-	-
ScriptGetFontProperties	x	0x0000000000405008	0x0000000000405008	0 (0x0000)	-	-
ScriptGetGlyphABCWidth	x	0x0000000000405022	0x0000000000405022	0 (0x0000)	-	-

sha256: 4006D4AF4E0F580703667703910E36D8530EB7721DAD40D293650DD4CEAB10F4 | cpu: 64-bit | file > type: executable | subsystem: console

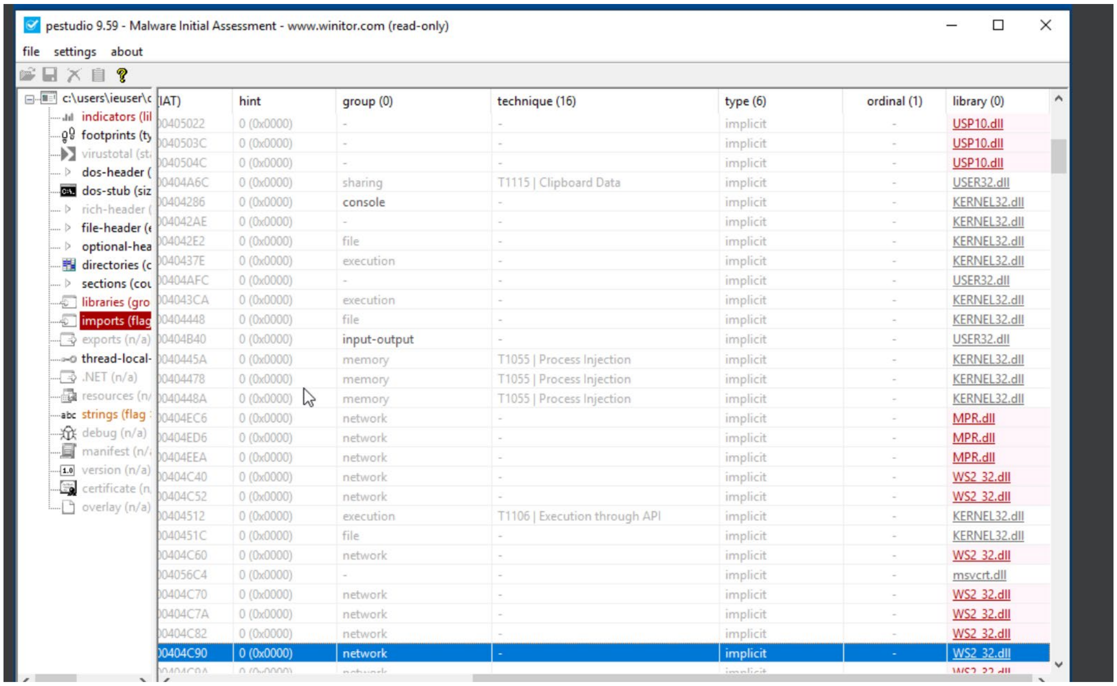
Ready to load or capture | No Packets | Profile: Default

xii.



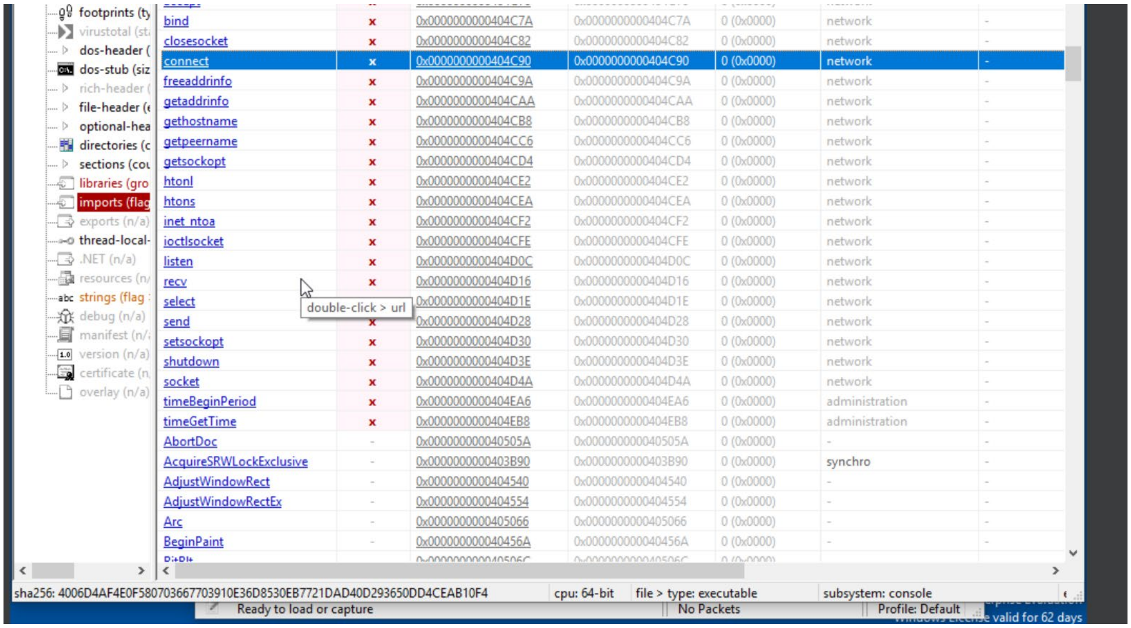
imports (450)	flag (73)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (0)	technique (16)
ScriptGetGlyphABCWidth	x	0x0000000000405022	0x0000000000405022	0 (0x0000)	-	-
ScriptItemize	x	0x000000000040503C	0x000000000040503C	0 (0x0000)	-	-
ScriptShape	x	0x000000000040504C	0x000000000040504C	0 (0x0000)	-	-
SetClipboardData	x	0x0000000000404A6C	0x0000000000404A6C	0 (0x0000)	sharing	T1115 | Clipbo
SetConsoleMode	x	0x0000000000404286	0x0000000000404286	0 (0x0000)	console	-
SetCurrentDirectoryA	x	0x00000000004042AE	0x00000000004042AE	0 (0x0000)	-	-
SetFileAttributesA	x	0x00000000004042E2	0x00000000004042E2	0 (0x0000)	file	-
SwitchToThread	x	0x000000000040437E	0x000000000040437E	0 (0x0000)	execution	-
SystemParametersInfoA	x	0x0000000000404AFC	0x0000000000404AFC	0 (0x0000)	-	-
TerminateProcess	x	0x00000000004043CA	0x00000000004043CA	0 (0x0000)	execution	-
UnmapViewOfFile	x	0x0000000000404448	0x0000000000404448	0 (0x0000)	file	-
UnregisterHotKey	x	0x0000000000404B40	0x0000000000404B40	0 (0x0000)	input-output	-
VirtualAlloc	x	0x000000000040445A	0x000000000040445A	0 (0x0000)	memory	T1055 | Proces
VirtualProtect	x	0x0000000000404478	0x0000000000404478	0 (0x0000)	memory	T1055 | Proces
VirtualQuery	x	0x000000000040448A	0x000000000040448A	0 (0x0000)	memory	T1055 | Proces
WNetClo	x	0x0000000000404EC6	0x0000000000404EC6	0 (0x0000)	network	-
WNetEnumResourceW	x	0x0000000000404ED6	0x0000000000404ED6	0 (0x0000)	network	-
WNetOpenEnumA	x	0x0000000000404EEA	0x0000000000404EEA	0 (0x0000)	network	-
WSAGetLastError	x	0x0000000000404C40	0x0000000000404C40	0 (0x0000)	network	-
WSAStartup	x	0x0000000000404C52	0x0000000000404C52	0 (0x0000)	network	-
WinExec	x	0x0000000000404512	0x0000000000404512	0 (0x0000)	execution	T1106 | Executi
WriteFile	x	0x000000000040451C	0x000000000040451C	0 (0x0000)	file	-
__WSAFDIsSet	x	0x0000000000404C60	0x0000000000404C60	0 (0x0000)	network	-
_wgetenv	x	0x00000000004056C4	0x00000000004056C4	0 (0x0000)	-	-
accept	x	0x0000000000404C70	0x0000000000404C70	0 (0x0000)	network	-
bind	x	0x0000000000404C7A	0x0000000000404C7A	0 (0x0000)	network	-
closesocket	x	0x0000000000404C82	0x0000000000404C82	0 (0x0000)	network	-
connect	x	0x0000000000404C90	0x0000000000404C90	0 (0x0000)	network	-

xiii.



(IAT)	hint	group (0)	technique (16)	type (6)	ordinal (1)	library (0)
00405022	0 (0x0000)	-	-	implicit	-	USP10.dll
0040503C	0 (0x0000)	-	-	implicit	-	USP10.dll
0040504C	0 (0x0000)	-	-	implicit	-	USP10.dll
00404A6C	0 (0x0000)	sharing	T1115 | Clipboard Data	implicit	-	USER32.dll
00404286	0 (0x0000)	console	-	implicit	-	KERNEL32.dll
004042AE	0 (0x0000)	-	-	implicit	-	KERNEL32.dll
004042E2	0 (0x0000)	file	-	implicit	-	KERNEL32.dll
0040437E	0 (0x0000)	execution	-	implicit	-	KERNEL32.dll
00404AFC	0 (0x0000)	-	-	implicit	-	USER32.dll
004043CA	0 (0x0000)	execution	-	implicit	-	KERNEL32.dll
00404448	0 (0x0000)	file	-	implicit	-	KERNEL32.dll
00404B40	0 (0x0000)	input-output	-	implicit	-	USER32.dll
0040445A	0 (0x0000)	memory	T1055 | Process Injection	implicit	-	KERNEL32.dll
00404478	0 (0x0000)	memory	T1055 | Process Injection	implicit	-	KERNEL32.dll
0040448A	0 (0x0000)	memory	T1055 | Process Injection	implicit	-	KERNEL32.dll
00404EC6	0 (0x0000)	network	-	implicit	-	MPR.dll
00404ED6	0 (0x0000)	network	-	implicit	-	MPR.dll
00404EEA	0 (0x0000)	network	-	implicit	-	MPR.dll
00404C40	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404C52	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404512	0 (0x0000)	execution	T1106 | Execution through API	implicit	-	KERNEL32.dll
0040451C	0 (0x0000)	file	-	implicit	-	KERNEL32.dll
00404C60	0 (0x0000)	network	-	implicit	-	WS2_32.dll
004056C4	0 (0x0000)	-	-	implicit	-	msvcrt.dll
00404C70	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404C7A	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404C82	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404C90	0 (0x0000)	network	-	implicit	-	WS2_32.dll

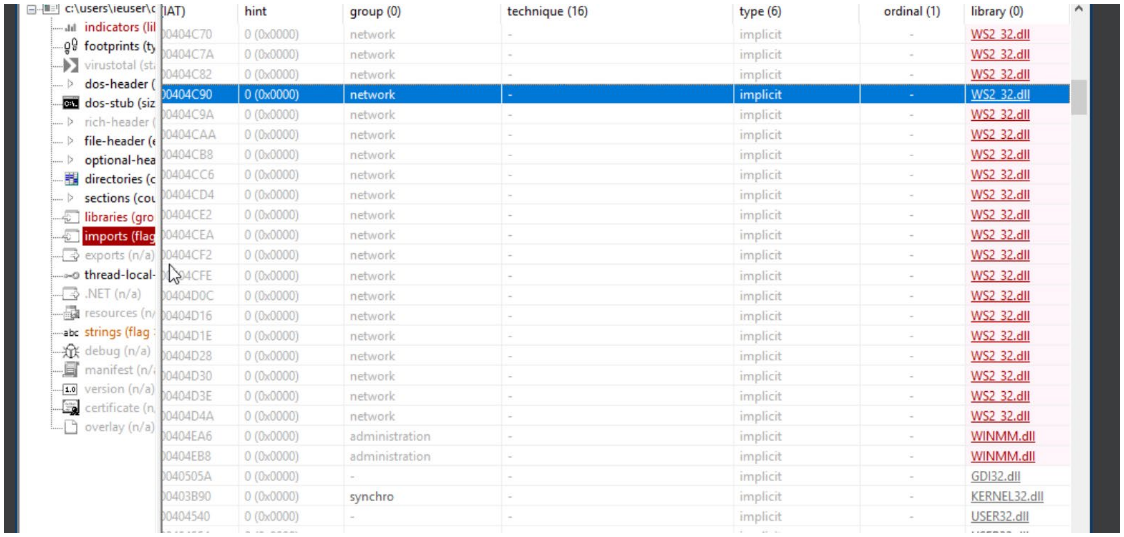
xiv.



bind	x	0x0000000000404C7A	0x0000000000404C7A	0 (0x0000)	network	-
closesocket	x	0x0000000000404C82	0x0000000000404C82	0 (0x0000)	network	-
connect	x	0x0000000000404C90	0x0000000000404C90	0 (0x0000)	network	-
freeaddrinfo	x	0x0000000000404C9A	0x0000000000404C9A	0 (0x0000)	network	-
getaddrinfo	x	0x0000000000404CAA	0x0000000000404CAA	0 (0x0000)	network	-
gethostname	x	0x0000000000404CB8	0x0000000000404CB8	0 (0x0000)	network	-
getpeername	x	0x0000000000404CC6	0x0000000000404CC6	0 (0x0000)	network	-
getsockopt	x	0x0000000000404CD4	0x0000000000404CD4	0 (0x0000)	network	-
htonl	x	0x0000000000404CE2	0x0000000000404CE2	0 (0x0000)	network	-
htons	x	0x0000000000404CEA	0x0000000000404CEA	0 (0x0000)	network	-
inet_ntoa	x	0x0000000000404CF2	0x0000000000404CF2	0 (0x0000)	network	-
ioctlsocket	x	0x0000000000404CFE	0x0000000000404CFE	0 (0x0000)	network	-
listen	x	0x0000000000404D0C	0x0000000000404D0C	0 (0x0000)	network	-
recv	x	0x0000000000404D16	0x0000000000404D16	0 (0x0000)	network	-
select	x	0x0000000000404D1E	0x0000000000404D1E	0 (0x0000)	network	-
send	x	0x0000000000404D28	0x0000000000404D28	0 (0x0000)	network	-
setsockopt	x	0x0000000000404D30	0x0000000000404D30	0 (0x0000)	network	-
shutdown	x	0x0000000000404D3E	0x0000000000404D3E	0 (0x0000)	network	-
socket	x	0x0000000000404D4A	0x0000000000404D4A	0 (0x0000)	network	-
timeBeginPeriod	x	0x0000000000404EA6	0x0000000000404EA6	0 (0x0000)	administration	-
timeGetTime	x	0x0000000000404EB8	0x0000000000404EB8	0 (0x0000)	administration	-
AbortDoc	-	0x000000000040505A	0x000000000040505A	0 (0x0000)	-	-
AcquireSRWLockExclusive	-	0x0000000000403B90	0x0000000000403B90	0 (0x0000)	synchro	-
AdjustWindowRect	-	0x0000000000404540	0x0000000000404540	0 (0x0000)	-	-
AdjustWindowRectEx	-	0x0000000000404554	0x0000000000404554	0 (0x0000)	-	-
Arc	-	0x0000000000405066	0x0000000000405066	0 (0x0000)	-	-
BeginPaint	-	0x000000000040456A	0x000000000040456A	0 (0x0000)	-	-

sha256: 4006D4AF4E0F580703667703910E36D8530EB7721DAD40D293650DD4CEAB10F4 | cpu: 64-bit | file > type: executable | subsystem: console

Ready to load or capture | No Packets | Profile: Default

xv. 

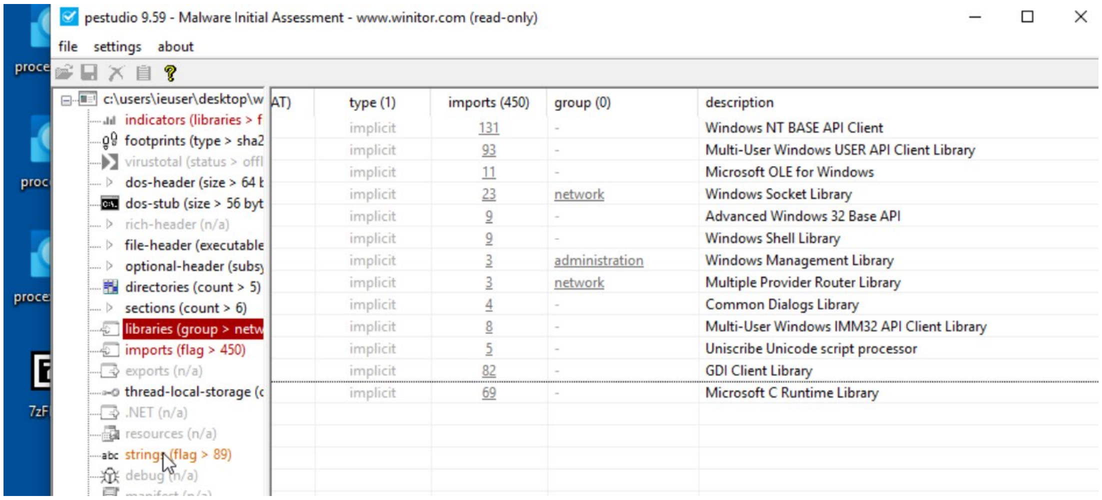
```
c:\users\ieuser\c
  indicators (lil
  footprints (ty
  virustotal (st
  dos-header (
  dos-stub (siz
  rich-header (
  file-header (e
  optional-hea
  directories (c
  sections (cou
  libraries (gro
  imports (flag
  exports (n/a)
  thread-local-
  .NET (n/a)
  resources (n/
  strings (flag
  debug (n/a)
  manifest (n/
  version (n/a)
  certificate (n
  overlay (n/a)
```

IAT)	hint	group (0)	technique (16)	type (6)	ordinal (1)	library (0)
00404C70	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404C7A	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404C82	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404C90	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404C9A	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404CAA	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404CB8	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404CC6	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404CD4	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404CE2	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404CEA	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404CF2	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404CFE	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404D0C	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404D16	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404D1E	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404D28	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404D30	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404D3E	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404D4A	0 (0x0000)	network	-	implicit	-	WS2_32.dll
00404EA6	0 (0x0000)	administration	-	implicit	-	WINMM.dll
00404EB8	0 (0x0000)	administration	-	implicit	-	WINMM.dll
0040505A	0 (0x0000)	-	-	implicit	-	GDI32.dll
00403B90	0 (0x0000)	synchro	-	implicit	-	KERNEL32.dll
00404540	0 (0x0000)	-	-	implicit	-	USER32.dll

xvi. **Findings:**

1. All these imports further show the evidence of the network and data manipulation of the malware from the important dll library that allows these imports to function.

xvii. **Libraries**

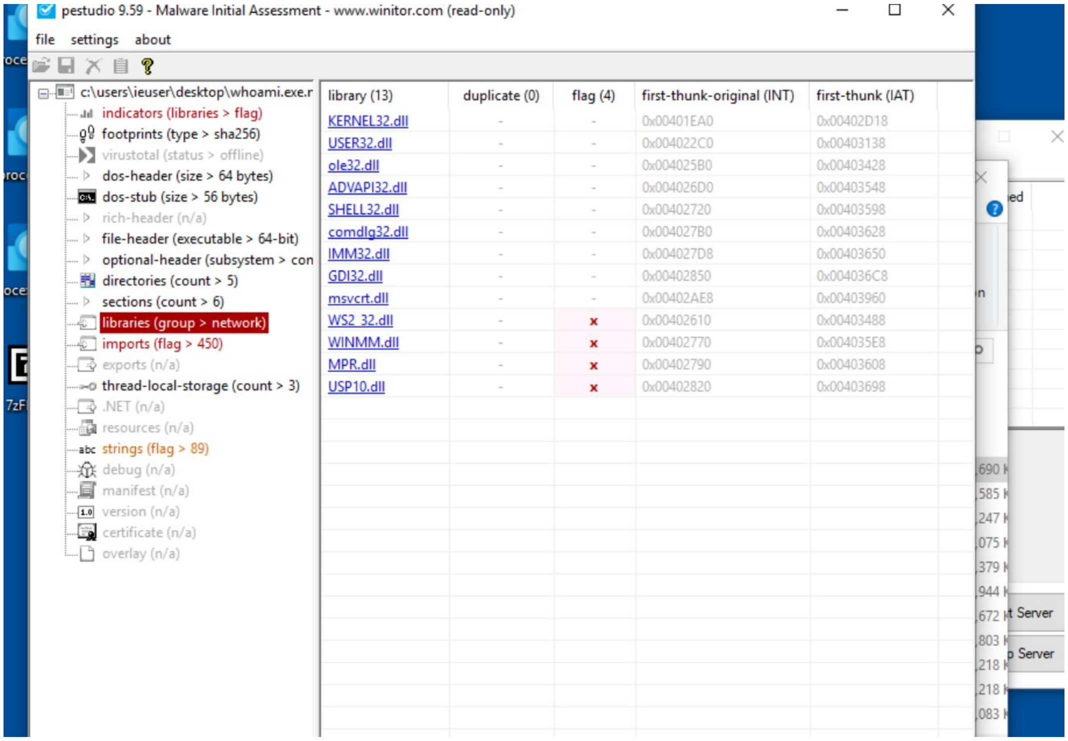
xviii. 

pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)

```
c:\users\ieuser\desktop\w
  indicators (libraries > f
  footprints (type > sha2
  virustotal (status > offl
  dos-header (size > 64 b
  dos-stub (size > 56 byt
  rich-header (n/a)
  file-header (executable
  optional-header (subsy
  directories (count > 5)
  sections (count > 6)
  libraries (group > netw
  imports (flag > 450)
  exports (n/a)
  thread-local-storage (c
  .NET (n/a)
  resources (n/a)
  strings (flag > 89)
  debug (n/a)
```

AT)	type (1)	imports (450)	group (0)	description
	implicit	131	-	Windows NT BASE API Client
	implicit	93	-	Multi-User Windows USER API Client Library
	implicit	11	-	Microsoft OLE for Windows
	implicit	23	network	Windows Socket Library
	implicit	9	-	Advanced Windows 32 Base API
	implicit	9	-	Windows Shell Library
	implicit	3	administration	Windows Management Library
	implicit	3	network	Multiple Provider Router Library
	implicit	4	-	Common Dialogs Library
	implicit	8	-	Multi-User Windows IMM32 API Client Library
	implicit	5	-	Uniscribe Unicode script processor
	implicit	82	-	GDI Client Library
	implicit	69	-	Microsoft C Runtime Library

xix.


pestudio 9.59 - Malware Initial Assessment - www.winitor.com (read-only)
file
settings
about

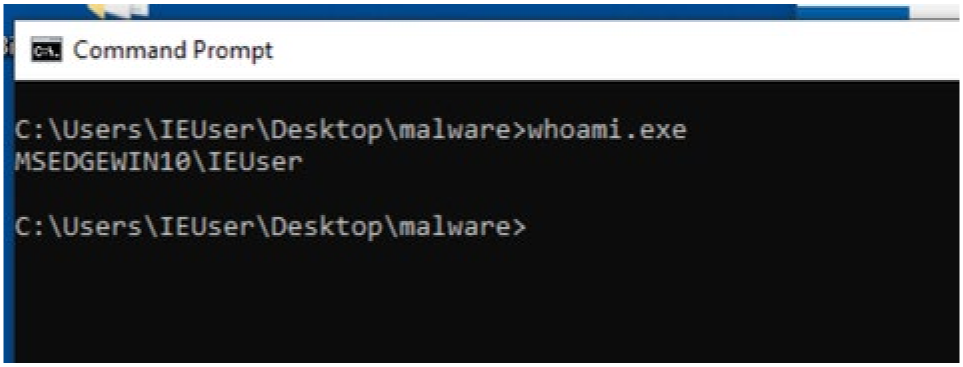
- c:\users\ieuser\desktop\whoami.exe.r
  - indicators (libraries > flag)
  - footprints (type > sha256)
  - virustotal (status > offline)
  - dos-header (size > 64 bytes)
  - dos-stub (size > 56 bytes)
  - rich-header (n/a)
  - file-header (executable > 64-bit)
  - optional-header (subsystem > con
  - directories (count > 5)
  - sections (count > 6)
  - libraries (group > network)
  - imports (flag > 450)
  - exports (n/a)
  - thread-local-storage (count > 3)
  - .NET (n/a)
  - resources (n/a)
  - strings (flag > 89)
  - debug (n/a)
  - manifest (n/a)
  - version (n/a)
  - certificate (n/a)
  - overlay (n/a)

library (13)	duplicate (0)	flag (4)	first-thunk-original (INT)	first-thunk (IAT)
KERNEL32.dll	-	-	0x00401EA0	0x00402D18
USER32.dll	-	-	0x004022C0	0x00403138
ole32.dll	-	-	0x004025B0	0x00403428
ADVAPI32.dll	-	-	0x004026D0	0x00403548
SHELL32.dll	-	-	0x00402720	0x00403598
comdlg32.dll	-	-	0x004027B0	0x00403628
IMM32.dll	-	-	0x004027D8	0x00403650
GDI32.dll	-	-	0x00402850	0x004036C8
msvcrt.dll	-	-	0x00402AE8	0x00403960
WS2_32.dll	-	x	0x00402610	0x00403488
WINMM.dll	-	x	0x00402770	0x004035E8
MPR.dll	-	x	0x00402790	0x00403608
USP10.dll	-	x	0x00402820	0x00403698

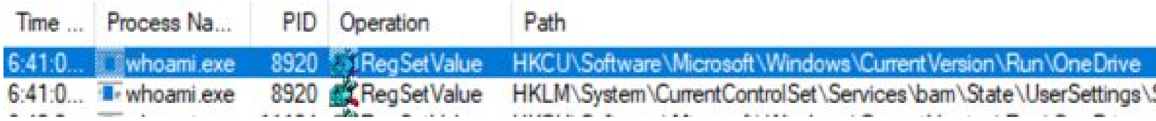
xx. Findings:

1. 4 of the 13 libraries (WS2_32, WINMM, MPR, USP10) are marked with a flag indicating suspicious and malicious usage of these libraries. These correspond to key system functions that allow for network communications, multimedia operations, network resource management, and text rendering which implies how the malware establishes connections, send/receive data, interact with sound/time functions, and manipulate how text is processed or displayed.

Dynamic Analysis (Host)

1. **Console output after running the binary**
    a. 

```
Command Prompt

C:\Users\IEUser\Desktop\malware>whoami.exe
MSEDGEWIN10\IEUser

C:\Users\IEUser\Desktop\malware>
```

    b. The output appears to be normal
2. **Procmon**
    a. Registry
        i. RegSetValue Operation
        ii. 

Time ...	Process Na...	PID	Operation	Path
6:41:0...	whoami.exe	8920	RegSetValue	HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OneDrive
6:41:0...	whoami.exe	8920	RegSetValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S

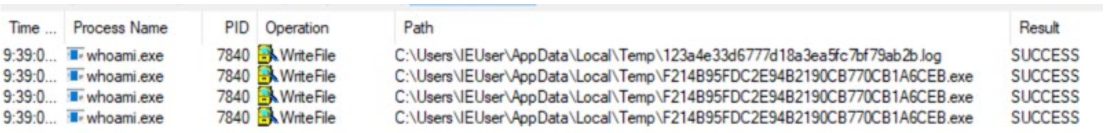
        iii. The first registry key written to is HKCU\Software\Microsoft\Windows\CurrentVersion\Run\OneDrive and sets the value to the path of the downloaded exe file in the AppData\Temp directory

The second registry key written to is to a key that starts with HKLM and ends in the path of the whoami binary and writes binary data to the value.

It is clear that the malware sample does this to maintain persistence. The HKCU root directory for registry keys is for the current user and it appears that it is trying to make Windows think that the OneDrive executable is the downloaded file and also configure it so that it runs every time the user logs in. This would only apply to the current user though.

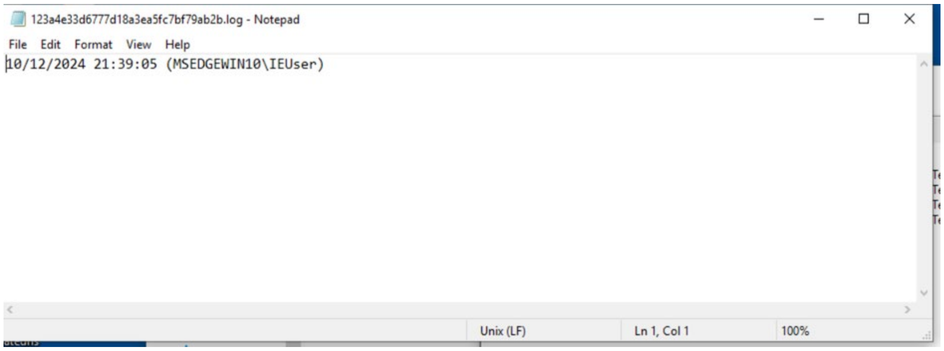
The second write operation could also be for persistence but for the whole system, and instead of the downloaded exe file it uses the original whoami executable. It allows the malware to establish system-wide persistence. Writing to it ensures that the malware runs not only for the current user but for all users on the system meaning that the malware will execute whenever any user logs into the system. The malware will survive even if the compromised user logs out.

b. File IO
   i. FileWrite operation



Time ...	Process Name	PID	Operation	Path	Result
9:39:0...	whoami.exe	7840	WriteFile	C:\Users\IEUser\AppData\Local\Temp\123a4e33d6777d18a3ea5fc7bf79ab2b.log	SUCCESS
9:39:0...	whoami.exe	7840	WriteFile	C:\Users\IEUser\AppData\Local\Temp\F214B95FDC2E94B2190CB770CB1A6CEB.exe	SUCCESS
9:39:0...	whoami.exe	7840	WriteFile	C:\Users\IEUser\AppData\Local\Temp\F214B95FDC2E94B2190CB770CB1A6CEB.exe	SUCCESS
9:39:0...	whoami.exe	7840	WriteFile	C:\Users\IEUser\AppData\Local\Temp\F214B95FDC2E94B2190CB770CB1A6CEB.exe	SUCCESS

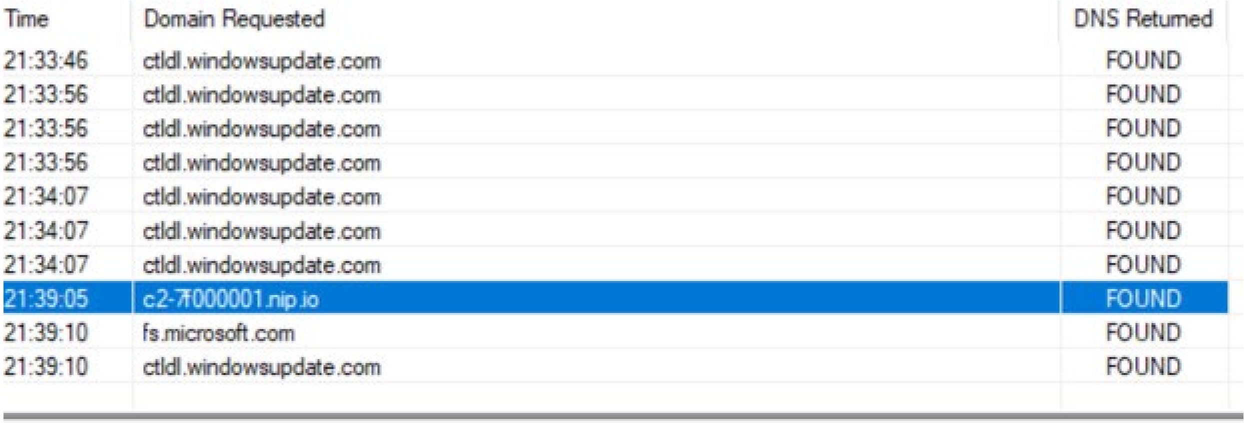
   ii. Procmon detected the program creating and writing to two files in the C:\Users\IEUser\Appdata\Local\Temp directory. A log file and an executable which matches the file name wireshark detected.


123a4e33d6777d18a3ea5fc7bf79ab2b.log - Notepad
File Edit Format View Help
Unix (LF)
Ln 1, Col 1
100%

```
10/12/2024 21:39:05 (MSEDGEWIN10\IEUser)
```

The contents of the log file written to the AppData\Local\Temp directory

3. ApateDNS

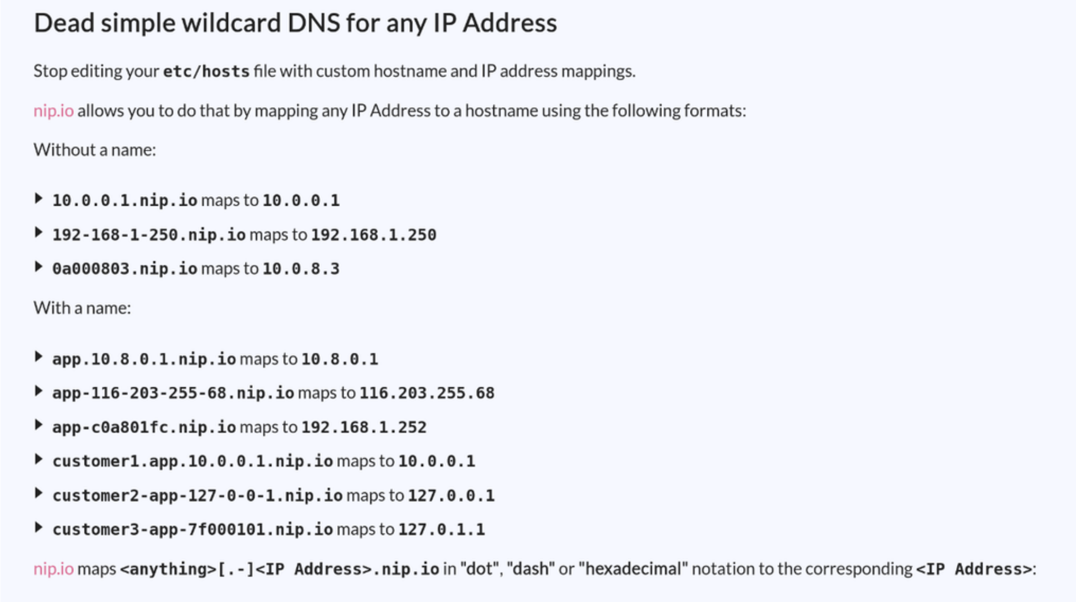


Time	Domain Requested	DNS Returned
21:33:46	ctldl.windowsupdate.com	FOUND
21:33:56	ctldl.windowsupdate.com	FOUND
21:33:56	ctldl.windowsupdate.com	FOUND
21:33:56	ctldl.windowsupdate.com	FOUND
21:34:07	ctldl.windowsupdate.com	FOUND
21:34:07	ctldl.windowsupdate.com	FOUND
21:34:07	ctldl.windowsupdate.com	FOUND
21:39:05	c2-7f000001.nip.io	FOUND
21:39:10	fs.microsoft.com	FOUND
21:39:10	ctldl.windowsupdate.com	FOUND

a. A DNS request to c2-7f000001.nip.io

b. The nip.io domain is a wildcard domain service that resolves to whatever ip address appears last in the subdomain. In this case it would resolve to 7f000001 which is the hexadecimal of the localhost ip address 127.0.0.0.1. This could mean that part of the application is running an http server to obfuscate part of the binary away, but it is more likely it was defanged from the original malware sample.

i. Here is the description of their service from their website:



Dead simple wildcard DNS for any IP Address

Stop editing your **`etc/hosts`** file with custom hostname and IP address mappings.

nip.io allows you to do that by mapping any IP Address to a hostname using the following formats:

Without a name:

- **`10.0.0.1.nip.io`** maps to **`10.0.0.1`**
- **`192-168-1-250.nip.io`** maps to **`192.168.1.250`**
- **`0a000803.nip.io`** maps to **`10.0.8.3`**

With a name:

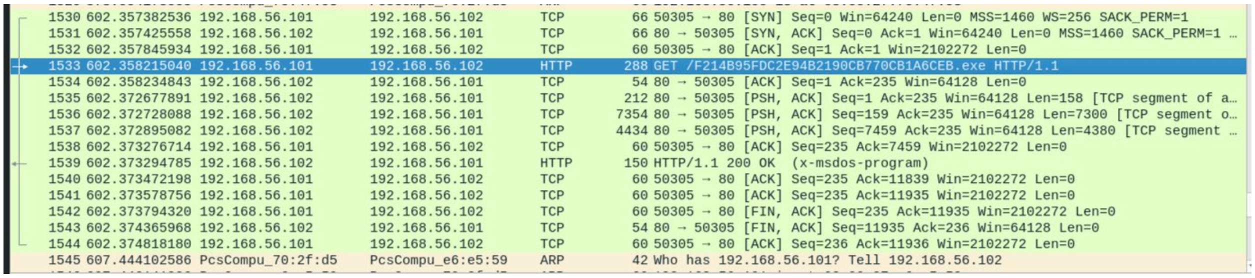
- **`app.10.8.0.1.nip.io`** maps to **`10.8.0.1`**
- **`app-116-203-255-68.nip.io`** maps to **`116.203.255.68`**
- **`app-c0a801fc.nip.io`** maps to **`192.168.1.252`**
- **`customer1.app.10.0.0.1.nip.io`** maps to **`10.0.0.1`**
- **`customer2-app-127-0-0-1.nip.io`** maps to **`127.0.0.1`**
- **`customer3-app-7f000101.nip.io`** maps to **`127.0.1.1`**

nip.io maps **`<anything>[.-]<IP Address>.nip.io`** in "dot", "dash" or "hexadecimal" notation to the corresponding **`<IP Address>`**:

Dynamic Analysis (Network)

4. **Wireshark**

   a. Filter smtp, http, dns for C2 servers

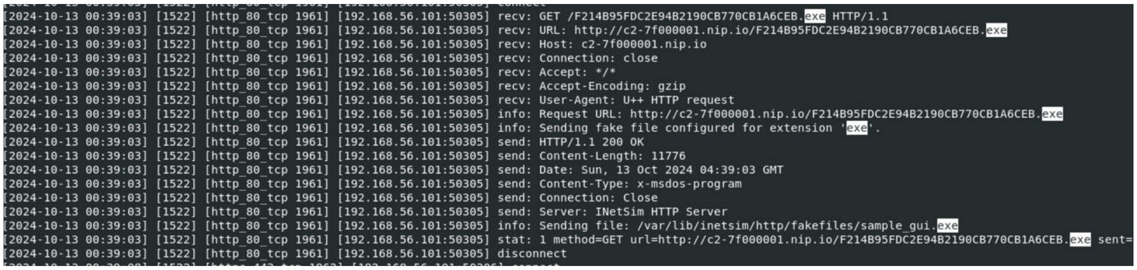


```
1530 602.357382536 192.168.56.101     192.168.56.102     TCP       66 50305 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
1531 602.357425558 192.168.56.102     192.168.56.101     TCP       66 80 → 50305 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM=1 …
1532 602.357845934 192.168.56.101     192.168.56.102     TCP       60 50305 → 80 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
1533 602.358215040 192.168.56.101     192.168.56.102     HTTP     288 GET /F214B95FDC2E94B2190CB770CB1A6CEB.exe HTTP/1.1
1534 602.358234843 192.168.56.102     192.168.56.101     TCP       54 80 → 50305 [ACK] Seq=1 Ack=235 Win=64128 Len=0
1535 602.372677891 192.168.56.102     192.168.56.101     TCP      212 80 → 50305 [PSH, ACK] Seq=1 Ack=235 Win=64128 Len=158 [TCP segment of a…
1536 602.372728088 192.168.56.102     192.168.56.101     TCP     7354 80 → 50305 [PSH, ACK] Seq=159 Ack=235 Win=64128 Len=7300 [TCP segment o…
1537 602.372895082 192.168.56.102     192.168.56.101     TCP     4434 80 → 50305 [PSH, ACK] Seq=7459 Ack=235 Win=64128 Len=4380 [TCP segment …
1538 602.373276714 192.168.56.101     192.168.56.102     TCP       60 50305 → 80 [ACK] Seq=235 Ack=7459 Win=2102272 Len=0
1539 602.373294785 192.168.56.102     192.168.56.101     HTTP     150 HTTP/1.1 200 OK  (x-msdos-program)
1540 602.373472198 192.168.56.101     192.168.56.102     TCP       60 50305 → 80 [ACK] Seq=235 Ack=11839 Win=2102272 Len=0
1541 602.373578756 192.168.56.101     192.168.56.102     TCP       60 50305 → 80 [ACK] Seq=235 Ack=11935 Win=2102272 Len=0
1542 602.373794320 192.168.56.101     192.168.56.102     TCP       60 50305 → 80 [FIN, ACK] Seq=235 Ack=11935 Win=2102272 Len=0
1543 602.374365968 192.168.56.102     192.168.56.101     TCP       54 80 → 50305 [FIN, ACK] Seq=11935 Ack=236 Win=64128 Len=0
1544 602.374818180 192.168.56.101     192.168.56.102     TCP       60 50305 → 80 [ACK] Seq=236 Ack=11936 Win=2102272 Len=0
1545 607.444102586 PcsCompu_70:2f:d5  PcsCompu_e6:e5:59  ARP       42 Who has 192.168.56.101? Tell 192.168.56.102
```

We can clearly see an HTTP GET request to an exe file which inetsim responded with its default executable. This indicates that the malwarre us attempting to communicate with a C2 server. Malware that uses HTTP traffic as a communication channel can blend in with normal activity making it harder for security systems to detect it.

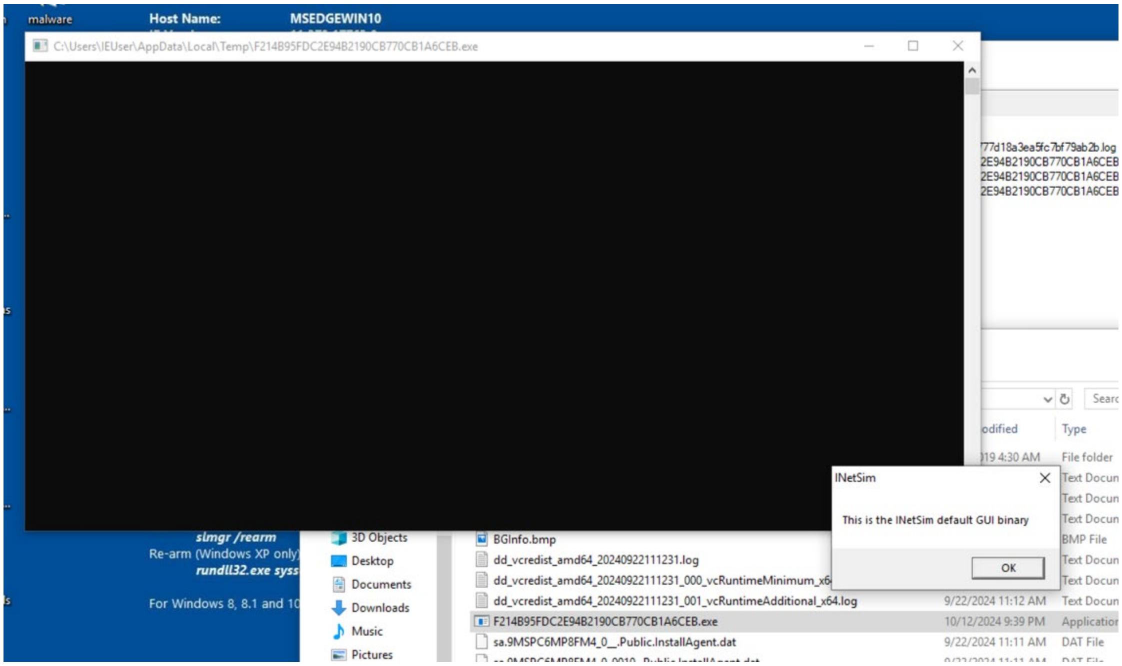
5. **Inetsim Logs**

   a. /var/log/inetsim/service.log

i. 

```
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] recv: GET /F214B95FDC2E94B2190CB770CB1A6CEB.exe HTTP/1.1
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] recv: URL: http://c2-7f000001.nip.io/F214B95FDC2E94B2190CB770CB1A6CEB.exe
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] recv: Host: c2-7f000001.nip.io
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] recv: Connection: close
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] recv: Accept: */*
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] recv: Accept-Encoding: gzip
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] recv: User-Agent: U++ HTTP request
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] info: Request URL: http://c2-7f000001.nip.io/F214B95FDC2E94B2190CB770CB1A6CEB.exe
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] info: Sending fake file configured for extension 'exe'.
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] send: HTTP/1.1 200 OK
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] send: Content-Length: 11776
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] send: Date: Sun, 13 Oct 2024 04:39:03 GMT
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] send: Content-Type: x-msdos-program
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] send: Connection: Close
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] send: Server: INetSim HTTP Server
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] info: Sending file: /var/lib/inetsim/http/fakefiles/sample_gui.exe
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] stat: 1 method=GET url=http://c2-7f000001.nip.io/F214B95FDC2E94B2190CB770CB1A6CEB.exe sent=
[2024-10-13 00:39:03] [1522] [http_80_tcp 1961] [192.168.56.101:50305] disconnect
```

Inetsim logged an http GET request to an exe file that starts with F21 on the strange c2-7f000001.nip.io domain.

ii. 

C:\Users\IEUser\AppData\Local\Temp\F214B95FDC2E94B2190CB770CB1A6CEB.exe

INetSim

This is the INetSim default GUI binary

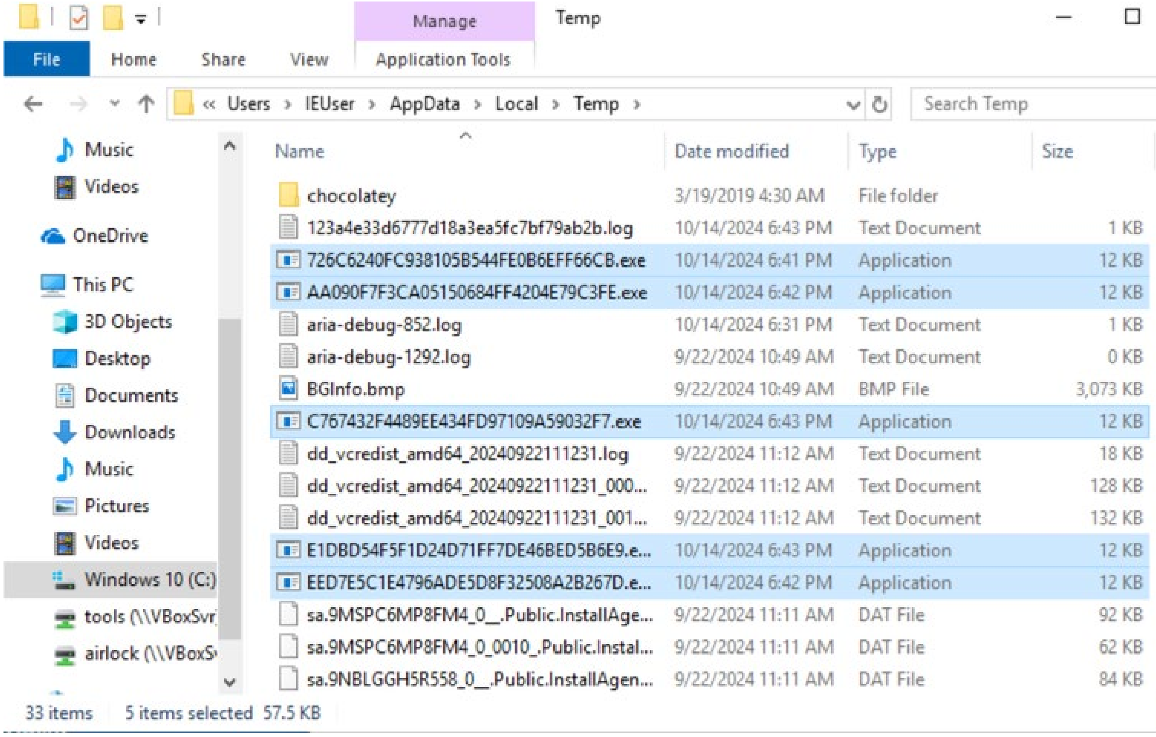
OK

```
BGInfo.bmp
dd_vcredist_amd64_20240922111231.log
dd_vcredist_amd64_20240922111231_000_vcRuntimeMinimum_x6
dd_vcredist_amd64_20240922111231_001_vcRuntimeAdditional_x64.log   9/22/2024 11:12 AM   Text Docun
F214B95FDC2E94B2190CB770CB1A6CEB.exe                               10/12/2024 9:39 PM   Applicatior
sa.9MSPC6MP8FM4_0_.Public.InstallAgent.dat                         9/22/2024 11:11 AM   DAT File
```

This is the result of running the downloaded exe file in AppData\Local\Temp directory

iii. After running the binary multiple times, the name of the downloaded exe file changes every time. It appears to be a computed hash of some sort because they all have the same length and only contain hex digits.

iv.



Name	Date modified	Type	Size
chocolatey	3/19/2019 4:30 AM	File folder	
123a4e33d6777d18a3ea5fc7bf79ab2b.log	10/14/2024 6:43 PM	Text Document	1 KB
726C6240FC938105B544FE0B6EFF66CB.exe	10/14/2024 6:41 PM	Application	12 KB
AA090F7F3CA05150684FF4204E79C3FE.exe	10/14/2024 6:42 PM	Application	12 KB
aria-debug-852.log	10/14/2024 6:31 PM	Text Document	1 KB
aria-debug-1292.log	9/22/2024 10:49 AM	Text Document	0 KB
BGInfo.bmp	9/22/2024 10:49 AM	BMP File	3,073 KB
C767432F4489EE434FD97109A59032F7.exe	10/14/2024 6:43 PM	Application	12 KB
dd_vcredist_amd64_20240922111231.log	9/22/2024 11:12 AM	Text Document	18 KB
dd_vcredist_amd64_20240922111231_000...	9/22/2024 11:12 AM	Text Document	128 KB
dd_vcredist_amd64_20240922111231_001...	9/22/2024 11:12 AM	Text Document	132 KB
E1DBD54F5F1D24D71FF7DE46BED5B6E9.e...	10/14/2024 6:43 PM	Application	12 KB
EED7E5C1E4796ADE5D8F32508A2B267D.e...	10/14/2024 6:42 PM	Application	12 KB
sa.9MSPC6MP8FM4_0__.Public.InstallAge...	9/22/2024 11:11 AM	DAT File	92 KB
sa.9MSPC6MP8FM4_0_0010_.Public.Instal...	9/22/2024 11:11 AM	DAT File	62 KB
sa.9NBLGGH5R558_0__.Public.InstallAgen...	9/22/2024 11:11 AM	DAT File	84 KB

33 items 5 items selected 57.5 KB

All of the highlighted files were downloaded by whoami.exe

Conclusion

After running both static and dynamic analyses we have concluded that this malware sample has networking properties and attempts to obtain another .exe file from the c2-7f000001 domain. The malware imports functions from the WS2_32.dll library, which includes socket, connect, recv, send, and closesocket. Each time the malware downloads an executable from the c2-7f000001 domain, the file name changes, indicating an effort to evade detection through varying the file's signature. Additionally, this piece of malware attempts to write a log and an .exe into the user's AppData\Local\Temp directory folder. whoami.exe has a persistence mechanism by writing to a directory key to the windows\run folder pointing to the .exe file, ensuring it runs each time a user logs in.

Appendix

- Cassandra Guevara: Reviewed analysis and expanded on the findings.
- Ryan Hellwege: Dynamic analysis screenshots and explanation
- Kyle Ho: Reviewing and editing analyses and findings
- Phu Lam: Static Analysis and Findings
- Wayne Muse: Reviewed Analyses and conclusion, and organized the project discord