FINAL REPORT

I. PART 1-1

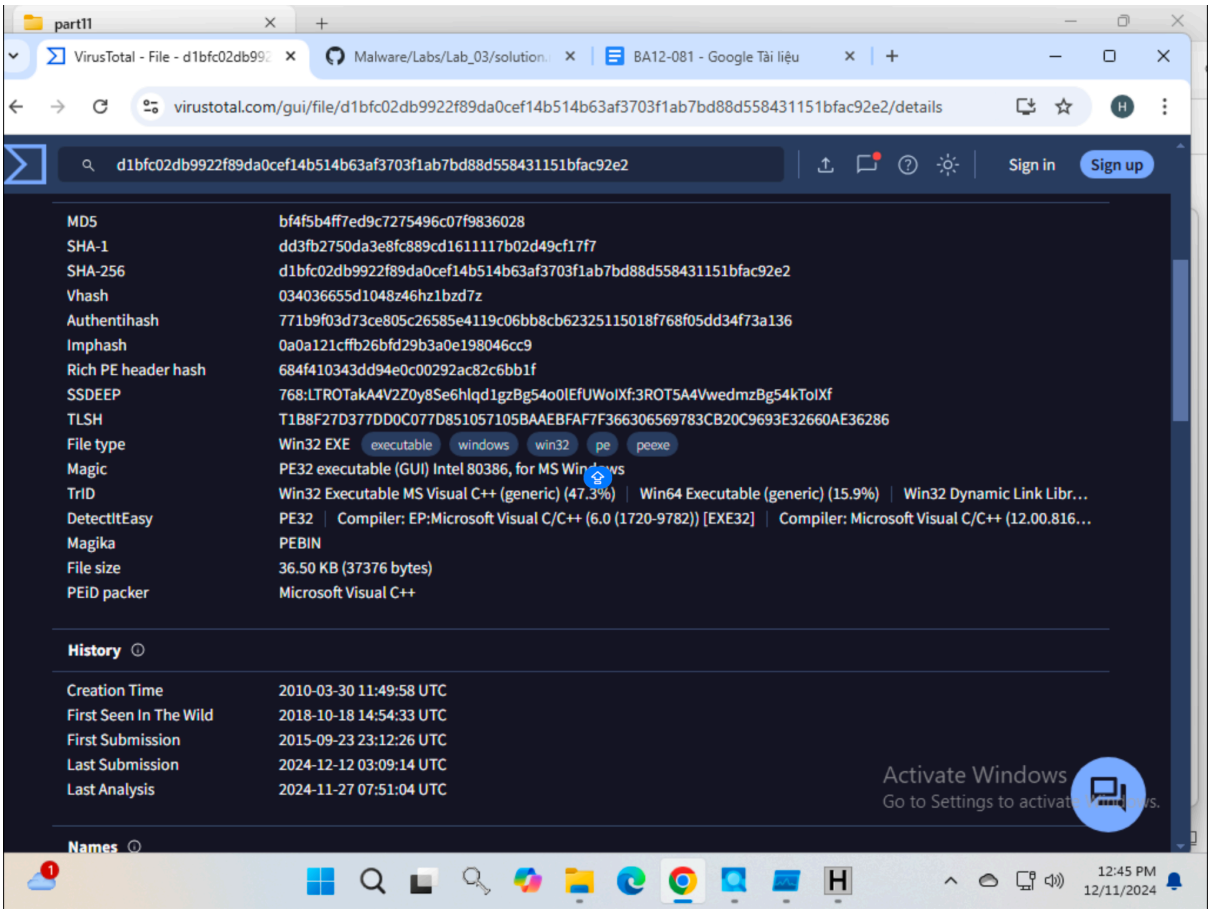
A. Basic Static

1. File Information

File: part11
Size: 37,376 bytes

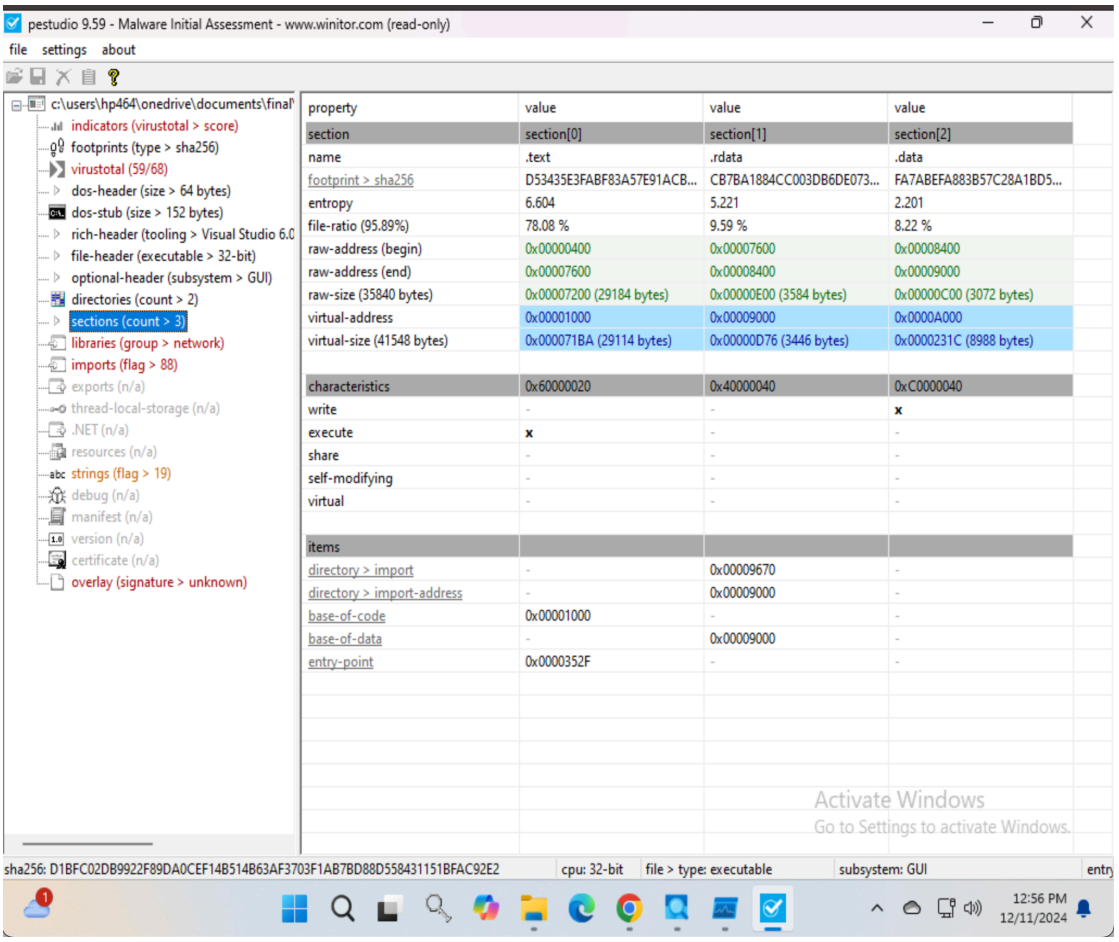
2. Virus Total

Detection ratio: 59/68
Target Machine: Intel 386 or later processors and compatible processors
Compilation Timestamp: 2010-03-30 11:49:58 UTC
Entry Point: 13615
Contained Sections: 3



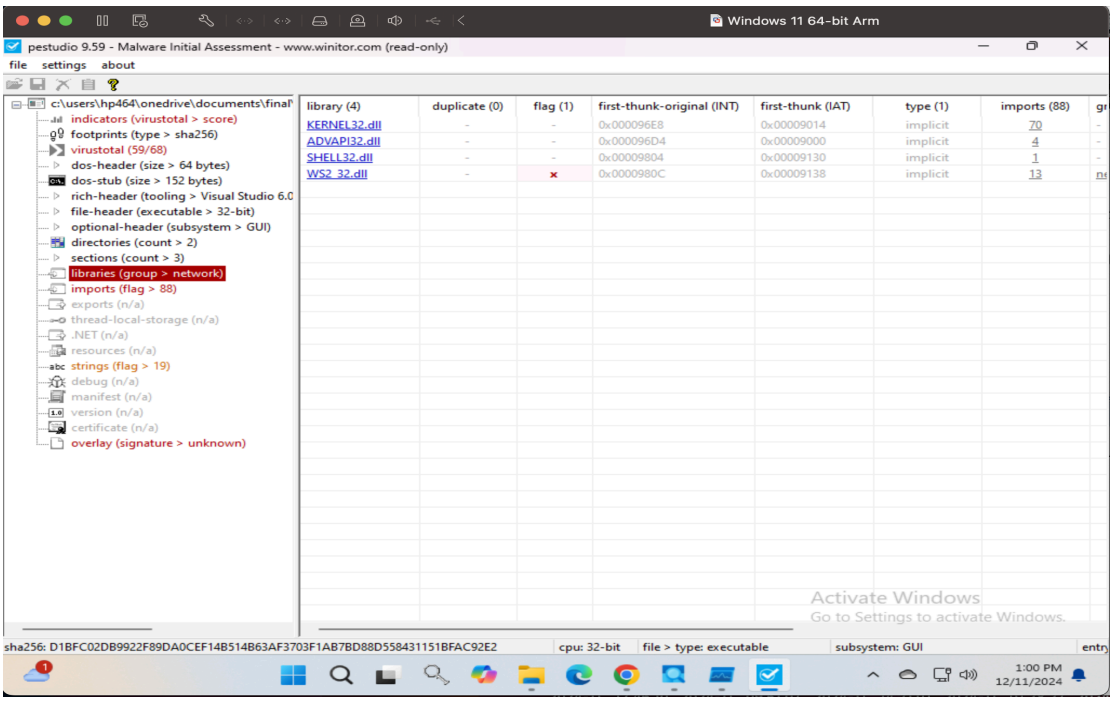
3. PESTUDIO

a) Sections

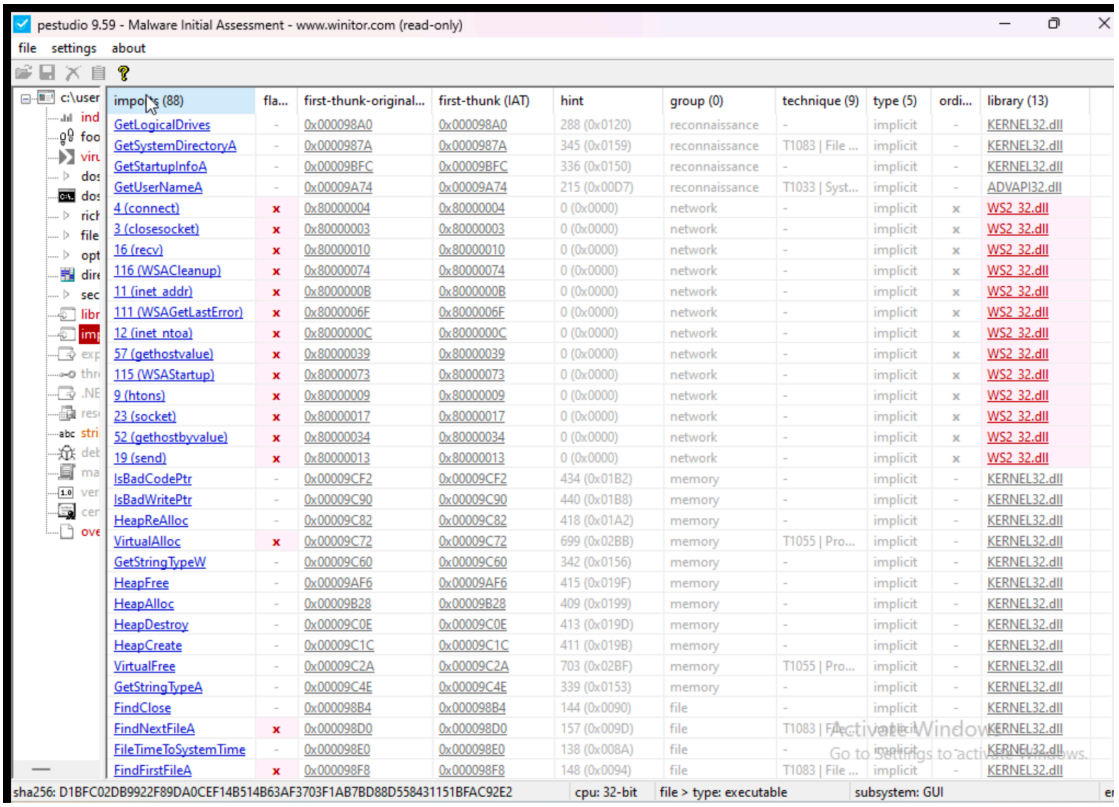


b) Libraries

Import KERNEL32.dll, ADVAPI32.dll, SHELL32.dll, WS2 32.dll



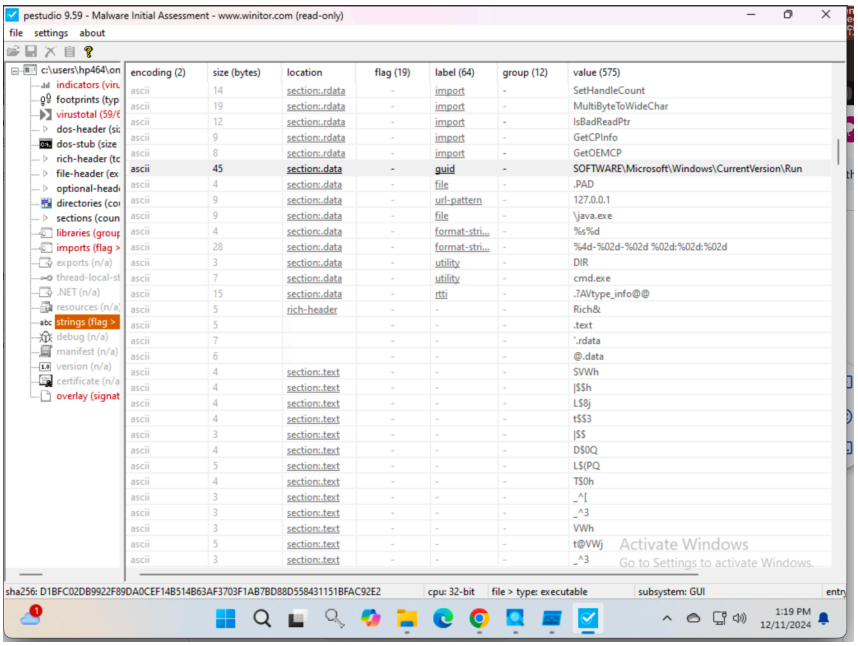
c) imports



- GetLogicalDrives: Retrieves bitmasks representing all available drives. This could be leveraged for environmental keying or to identify the host system.

- Gethostbyname: Resolves a hostname, potentially used to identify the attacker's host for communication purposes.
- GetOEMCP: Retrieves the OEM code page, which might be used to detect virtual machine environments.

d) Strings



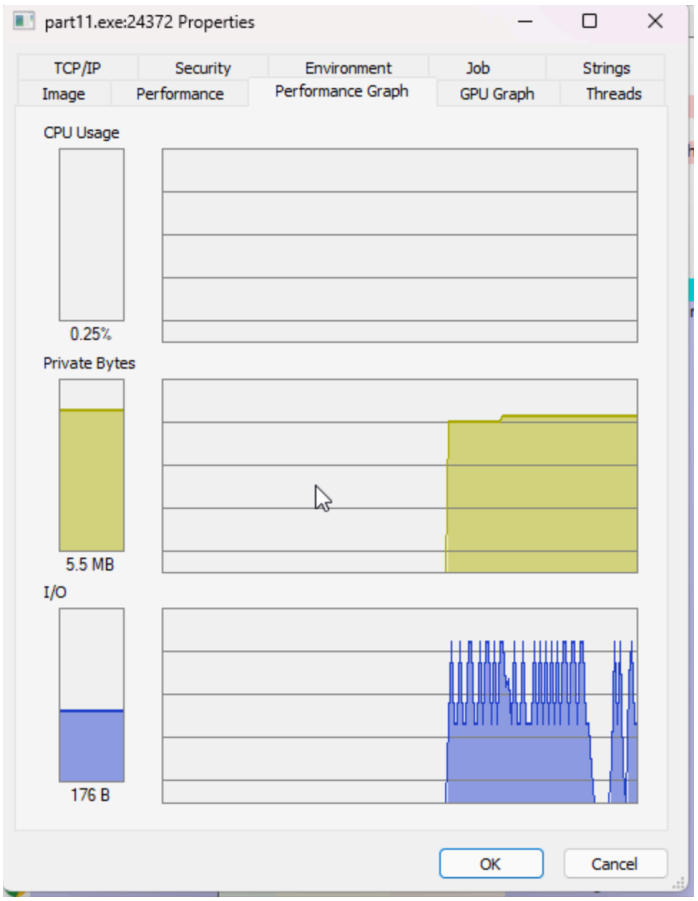
It sets the key in 'SOFTWARE\Microsoft\Windows\CurrentVersion\Run' to 'C:\DOCUME~1\User\java.exe', which is a copy of itself that it made. Some host-based signatures are in documents and settings for the user and copies under 'java.exe'.

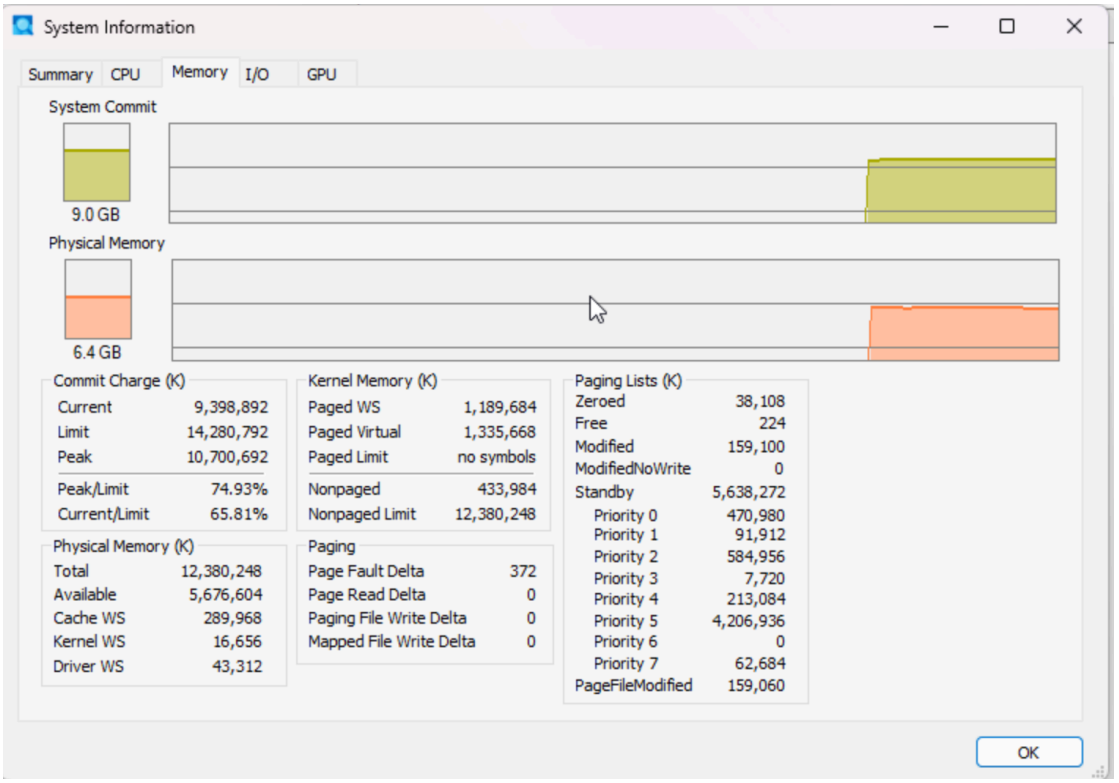
B. Basic Dynamic

1. Purpose

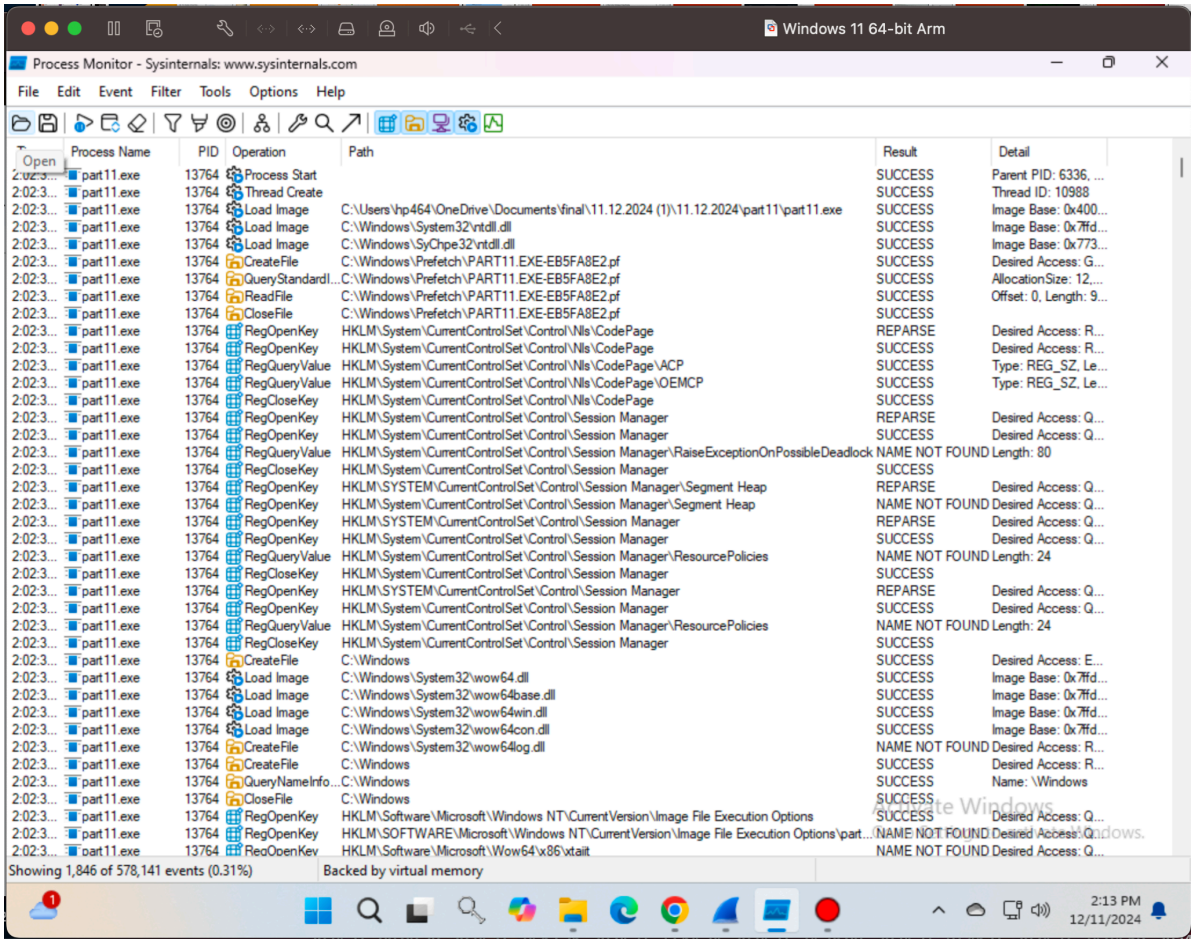
Running the program and observing its impact on the system provides a direct understanding of the malware's behavior. This practical insight helps establish context for advanced static analysis when disassembling the executable. Additionally, it enables the development of host- or network-based signatures to detect the presence of the malware on systems in the future.

2. Process Explorer





3. Process Promon



C. Advanced Static

Lists Processes (0x0402310):

- Likely a function to list running processes on the system. It might use APIs like CreateToolhelp32Snapshot, Process32First, and Process32Next. Utilizes the following Windows API functions:

  CreateToolhelp32Snapshot: Captures a snapshot of all processes.

  Process32First: Retrieves the first process in the snapshot.

  Process32Next: Iterates through the remaining processes.

Remote Shell (0x0402490 and 0x0402660):

- These functions could enable a remote shell, allowing an attacker to execute commands on the infected machine. They might interact with cmd.exe or send/receive commands over a socket

  CreateProcessA: Starts a new process

  PeekNamedPipe: Reads data from a pipe to check if there's input/output.

  WriteFile: Sends commands or responses through a pipe.

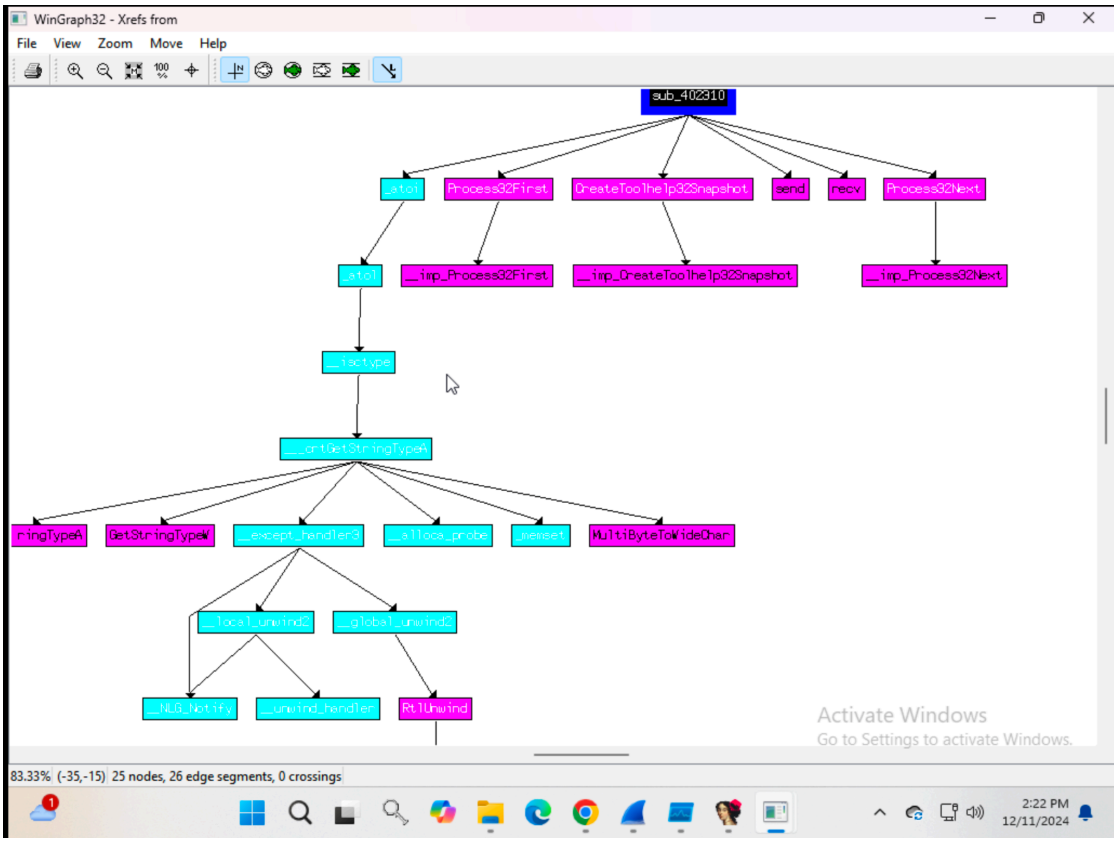
.

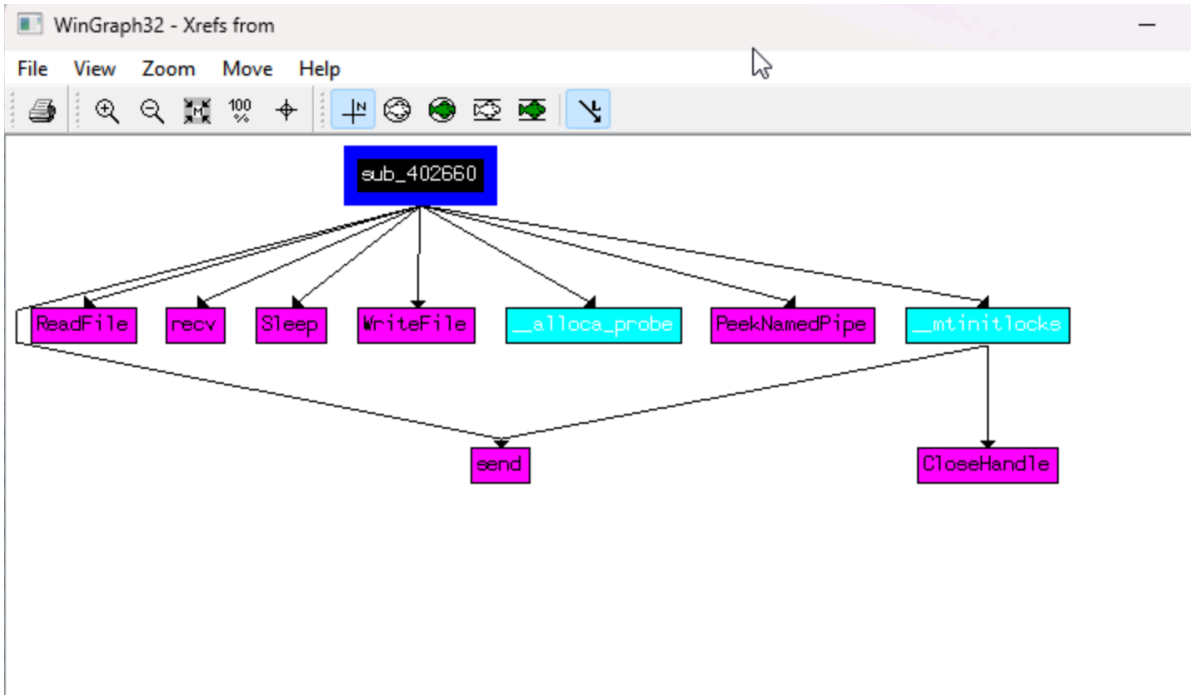
Upload File (0x00402210):

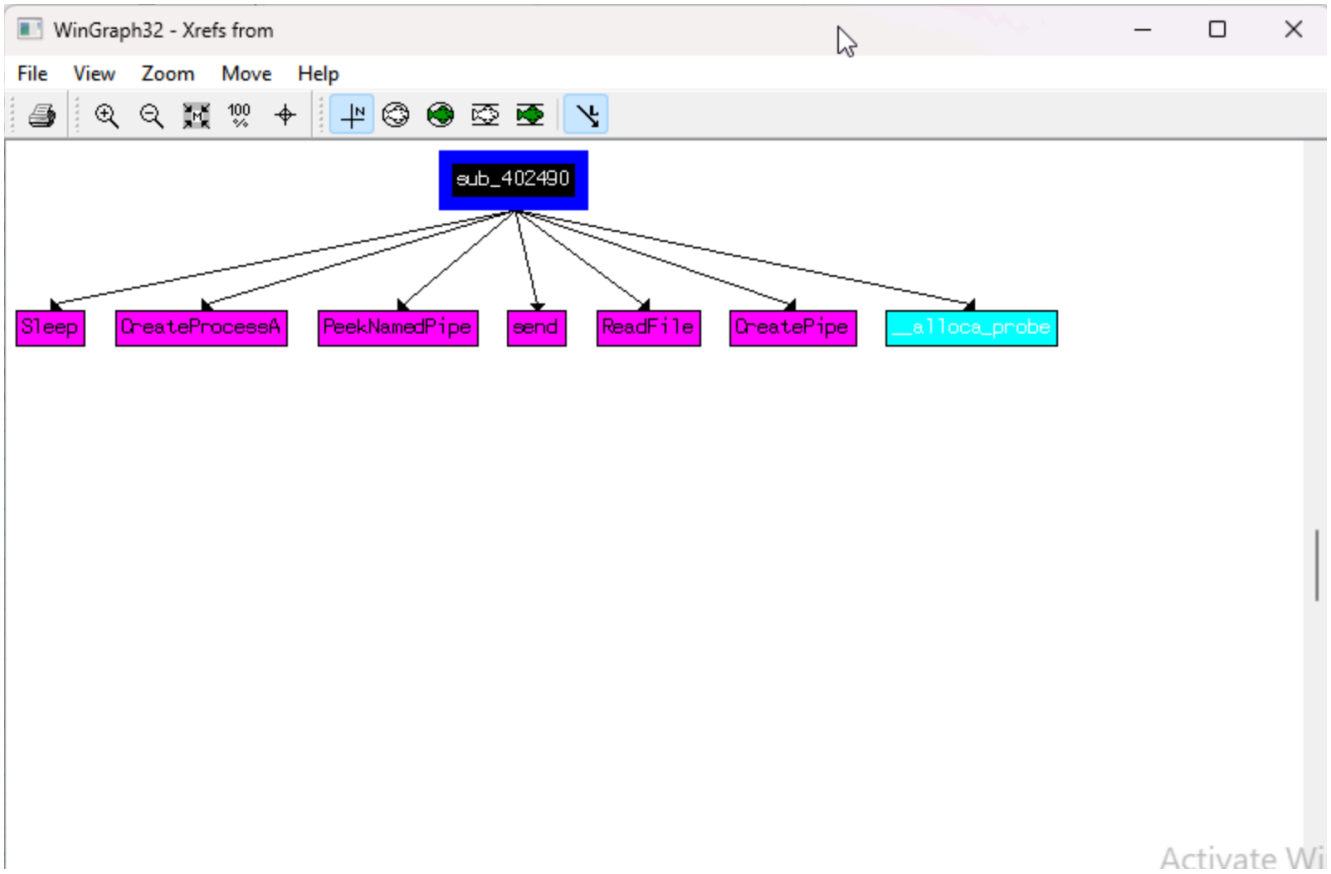
- The sub_402210 function (previously analyzed) is used to XOR encrypt a file with the key 0x55 and upload it to a remote server via a socket.

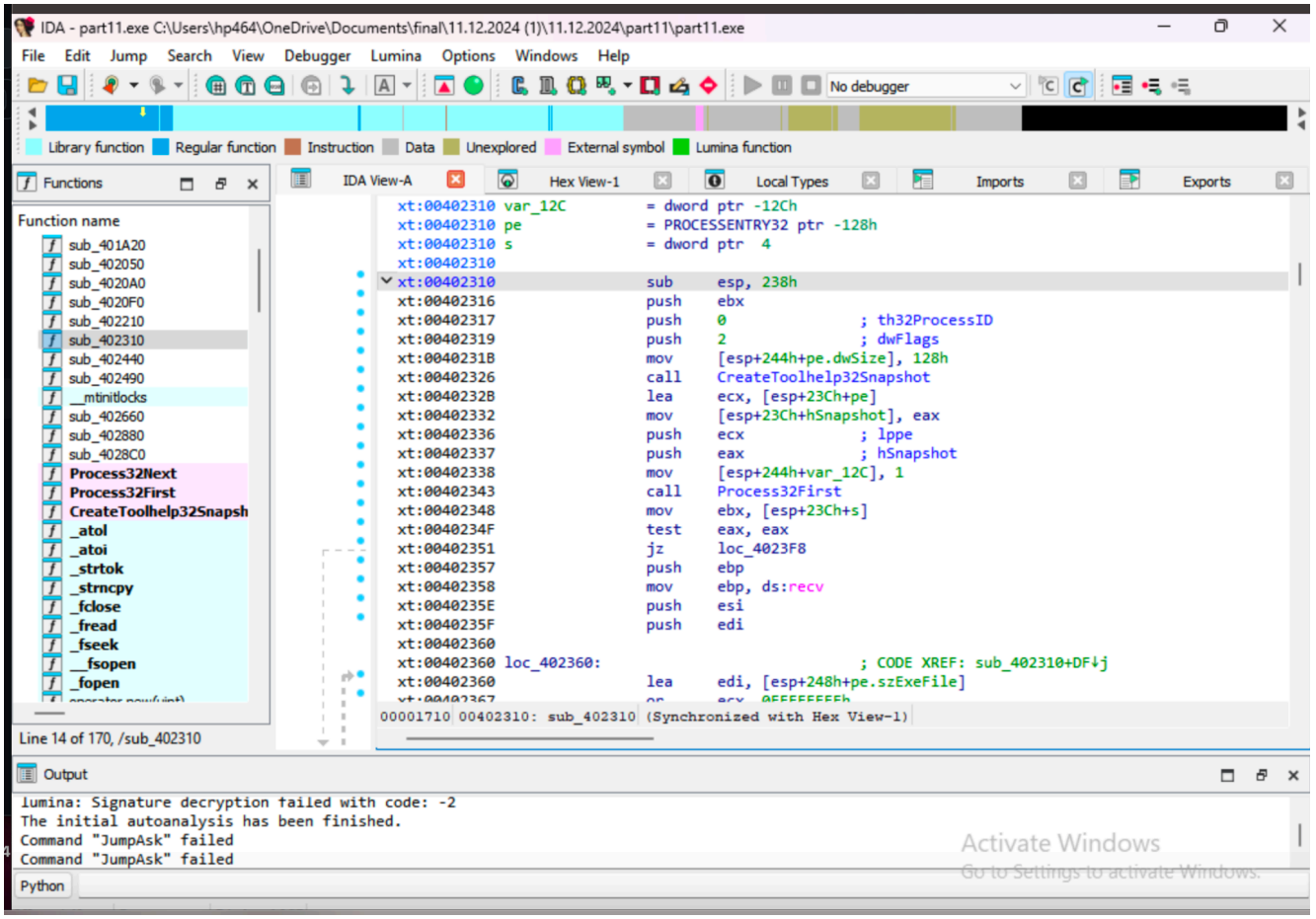
Command Identifiers:

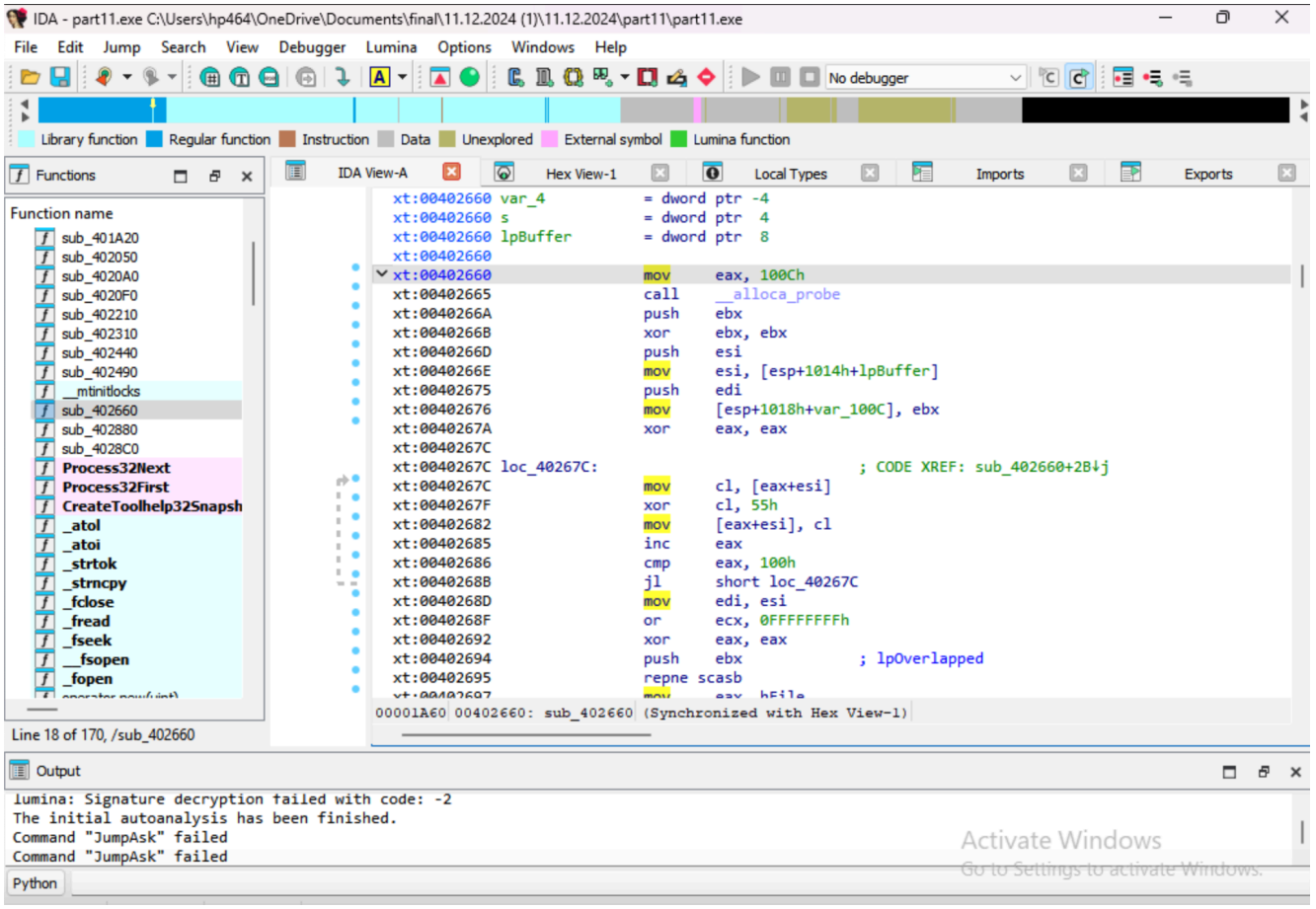
- **0x2**: Lists directory contents.
- **0x5**: Downloads a file to the infected machine.
- **0x8**: Terminates a process using its PID.


WinGraph32 - Xrefs from
File View Zoom Move Help
sub_402810
_atoi
Process32First
CreateToolhelp32Snapshot
send
recv
Process32Next
_atoi
__imp_Process32First
__imp_CreateToolhelp32Snapshot
__imp_Process32Next
__isctype
__crtGetStringTypeA
ringTypeA
GetStringTypeW
__except_handler3
__alloca_probe
_memset
MultiByteToWideChar
__local_unwind2
__global_unwind2
_NLG_Notify
_unwind_handler
RtlUnwind
Activate Windows
Go to Settings to activate Windows.
83.33% (-35,-15) 25 nodes, 26 edge segments, 0 crossings
2:22 PM
12/11/2024


WinGraph32 - Xrefs from
File View Zoom Move Help
sub_402660
ReadFile
recv
Sleep
WriteFile
__alloca_probe
PeekNamedPipe
__mtinitlocks
send
CloseHandle


WinGraph32 - Xrefs from
File View Zoom Move Help
sub_402490
Sleep
CreateProcessA
PeekNamedPipe
send
ReadFile
CreatePipe
__alloca_probe
Activate Wi


IDA - part11.exe C:\Users\hp464\OneDrive\Documents\final\11.12.2024 (1)\11.12.2024\part11\part11.exe
File Edit Jump Search View Debugger Lumina Options Windows Help
No debugger
Library function Regular function Instruction Data Unexplored External symbol Lumina function
Functions
Function name
sub_401A20
sub_402050
sub_4020A0
sub_4020F0
sub_402210
sub_402310
sub_402440
sub_402490
__mtinitlocks
sub_402660
sub_402880
sub_4028C0
Process32Next
Process32First
CreateToolhelp32Snapsh
_atol
_atoi
_strtok
_strncpy
_fclose
_fread
_fseek
__fsopen
_fopen
Line 14 of 170, /sub_402310
IDA View-A
Hex View-1
Local Types
Imports
Exports
xt:00402310 var_12C = dword ptr -12Ch
xt:00402310 pe = PROCESSENTRY32 ptr -128h
xt:00402310 s = dword ptr 4
xt:00402310
xt:00402310 sub esp, 238h
xt:00402316 push ebx
xt:00402317 push 0 ; th32ProcessID
xt:00402319 push 2 ; dwFlags
xt:0040231B mov [esp+244h+pe.dwSize], 128h
xt:00402326 call CreateToolhelp32Snapshot
xt:0040232B lea ecx, [esp+23Ch+pe]
xt:00402332 mov [esp+23Ch+hSnapshot], eax
xt:00402336 push ecx ; lppe
xt:00402337 push eax ; hSnapshot
xt:00402338 mov [esp+244h+var_12C], 1
xt:00402343 call Process32First
xt:00402348 mov ebx, [esp+23Ch+s]
xt:0040234F test eax, eax
xt:00402351 jz loc_4023F8
xt:00402357 push ebp
xt:00402358 mov ebp, ds:recv
xt:0040235E push esi
xt:0040235F push edi
xt:00402360
xt:00402360 loc_402360: ; CODE XREF: sub_402310+DF↓j
xt:00402360 lea edi, [esp+248h+pe.szExeFile]
00001710 00402310: sub_402310 (Synchronized with Hex View-1)
Output
lumina: Signature decryption failed with code: -2
The initial autoanalysis has been finished.
Command "JumpAsk" failed
Command "JumpAsk" failed
Python
Activate Windows
Go to Settings to activate Windows.



D. Conclusion

part11.exe is a multi-functional backdoor with persistence, process monitoring, file upload, and remote command execution capabilities. Its ability to communicate with a remote server and execute commands remotely makes it a serious threat to compromised systems. Effective mitigation includes monitoring for registry modifications, detecting unauthorized file copies in user directories, and inspecting network traffic for suspicious DNS requests or encoded communications.

E. Resources

PE Studio: https://www.winitor.com/download
IDA Professtional: https://hex-rays.com/ida-pro