



FINAL REPORT

I. PART 1-1	3
A. Basic Static	3
1. File Information	3
2. Virus Total	3
3. PESTUDIO	4
B. Basic Dynamic	6
1. Purpose	6
2. Process Explorer	7
3. Process Promon	8
C. Advanced Static	8

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

The screenshot shows a web browser window displaying the VirusTotal analysis page for the file `d1bfc02db9922f89da0cef14b514b63af3703f1ab7bd88d558431151bfac92e2`. The page provides detailed static analysis information, including:

- Hashes:
 - MD5: bf4f5b4ff7ed9c7275496c07f9836028
 - SHA-1: dd3fb2750da3e8fc889cd1611117b02d49cf17f7
 - SHA-256: d1bfc02db9922f89da0cef14b514b63af3703f1ab7bd88d558431151bfac92e2
 - Vhash: 034036655d1048z46hz1bzd7z
 - Authentihash: 771b9f03d73ce805c26585e4119c06bb8cb62325115018f768f05dd34f73a136
 - Imphash: 0a0a121cffb26bfd29b3a0e198046cc9
 - Rich PE header hash: 684f410343dd94e0c00292ac82c6bb1f
 - SSDeep: 768:LTOtakA4VZ0y8Se6hlqd1gzBg54o0lEfUWoIxf:3ROT5A4VwedmzBg54kTolXf
 - TLSH: T188F27D377DD0C077D851057105BAEBFAF7F366306569783CB20C9693E32660AE36286
- File type: Win32 EXE (executable, windows, win32, pe, pexe)
- Magic: PE32 executable (GUI) Intel 80386, for MS Win32
- TrID: Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (1.7%)
- DetectItEasy: PE32 | Compiler: EP:Microsoft Visual C/C++ (6.0 (1720-9782)) [EXE32] | Compiler: Microsoft Visual C/C++ (12.00.816...)
- Magika: PEBIN
- File size: 36.50 KB (37376 bytes)
- PEID packer: Microsoft Visual C++

Below the analysis table, there is a "History" section showing submission details:

Event	Date
Creation Time	2010-03-30 11:49:58 UTC
First Seen In The Wild	2018-10-18 14:54:33 UTC
First Submission	2015-09-23 23:12:26 UTC
Last Submission	2024-12-12 03:09:14 UTC
Last Analysis	2024-11-27 07:51:04 UTC

At the bottom right, there is a "Activate Windows" button with the text "Go to Settings to activate Windows".

3. PESTUDIO

a) Sections

The screenshot shows the PEStudio interface for analyzing a file named 'final'. The left pane displays a tree view of file indicators, including:

- indicators (virustotal > score)
- footprints (type > sha256)
- virus total (59/68)
- dos-header (size > 64 bytes)
- dos-stub (size > 152 bytes)
- rich-header (tooling > Visual Studio 6.0)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 2)
- sections (count > 3) **(highlighted)**
- libraries (group > network)
- imports (flag > 88)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)
- resources (n/a)
- strings (flag > 19)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (signature > unknown)

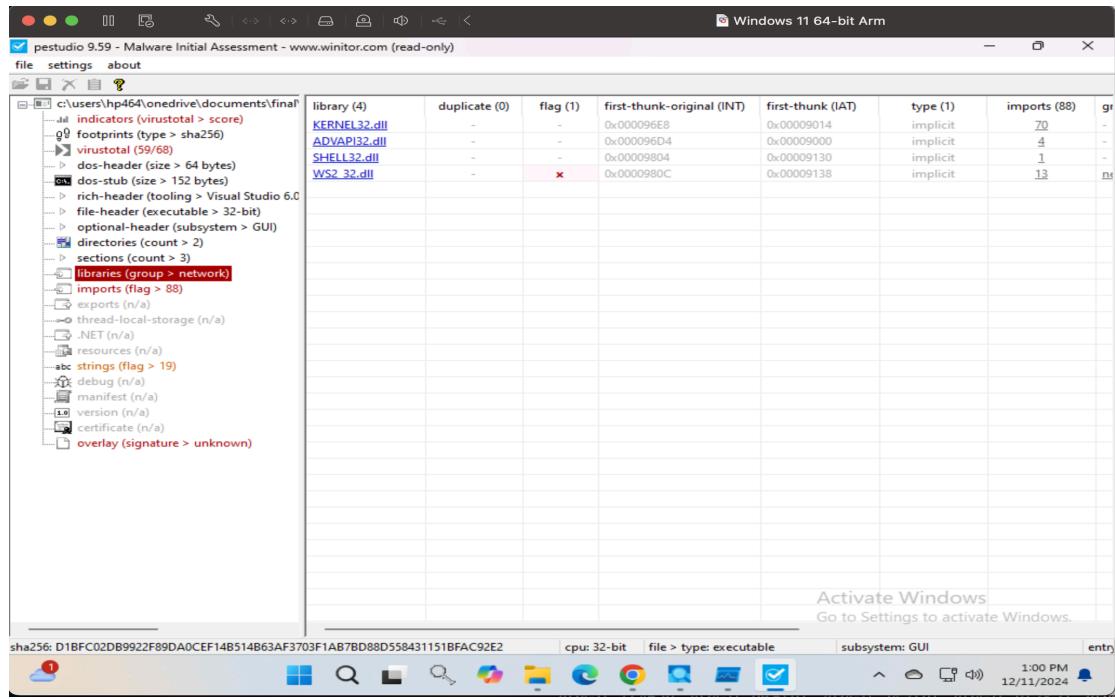
The right pane displays detailed section properties for three sections:

property	value	value	value
section	section[0]	section[1]	section[2]
name	.text	.rdata	.data
footprint > sha256	D5345E3FABF83A57E91ACB...	CB7BA1884CC003DB6DE073...	FA7ABEFA883B57C28A1BD5...
entropy	6.604	5.221	2.201
file-ratio (95.89%)	78.08 %	9.59 %	8.22 %
raw-address (begin)	0x00000400	0x00007600	0x00008400
raw-address (end)	0x00007600	0x00008400	0x00009000
raw-size (35840 bytes)	0x00007200 (29184 bytes)	0x0000E000 (3584 bytes)	0x0000C000 (3072 bytes)
virtual-address	0x00001000	0x00009000	0x0000A000
virtual-size (41548 bytes)	0x000071BA (29114 bytes)	0x0000D76 (3446 bytes)	0x0000231C (8988 bytes)
characteristics	0x60000020	0x40000040	0xC0000040
write	-	-	x
execute	x	-	-
share	-	-	-
self-modifying	-	-	-
virtual	-	-	-
items			
directory > import	-	0x00009670	-
directory > import-address	-	0x00009000	-
base-of-code	0x00001000	-	-
base-of-data	-	0x00009000	-
entry-point	0x0000352F	-	-

At the bottom, the status bar shows: sha256: D1BFC02DB9922F89DA0CEF14B514B63AF3703F1AB7BD88D558431151BFAC92E2, cpu: 32-bit, file > type: executable, subsystem: GUI, entry.

b) Libraries

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



c) imports

impo... (88)	fla...	first-thunk-original...	first-thunk (IAT)	hint	group (0)	technique (9)	type (5)	ordi...	library (13)
GetLogicalDrives	-	0x000098A0	0x000098A0	288 (0x0120)	reconnaissance	-	implicit	-	KERNEL32.dll
GetSystemDirectoryA	-	0x0000987A	0x0000987A	345 (0x0159)	reconnaissance	T1083 File ...	implicit	-	KERNEL32.dll
GetStartupInfoA	-	0x00009BFC	0x00009BFC	336 (0x0150)	reconnaissance	-	implicit	-	KERNEL32.dll
GetUserNameA	-	0x00009A74	0x00009A74	215 (0x00D7)	reconnaissance	T1033 Syst...	implicit	-	ADVAPI32.dll
4_(connect)	x	0x80000004	0x80000004	0 (0x0000)	network	-	implicit	x	WS2_32.dll
3_(closesocket)	x	0x80000003	0x80000003	0 (0x0000)	network	-	implicit	x	WS2_32.dll
16_(recv)	x	0x80000010	0x80000010	0 (0x0000)	network	-	implicit	x	WS2_32.dll
11_(inet_addr)	x	0x8000000B	0x8000000B	0 (0x0000)	network	-	implicit	x	WS2_32.dll
111_(WSAGetLastError)	x	0x8000006F	0x8000006F	0 (0x0000)	network	-	implicit	x	WS2_32.dll
12_(inet_ntoa)	x	0x8000000C	0x8000000C	0 (0x0000)	network	-	implicit	x	WS2_32.dll
57_(gethostvalue)	x	0x80000039	0x80000039	0 (0x0000)	network	-	implicit	x	WS2_32.dll
115_(WSAStartup)	x	0x80000073	0x80000073	0 (0x0000)	network	-	implicit	x	WS2_32.dll
9_(htonl)	x	0x80000009	0x80000009	0 (0x0000)	network	-	implicit	x	WS2_32.dll
23_(socket)	x	0x80000017	0x80000017	0 (0x0000)	network	-	implicit	x	WS2_32.dll
52_(gethostbynamevalue)	x	0x80000034	0x80000034	0 (0x0000)	network	-	implicit	x	WS2_32.dll
19_(send)	x	0x80000013	0x80000013	0 (0x0000)	network	-	implicit	x	WS2_32.dll
IsBadCodePtr	-	0x00009CF2	0x00009CF2	434 (0x01B2)	memory	-	implicit	-	KERNEL32.dll
IsBadWritePtr	-	0x00009C90	0x00009C90	440 (0x01B8)	memory	-	implicit	-	KERNEL32.dll
HeapReAlloc	-	0x00009C82	0x00009C82	418 (0x01A2)	memory	-	implicit	-	KERNEL32.dll
VirtualAlloc	x	0x00009C72	0x00009C72	699 (0x28B)	memory	T1055 Pro...	implicit	-	KERNEL32.dll
GetStringTypeW	-	0x00009C60	0x00009C60	342 (0x0156)	memory	-	implicit	-	KERNEL32.dll
HeapFree	-	0x00009A F6	0x00009A F6	415 (0x019F)	memory	-	implicit	-	KERNEL32.dll
HeapAlloc	-	0x00009B28	0x00009B28	409 (0x0199)	memory	-	implicit	-	KERNEL32.dll
HeapDestroy	-	0x00009C0E	0x00009C0E	413 (0x019D)	memory	-	implicit	-	KERNEL32.dll
HeapCreate	-	0x00009C1C	0x00009C1C	411 (0x019B)	memory	-	implicit	-	KERNEL32.dll
VirtualFree	-	0x00009C2A	0x00009C2A	703 (0x028F)	memory	T1055 Pro...	implicit	-	KERNEL32.dll
GetStringTypeA	-	0x00009C4E	0x00009C4E	339 (0x0153)	memory	-	implicit	-	KERNEL32.dll
FindClose	-	0x00009884	0x00009884	144 (0x0090)	file	-	implicit	-	KERNEL32.dll
FindNextFileA	x	0x000098D0	0x000098D0	157 (0x009D)	file	T1083 A... File ...	implicit	-	KERNEL32.dll
FileTimeToSystemTime	-	0x000098E0	0x000098E0	138 (0x008A)	file	-	implicit	-	KERNEL32.dll
FindFirstFileA	x	0x000098F8	0x000098F8	148 (0x0094)	file	T1083 File ...	implicit	-	KERNEL32.dll

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

- Gethostname: 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

	encoding (2)	size (bytes)	location	flag (19)	label (64)	group (12)	value (575)
indicators (vir)	ascii	14	section:rdata	-	import	-	SetHandleCount
footprints (typ)	ascii	19	section:rdata	-	import	-	MultiByteToWideChar
virustotal (59/	ascii	12	section:rdata	-	import	-	IsBadReadPtr
> dos-header (si)	ascii	9	section:rdata	-	import	-	GetCInfo
dos-stub (size)	ascii	8	section:rdata	-	import	-	GetOEMCP
rich-header (tc)	ascii	45	section:data	-	guid	-	SOFTWARE\Microsoft\Windows\CurrentVersion\Run
file-header (ex)	ascii	4	section:data	-	file	-	.PAD
optional-head	ascii	9	section:data	-	url-pattern	-	127.0.0.1
directories (co)	ascii	9	section:data	-	file	-	\java.exe
sections (cou)	ascii	4	section:data	-	format-stru	-	%d
libraries (group)	ascii	28	section:data	-	format-stru	-	%4d-%02d-%02d %02d%02d:%02d
imports (flag >	ascii	3	section:data	-	utility	-	DIR
exports (n/a)	ascii	7	section:data	-	utility	-	cmd.exe
thread-local-st	ascii	15	section:data	-	rtti	-	:AVType_info@@
.NET (n/a)	ascii	5	rich-header	-	-	-	Rich&
resources (r/s)	ascii	5	-	-	-	-	.text
strings (flag >	ascii	6	-	-	-	-	'.data
debug (n/a)	ascii	7	-	-	-	-	@.data
manifest (n/a)	ascii	4	section:text	-	-	-	SVWh
version (n/a)	ascii	4	section:text	-	-	-	JSNh
certificate (n/a)	ascii	4	section:text	-	-	-	L\$bj
overlay (signat	ascii	4	section:text	-	-	-	t\$S3
	ascii	3	section:text	-	-	-	JS
	ascii	4	section:text	-	-	-	D\$0Q
	ascii	5	section:text	-	-	-	L\$PQ
	ascii	4	section:text	-	-	-	T\$0h
	ascii	3	section:text	-	-	-	.^[
	ascii	3	section:text	-	-	-	.^3
	ascii	3	section:text	-	-	-	VWh
	ascii	5	section:text	-	-	-	t@VWj
	ascii	3	section:text	-	-	-	.^3

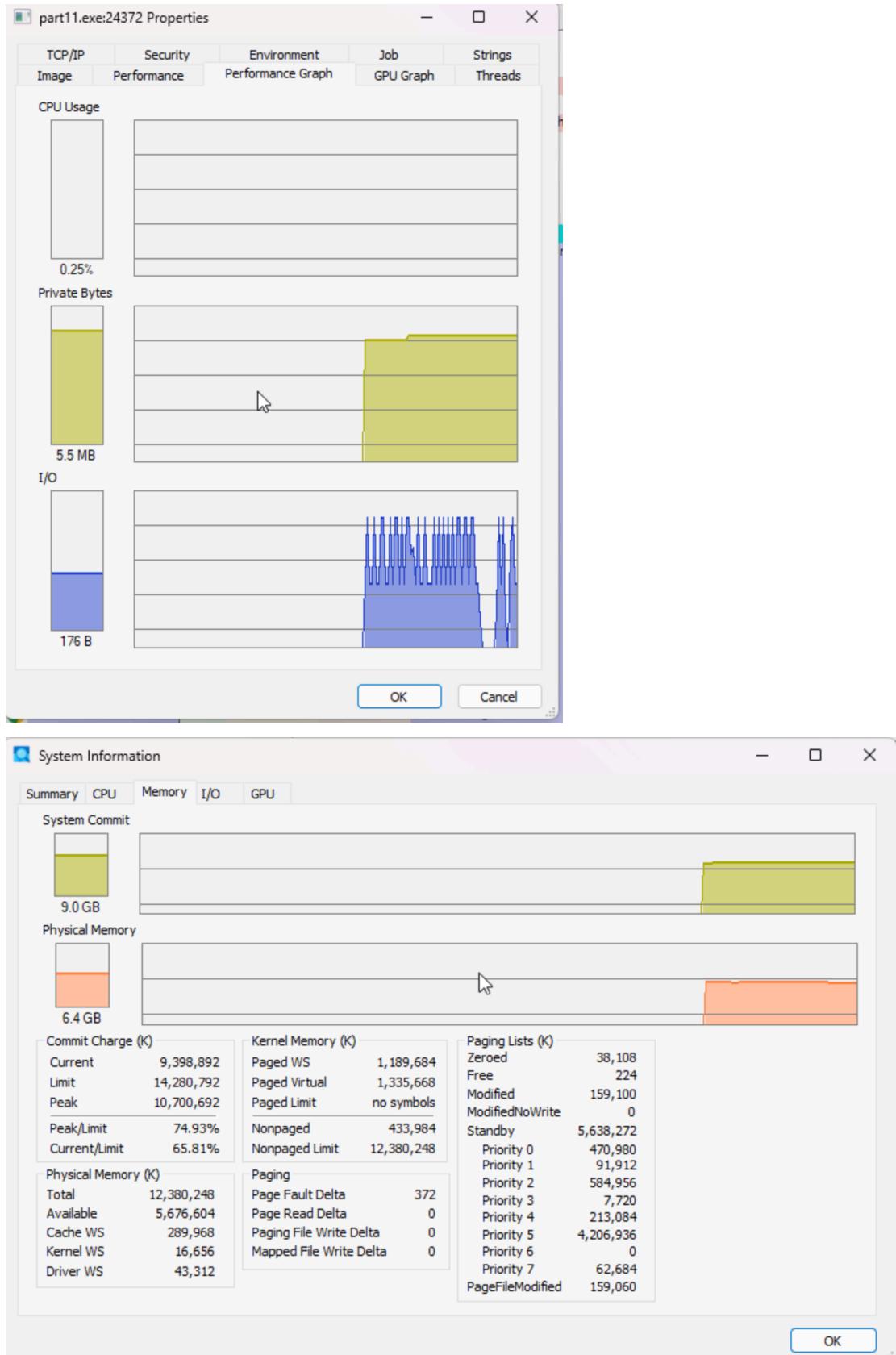
It sets the key in 'SOFTWARE\Microsoft\Windows\CurrentVersion\Run' to 'C:\DOCUME~1\User\java.exe', which is a copy of itself that it made. Some host-based signatures are in documents and settings for the user and copies under 'java.exe'.

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

Process Monitor - Sysinternals: www.sysinternals.com

Windows 11 64-bit Arm

Process Name	PID	Operation	Path	Result	Detail
2:023... part11.exe	13764	Process Start		SUCCESS	Parent PID: 6336, ...
2:023... part11.exe	13764	Thread Create		SUCCESS	Thread ID: 10588
2:023... part11.exe	13764	Load Image	C:\Users\hp464\OneDrive\Documents\final\11.12.2024 (1)\11.12.2024\part11\part11.exe	SUCCESS	Image Base: 0x400...
2:023... part11.exe	13764	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7fd...
2:023... part11.exe	13764	Load Image	C:\Windows\SyChpe32\ntdll.dll	SUCCESS	Image Base: 0x773...
2:023... part11.exe	13764	CreateFile	C:\Windows\Prefetch\PART11.EXE-EB5FA8E2.pf	SUCCESS	Desired Access: G...
2:023... part11.exe	13764	QueryStandard...	C:\Windows\Prefetch\PART11.EXE-EB5FA8E2.pf	SUCCESS	AllocationSize: 12...
2:023... part11.exe	13764	ReadFile	C:\Windows\Prefetch\PART11.EXE-EB5FA8E2.pf	SUCCESS	Offset: 0, Length: 9...
2:023... part11.exe	13764	CloseFile	C:\Windows\Prefetch\PART11.EXE-EB5FA8E2.pf	SUCCESS	
2:023... part11.exe	13764	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	REPARSE	Desired Access: R...
2:023... part11.exe	13764	RegOpenKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	Desired Access: R...
2:023... part11.exe	13764	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\ACP	SUCCESS	Type: REG_SZ, Le...
2:023... part11.exe	13764	RegQueryValue	HKLM\System\CurrentControlSet\Control\Nls\CodePage\OEMCP	SUCCESS	Type: REG_SZ, Le...
2:023... part11.exe	13764	RegCloseKey	HKLM\System\CurrentControlSet\Control\Nls\CodePage	SUCCESS	
2:023... part11.exe	13764	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
2:023... part11.exe	13764	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
2:023... part11.exe	13764	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibleDeadlock	NAME NOT FOUND	Length: 80
2:023... part11.exe	13764	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
2:023... part11.exe	13764	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Q...
2:023... part11.exe	13764	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Q...
2:023... part11.exe	13764	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
2:023... part11.exe	13764	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	SUCCESS	Desired Access: Q...
2:023... part11.exe	13764	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
2:023... part11.exe	13764	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Q...
2:023... part11.exe	13764	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Q...
2:023... part11.exe	13764	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
2:023... part11.exe	13764	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
2:023... part11.exe	13764	CreateFile	C:\Windows	SUCCESS	Desired Access: E...
2:023... part11.exe	13764	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7fd...
2:023... part11.exe	13764	Load Image	C:\Windows\System32\wow64base.dll	SUCCESS	Image Base: 0x7fd...
2:023... part11.exe	13764	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7fd...
2:023... part11.exe	13764	CreateFile	C:\Windows\System32\wow64con.dll	SUCCESS	Image Base: 0x7fd...
2:023... part11.exe	13764	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: R...
2:023... part11.exe	13764	QueryNameInfo...	C:\Windows	SUCCESS	Desired Access: R...
2:023... part11.exe	13764	CloseFile	C:\Windows	SUCCESS	Name: '\Windows
2:023... part11.exe	13764	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	SUCCESS	Desired Access: Q...
2:023... part11.exe	13764	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\part...	NAME NOT FOUND	Desired Access: Q...
2:023... part11.exe	13764	ReOpenKey	HKLM\Software\Microsoft\Wow64\x86\xtait	NAME NOT FOUND	Desired Access: Q...

Showing 1,846 of 578,141 events (0.31%) Backed by virtual memory

2:023... part11.exe 13764 2:13 PM 12/11/2024

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.

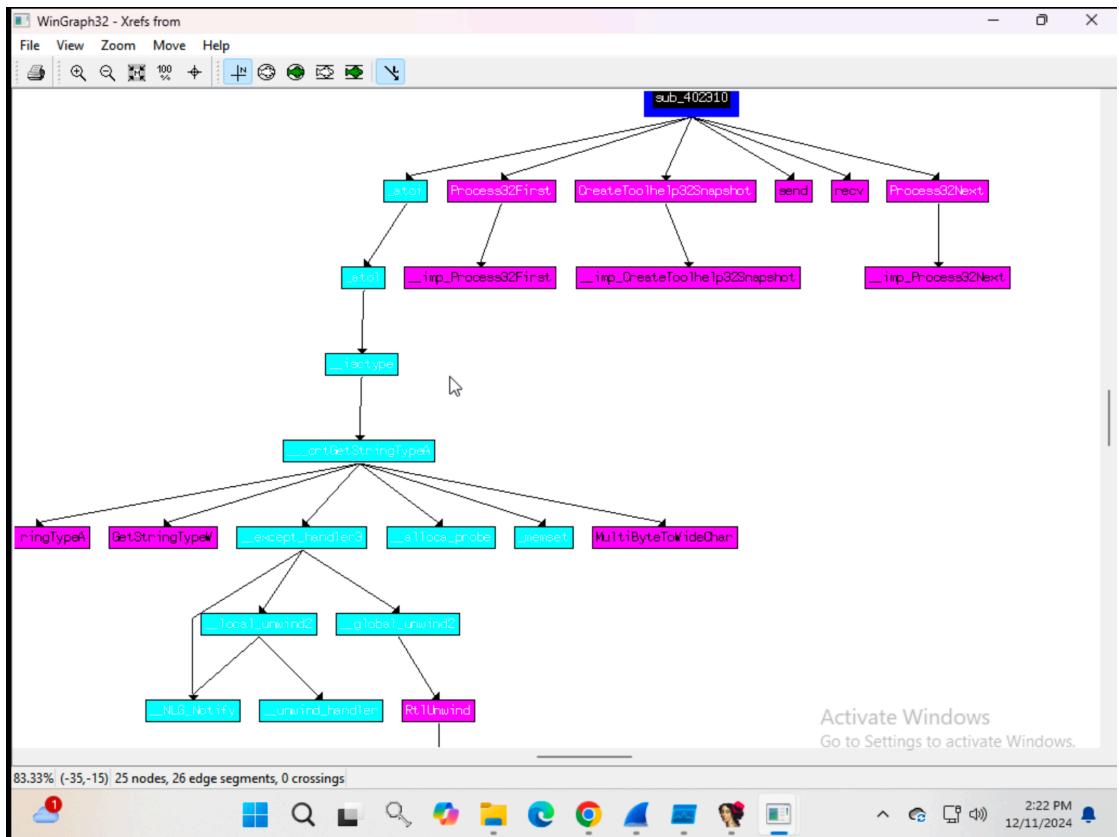
WriteFile: Sends commands or responses through a pipe.

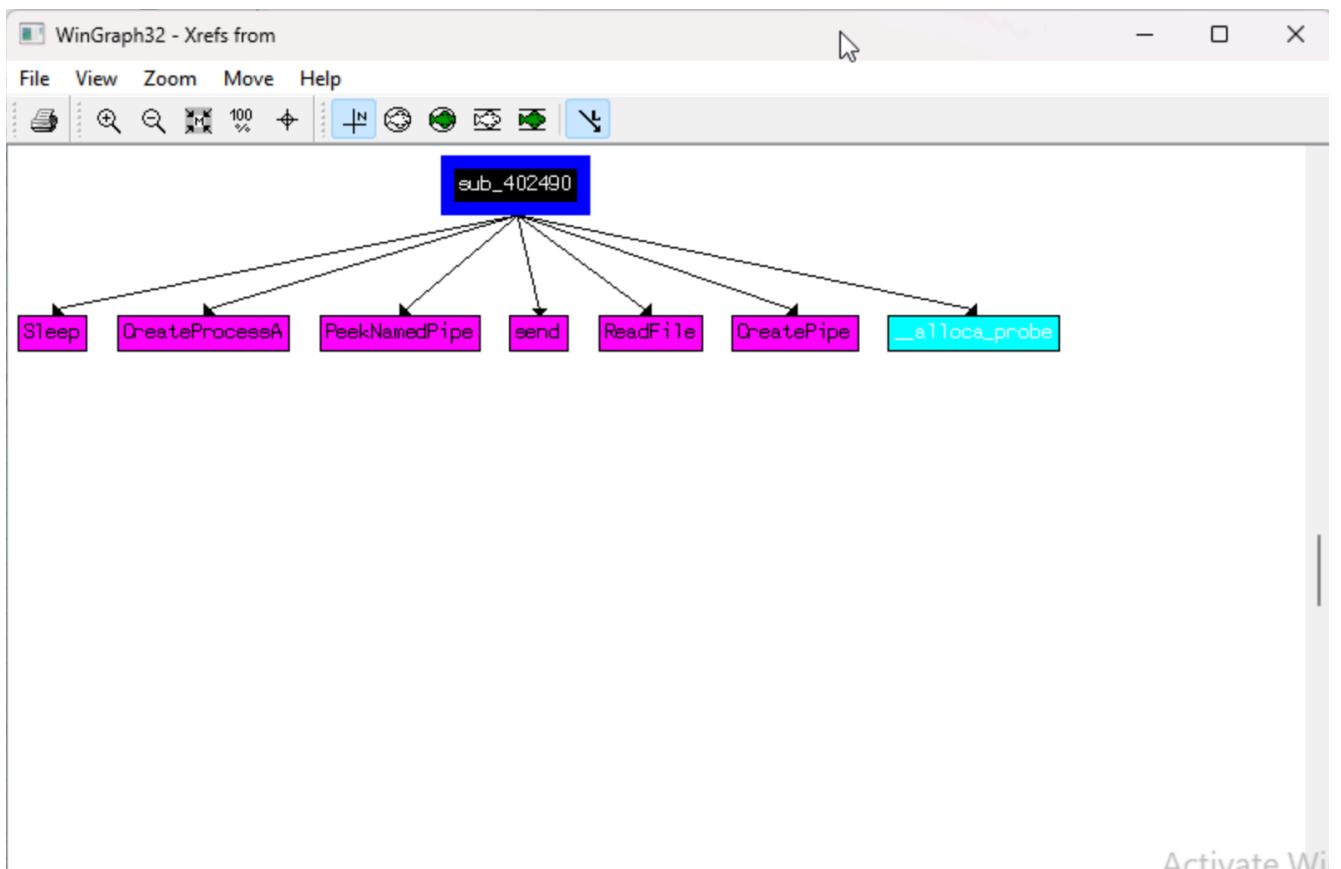
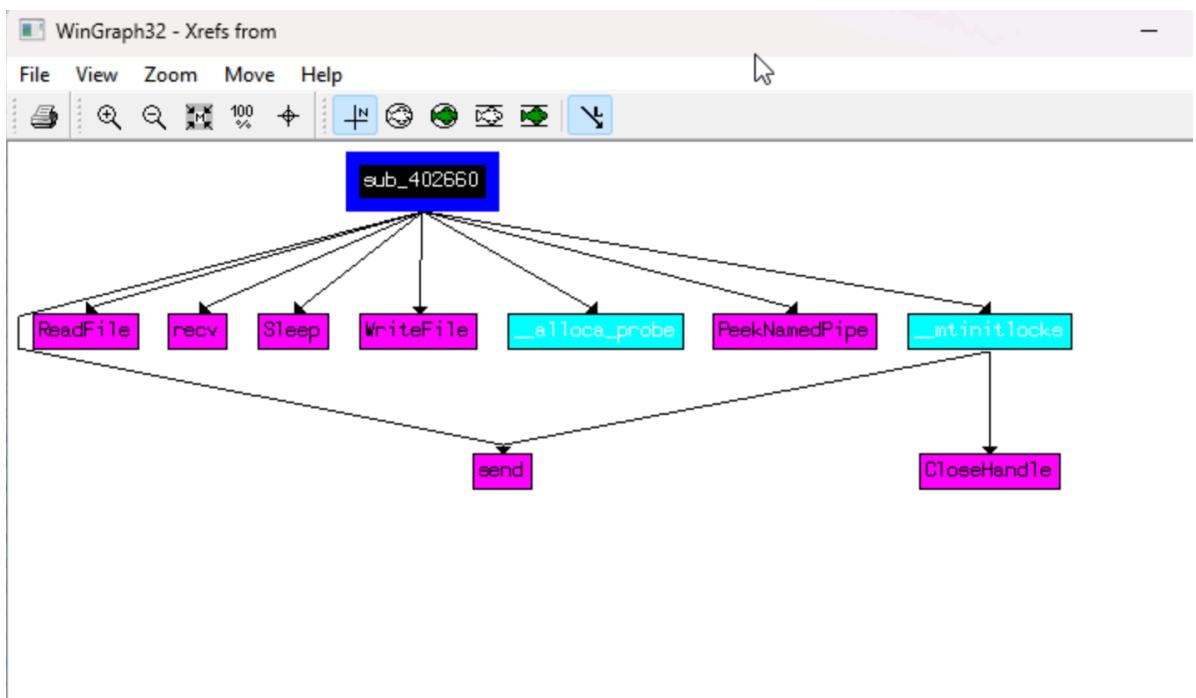
Upload File (0x00402210):

- 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.





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

Library function Regular function Instruction Data Unexplored External symbol Lumina function

Functions IDA View-A Hex View-1 Local Types Imports Exports

Function name

- sub_401A20
- sub_402050
- sub_4020A0
- sub_4020F0
- sub_402210
- sub_402310
- sub_402440
- sub_402490
- _mtriflocks
- sub_402660
- sub_402880
- sub_4028C0
- Process32Next
- Process32First
- CreateToolhelp32Snapshot
- _atoi
- _atoi
- _strtok
- _strcpy
- _fclose
- _fread
- _fseek
- _fopen
- _fsopen
- _open

Line 14 of 170, /sub_402310

xt:00402310 var_12C = dword ptr -12Ch
xt:00402310 pe = PROCESSENTRY32 ptr -128h
xt:00402310 s = dword ptr 4

xt:00402310 sub esp, 238h
push ebx
push 0 ; th32ProcessID
push 2 ; dwFlags
mov [esp+244h+pe.dwSize], 128h
call CreateToolhelp32Snapshot
lea ecx, [esp+23Ch+pe]
mov [esp+23Ch+hSnapshot], eax
push ecx ; lppe
push eax ; hSnapshot
mov [esp+244h+var_12C], 1
call Process32First
mov ebx, [esp+23Ch+s]
test eax, eax
jz loc_4023F8
push ebp
mov ebp, ds:recv
push esi
push edi

xt:00402360 loc_402360: ; CODE XREF: sub_402310+DF↓
lea edi, [esp+248h+pe.szExeFile]
xor eax, eax

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

Activate Windows
Go to Settings to activate Windows.

Python

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

Library function Regular function Instruction Data Unexplored External symbol Lumina function

Functions IDA View-A Hex View-1 Local Types Imports Exports

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
- CreateToolhelp32Snapshot
- _atol
- _atoi
- _strtok
- _strncpy
- _fclose
- _fread
- _fseek
- _fsopen
- _fopen
- connectback

```

xt:00402660 var_4      = dword ptr -4
xt:00402660 s          = dword ptr 4
xt:00402660 lpBuffer   = dword ptr 8
xt:00402660
    mov    eax, 100Ch
    call   _alloca_probe
    push   ebx
    xor    ebx, ebx
    push   esi
    mov    esi, [esp+1014h+lpBuffer]
    push   edi
    mov    [esp+1018h+var_100C], ebx
    xor    eax, eax
    ; CODE XREF: sub_402660+2B1j
    mov    cl, [eax+esi]
    xor    cl, 55h
    mov    [eax+esi], cl
    inc    eax
    cmp    eax, 100h
    jl     short loc_40267C
    mov    edi, esi
    or    ecx, 0xFFFFFFFFh
    xor    eax, eax
    push   ebx
    push   eax
    repne scasd
    mov    eax, hfile
00001A60 00402660: sub_402660 (Synchronized with Hex View-1)

```

Line 18 of 170, /sub_402660

Output

Lumina: Signature decryption failed with code: -2
The initial autoanalysis has been finished.
Command "JumpAsk" failed
Command "JumpAsk" failed

Activate Windows
Go to Settings to activate Windows.

Python

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 Professional: <https://hex-rays.com/ida-pro>

