

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ



Syieun university for technology

University since application

IS department level 4

The Title of Research

(MALWARE STATIC ANALYSIS)

GROUP (C)

Students' preparation

Nader Ameen AL Hwaimail

SUPERVISE By

A/Shadi Bajri

The Session 2023-2024

The Files	Types
C1	Not Malware
C2	Malware (Trojan)
C3	Not Malwar
C4	Not Malwar

Info

There is a similarity between files C3 and C4

```

~/.../C/C $ ssdeep * > fuzzy.txt
~/.../C/C $ ssdeep -m fuzzy.txt * -s
/storage/emulated/0/Project_1/C/C/C1 matches fuzzy.txt:/storage/emulated/0/Project_1/C/C/C1 (100)
/storage/emulated/0/Project_1/C/C/C2 matches fuzzy.txt:/storage/emulated/0/Project_1/C/C/C2 (100)
/storage/emulated/0/Project_1/C/C/C3 matches fuzzy.txt:/storage/emulated/0/Project_1/C/C/C3 (100)
/storage/emulated/0/Project_1/C/C/C3 matches fuzzy.txt:/storage/emulated/0/Project_1/C/C/C4 (90)
/storage/emulated/0/Project_1/C/C/C4 matches fuzzy.txt:/storage/emulated/0/Project_1/C/C/C3 (90)
/storage/emulated/0/Project_1/C/C/C4 matches fuzzy.txt:/storage/emulated/0/Project_1/C/C/C4 (100)
/storage/emulated/0/Project_1/C/C/-s: No such file or directory

```

FuzzyHash



C4



C3

Trojan:

The Trojan virus first appeared in the early 1970s and was named after the famous Trojan Horse from Greek mythology. The target entity of a Trojan virus is typically a computer system or network, with the goal of gaining unauthorized access or causing damage to the system.

Trojan viruses can cause a variety of damages, including stealing sensitive information such as passwords and financial data, deleting files, disrupting system performance, and allowing remote access to the infected system for cybercriminals.

The reference

<https://www.fortinet.com/>

<https://www.webroot.com/>

Chapter I

C1

1- Files' Fingerprints (MD5, SHA1):

md5 ----> fcc8437ee3696f3caf5ac9e59ed8772e

sha1 ----> 8333718b08e91907204b962d0d2f3db7445e65ff

MD5:	fcc8437ee3696f3caf5ac9e59ed8772e
SHA1:	8333718b08e91907204b962d0d2f3db7445e65ff

Fingerprint

2- The first 3 result in virustotal:

Join the [VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

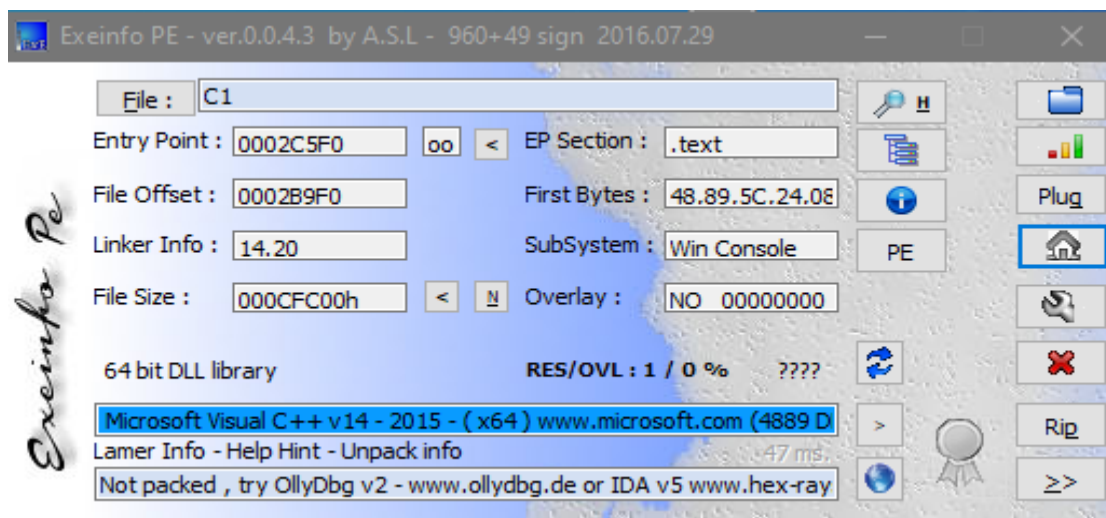
Security vendors' analysis ⓘ	Do you want to automate checks?
ClamAV	❗ Win.Malware.Rivts-10003407-0
Acronis (Static ML)	✅ Undetected
AhnLab-V3	✅ Undetected
AhnLab-V3	✅ Undetected
Acronis (Static ML)	✅ Undetected
ClamAV	❗ Win.Malware.Rivts-10003407-0

3- Text strings containing flags to mark the file as malicious or harmless:

4- was file has been packed or compressed (Packed)?

- BY Exeinfo PE the file C1 not packed

Not packed , try OllyDbg v2 - www.ollydbg.de or IDA v5 www.hex-rays.com or x64 debug v0024 www.x64dbg.com



5- Used libraries:

- There are 66 libraries in File C1

library (66)	flag (9)	first-thunk-original (INT)	type (2)	imports (393)	group	description
msvcrt.dll	-	0x000C38F8	implicit	42	-	Microsoft (
USER32.dll	-	0x000C35E8	implicit	3	-	Multi-User
ntdll.dll	-	0x000C3D50	implicit	88	-	NT Layer
api-ms-win-core...	-	0x000C3938	implicit	24	-	n/a
api-ms-win-core...	x	0x000C38B8	implicit	10	registry	ApiSet Stut
api-ms-win-core...	-	0x000C36E8	implicit	2	-	n/a
api-ms-win-core...	-	0x000C36A8	implicit	4	-	n/a
api-ms-win-core...	-	0x000C3728	implicit	2	-	n/a
api-ms-win-core...	-	0x000C3A70	implicit	12	-	n/a
api-ms-win-core...	-	0x000C3700	implicit	4	-	n/a
api-ms-win-core...	-	0x000C3A00	implicit	3	-	n/a
api-ms-win-core...	x	0x000C3808	implicit	17	-	ApiSet Stut

libraries	Short Description
msvcrt.dll	Microsoft C++ Runtime Library
USER32.dll	Multi-User Windows USER API Client Library
dwmapi.dll	Microsoft Desktop Window Manager API

Additional details: msvcrt.dll

The msvcrt.dll file is a part of the "Microsoft Visual Studio 6.0" and is crucial for most applications to work properly. It also contains program code that enables applications written in "Microsoft Visual C++" to run properly. The program code is basically string comparison tools and mathematic operations such as trigonometric operations. This is a very valuable file to programmers.

Some games or applications may need the file in the game/application installation folder. Copying it from Windows systemfolder to the install-folder of the game/application should fix that problem. <https://www.dll-files.com/>

USER32.dll

The "USER32.dll" library is a dynamic link library (DLL) file that is a part of the Windows operating system. It contains a set of functions and components that provide user interface services for Windows applications.

The "USER32.dll" library is responsible for managing and controlling windows, menus, dialog boxes, buttons, scrollbars, and other graphical elements of the user interface. It provides functions for creating and manipulating windows, handling user input, managing keyboard and mouse events, and performing various UI-related tasks. As for the source of the "USER32.dll" library, it is developed and provided by Microsoft as an integral component of the Windows operating system. It is not available for separate download or distribution. The library is typically installed along with the Windows operating system and is located in the "System32" folder on a Windows system. **More detail** <https://strontic.github.io/xcyclopedia/library/user32.dll>

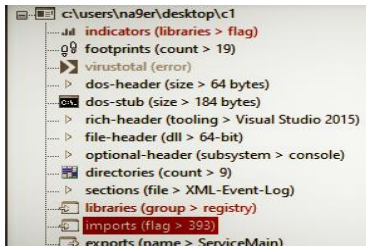
dwmapi.dll

The dwmapi.dll file is a crucial component of the Windows operating system, responsible for managing visual effects and GUI elements. However, it can encounter errors that may disrupt the functioning of applications and processes. By following the methods mentioned above, such as restarting the computer, running virus scans, updating Windows and drivers, performing SFC scans, and reinstalling or repairing applications, users can effectively resolve dwmapi.dll errors and restore the smooth operation of their Windows system.

<https://malwaretips.com/blogs/dwmapi-dll>

6- Import Function:

- There are 393 import functions in file C1



imports (393)	flag (115)	first-thunk-original (INT)	first-thunk (IAT)	hint	group (17)
NtWaitForSingleObject	-	0x000000000000C59F2	0x000000000000C59F2	652 (0x028C)	synchronizati
RtlLeaveCriticalSection	-	0x000000000000C479E	0x000000000000C479E	1232 (0x04D0)	synchronizati
RtlEnterCriticalSection	-	0x000000000000C4784	0x000000000000C4784	941 (0x03AD)	synchronizati
NtCreateEvent	-	0x000000000000C45D2	0x000000000000C45D2	276 (0x0114)	synchronizati
NtOpenEvent	x	0x000000000000C44DC	0x000000000000C44DC	414 (0x019E)	synchronizati
OpenSemaphoreW	-	0x000000000000C4CD8	0x000000000000C4CD8	33 (0x0021)	synchronizati
InitializeCriticalSection	-	0x000000000000C4E8C	0x000000000000C4E8C	24 (0x0018)	synchronizati
WaitForMultipleObjectsEx	-	0x000000000000C4A66	0x000000000000C4A66	53 (0x0035)	synchronizati
AcquireSRWLockExclusive	-	0x000000000000C4B78	0x000000000000C4B78	0 (0x0000)	synchronizati
CreateSemaphoreExW	-	0x000000000000C4E76	0x000000000000C4E76	11 (0x000B)	synchronizati
CreateMutexW	-	0x000000000000C509E	0x000000000000C509E	10 (0x000A)	synchronizati
LeaveCriticalSection	-	0x000000000000C4E5E	0x000000000000C4E5E	29 (0x001D)	synchronizati

Import Fun	Short Description
NtOpenEvent	Opens an existing event object
DeleteTimerQueueTimer	Deletes a timer from queue
RegisterServiceCtrlHandlerExW	Registers handler for controlling Windows services.

Additional details From: → <https://learn.microsoft.com/>

NtOpenEvent

ZwOpenEvent can open either notification or synchronization events. Events are used to coordinate execution. File system drivers can use events to enable a caller to wait for completion of the requested operation until the given event is set to the Signaled state.

```

C++
Copy

NTSYSCALLAPI NTSTATUS ZwOpenEvent(
    [out] PHANDLE      EventHandle,
    [in]  ACCESS_MASK   DesiredAccess,
    [in]  POBJECT_ATTRIBUTES ObjectAttributes
);

```

Syntax

DeleteTimerQueueTimer

function is a Windows API function that is used to delete a timer from a timer queue.

Timer queues are used to schedule timer callbacks, allowing applications to execute certain code at specific intervals or after a certain amount of time has elapsed. The **DeleteTimerQueueTimer** function allows you to cancel or remove a previously created timer from the timer queue, preventing the associated callback function from being executed.

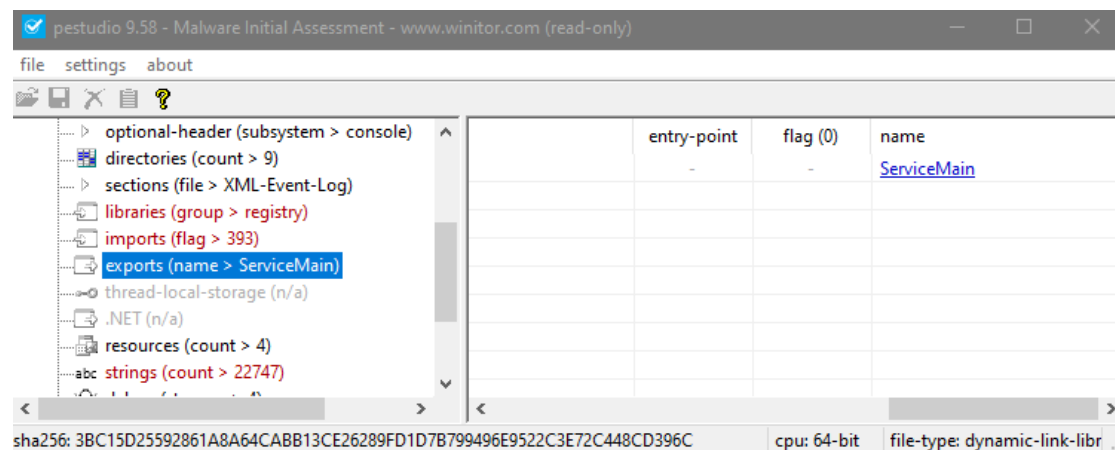
By calling **DeleteTimerQueueTimer**, you provide the handle to the timer queue and the timer to be deleted. Upon successful deletion, the resources associated with the timer are released, and the timer is removed from the queue.

```
C++ Copy  
  
BOOL DeleteTimerQueueTimer(  
    [in, optional] HANDLE TimerQueue,  
    [in]           HANDLE Timer,  
    [in, optional] HANDLE CompletionEvent  
);
```

Syntax

7- Export Function:

There is one only export function in file C1



Export Fun	Short Description
ServiceMain	Windows service entry point

A **ServiceMain** function in a service DLL can be coded as for one in a service program. Refer to Microsoft's documentation. However, some work that might be done in a service program can be avoided in a service DLL because it is already done by SVCHOST. First, there is per-process initialization which is not only convenient to be done by SVCHOST but is perhaps better attempted only once per process (as with initializing COM security). Second, though only since version 5.1, SVCHOST provides service DLLs with access to shared code and data. To learn the addresses, a service DLL should export a function named **SvchostPushServiceGlobals**, which SVCHOST calls before each call to any **ServiceMain** function in the DLL.

<https://www.geoffchappell.com/>.

Example

This example uses the following global definitions.

C++

Copy

```
#define SVCNAME TEXT("SvcName")

SERVICE_STATUS      gSvcStatus;
SERVICE_STATUS_HANDLE gSvcStatusHandle;
HANDLE                ghSvcStopEvent = NULL;
```

8- Section:

There are 7 section in file C1

sec	Section [0]	Section [1]	Section [2]	Section [3]	Section [4]	Section [4]	Section [6]
Name	.text	.rdata	.data	.pdata	.didat	.rsrc	.reloc
Raw-size in bytes	537088 bytes	266752 bytes	1536 bytes	25088 bytes	1024 bytes	11776 bytes	6656 bytes
Virtual size in bytes	536610 bytes	266342 bytes	15976 bytes	24756 bytes	776 bytes	11576 bytes	6512 bytes
Entry point .txt	0x0002C5F0	---	----	---	----	---	----
Raw add begin	0x00000400	0x00008360	0x0000C480	0x0000C4E0	0x0000CB00	0x0000CB40	0x0000CE20
Raw add end	0x00008360	0x0000C480	0x0000C4E0	0x0000CB00	0x0000CB40	0x0000CE20	0x0000CF00

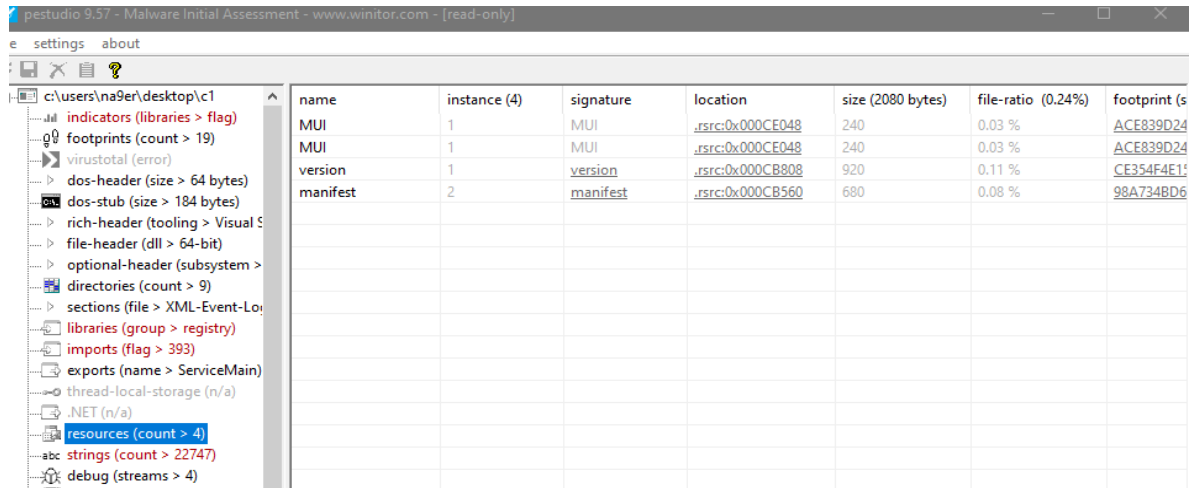
pestudio 9.57 - Malware Initial Assessment - www.winitor.com - [read-only]

file settings about

	value	value	value	value	value
section[2]	section[3]	section[4]	section[5]	section[6]	
.data	.pdata	.didat	.rsrc	.reloc	
B9BA01E6161AFC659238176...	B53C470EE134B3428F692421...	081CC183F747B9BA7A6B190...	0E6CA2998DF98FE3749A8C4...	203EFFBA93F6C3051E26B50...	
3.844	5.893	2.460	3.807	5.415	
0.18 %	2.95 %	0.12 %	1.38 %	0.78 %	
0x000C4800	0x000C4E00	0x000CB000	0x000CB400	0x000CE200	
0x000C4E00	0x000CB000	0x000CB400	0x000CE200	0x000CFC00	
0x00000600 (1536 bytes)	0x00006200 (25088 bytes)	0x00000400 (1024 bytes)	0x00002E00 (11776 bytes)	0x00001A00 (6656 bytes)	
0x000C7000	0x000CB000	0x000D2000	0x000D3000	0x000D6000	
0x00003E68 (15976 bytes)	0x000060B4 (24756 bytes)	0x00000308 (776 bytes)	0x00002D38 (11576 bytes)	0x00001970 (6512 bytes)	
0xC0000040	0x40000040	0xC0000040	0x40000040	0x42000040	
x	-	x	-	-	

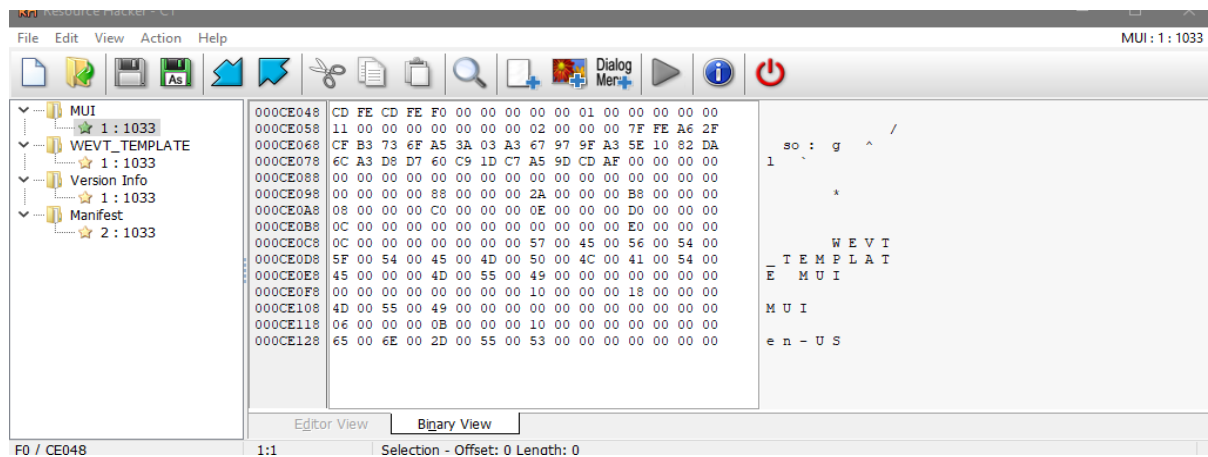
9- Count of resource:

There are 4 resources in file C1



name	instance (4)	signature	location	size (2080 bytes)	file-ratio (0.24%)	footprint (s)
MUI	1	MUI	.rsrc:0x000CE048	240	0.03 %	ACE839D24
MUI	1	MUI	.rsrc:0x000CE048	240	0.03 %	ACE839D24
version	1	version	.rsrc:0x000CB808	920	0.11 %	CE354F4E1
manifest	2	manifest	.rsrc:0x000CB560	680	0.08 %	98A7348D6

BY pestudio tool



Chapter II

C2

1- Files' Fingerprints (MD5, SHA1):

md5 ----> 28247211d1eb08370aa363f08821a653

sha1 ----> 9d16705ff7bd06d238b389f9320e1c646639c2f7

MD5:	28247211d1eb08370aa363f08821a653
SHA1:	9d16705ff7bd06d238b389f9320e1c646639c2f7

2- The first 3 result in virustotal:

86cb2ece83ce6aa8831c5dfd368aa847f3bae52b1f2eb2a3de093227b42772ec

63 / 72

63 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Similar More

86cb2ece83ce6aa8831c5dfd368aa847f3bae52b1f2eb2a3de093227b42772ec

Size: 73.00 KB | Last Analysis Date: 11 days ago

EXE

peexe direct-cpu-clock-access

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Popular threat label: trojan.poebot/agentwdr Threat categories: trojan worm miner Family labels: poebot agentwdr agentb

Security vendors' analysis

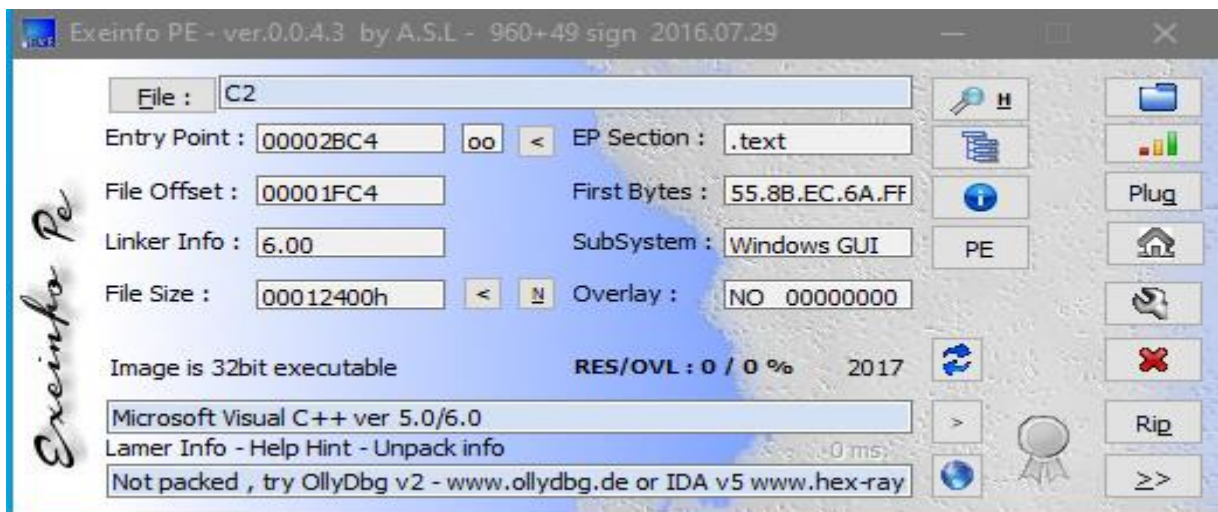
Security vendor	Detection	Security vendor	Detection
AhnLab-V3	Trojan.Win32.Generic.C1979935	Alibaba	Backdoor.Win32/Poebot.19730077
ALYac	Trojan.AgentWDCR.MUF	Antiy-AVL	Worm.Win32.AGeneric
Arcabit	Trojan.AgentWDCR.MUF	Avast	Win32:Evo-gen [Trj]

3- Text strings containing flags to mark the file as malicious or harmless:

The presence of error messages related to the Microsoft Visual C++ Runtime Library, such as "Runtime Error!" and various error codes (e.g., R6002, R6008, R6009, etc.), suggests that the

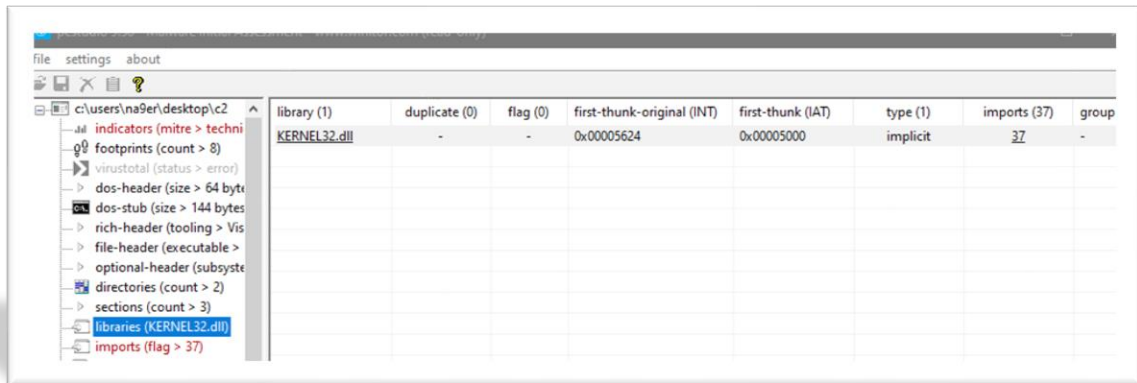
4- was file has been packed or compressed (Packed)?

- BY Exeinfo PE the file C2 not packed



5- Used libraries:

- There is ONE only libraries in File C2



libraries	Short Description
KERNEL32.dll	Windows NT BASE API Client

KERNEL32.dll:

Kernel32.dll is the 32-bit dynamic link library found in the Windows operating system kernel. It handles memory management, input/output operations, and interrupts. When Windows boots up, kernel32.dll is loaded into a protected memory space so other applications do not take that space over.

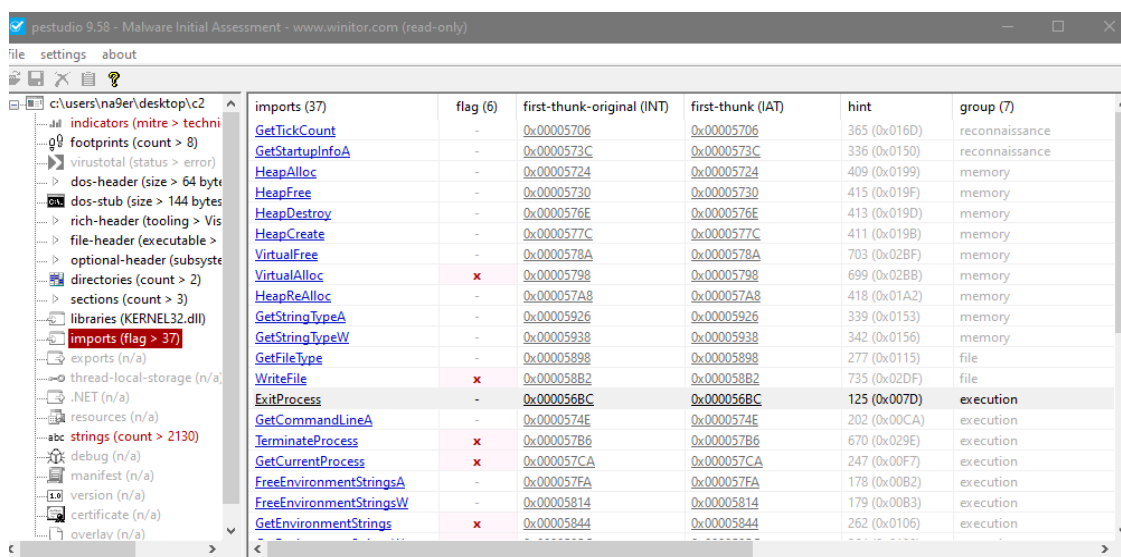
On occasion, though, users may encounter the “invalid page fault” error.

This error occurs when a program or application tries to access kernel32.dll’s protected memory space. Sometimes the error is caused by one particular program or application, and other times it is provoked by multiple files and applications.

The reference <https://www.webopedia.com/>

6- Import Function:

- There are 37 imports functions in file C2



Import Fun	Short Description
VirtualAlloc	Allocate virtual memory
WriteFile	Write to file
ExitProcess	Terminate current process

Additional details from: → <https://learn.microsoft.com/>

VirtualAlloc

The **VirtualAlloc** function is used to allocate memory in the virtual address space of a process. It reserves or commits a region of pages, allowing the process to use that memory for various purposes, such as storing data or executing code.

```

C++ Copy
LPVOID VirtualAlloc(
    [in, optional] LPVOID lpAddress,
    [in]           SIZE_T dwSize,
    [in]           DWORD  flAllocationType,
    [in]           DWORD  flProtect
);

```

Syntax

WriteFile

The **WriteFile** function is used to write data to a file or input/output (I/O) device. It is commonly used to write bytes, characters, or other data to a file, pipe, console, or serial communication resource.

```

C++ Copy
BOOL WriteFile(
    [in]           HANDLE      hFile,
    [in]           LPCVOID     lpBuffer,
    [in]           DWORD       nNumberOfBytesToWrite,
    [out, optional] LPDWORD     lpNumberOfBytesWritten,
    [in, out, optional] LPOVERLAPPED lpOverlapped
);

```

Syntax

ExitProcess

The **ExitProcess** function is used to terminate the calling process and exit it gracefully. It performs the necessary cleanup and terminates the process, including closing open handles and freeing resources.

```

C++ Copy

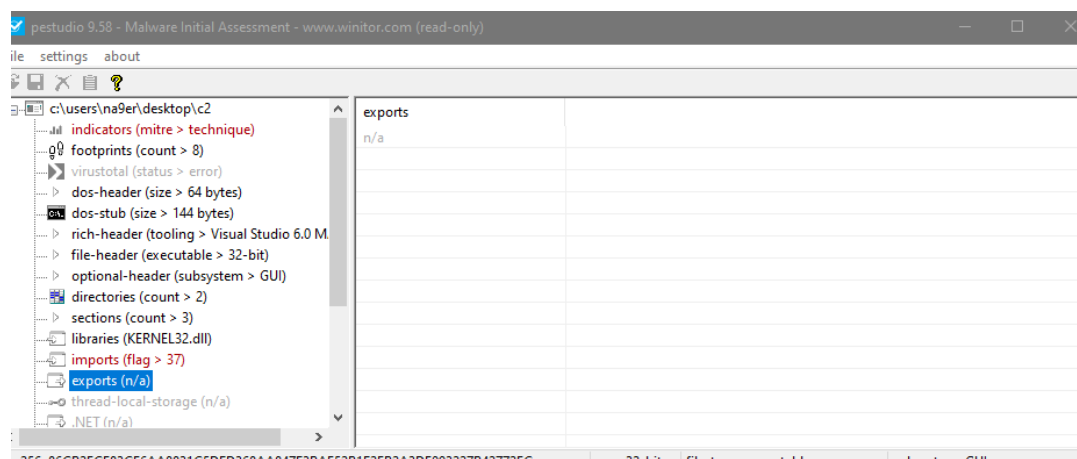
void ExitProcess(
    [in] UINT uExitCode
);

```

Syntax

7- Export Function:

- There is NO exports function in file C2



8- Section: → entropy 7,747

- There are Three section in file C2

sec	Section [0]	Section [1]	Section [2]
Name	.text	.rdata	.data
Raw-size in bytes	16384 bytes	2560 bytes	54784 bytes
Virtual size in bytes	16134 bytes	2378 bytes	55640 bytes
Entry point .txt	0x00002BC4	---	----
Raw add begin	0x00000400	0x00004400	0x00004E00
Raw add end	0x00004400	0x00004E00	0x00012400

CFF Explorer VIII - [C2]

File Settings ?

File: C2

- Dos Header
- NT Headers
- File Header
- Optional Header
- Data Directories [x]
- Section Headers [x]
- Import Directory
- Address Converter

Name	Virtual Size	Virtual Address	Raw Size	Raw Address	Reloc Address	Linenumbers	Relocations N...	Liner
000001C8	000001D0	000001D4	000001D8	000001DC	000001E0	000001E4	000001E8	000001EC
Byte[8]	Dword	Dword	Dword	Dword	Dword	Dword	Word	Word
.text	00003F06	00001000	00004000	00000400	00000000	00000000	0000	0000
.rdata	0000094A	00005000	00000A00	00004400	00000000	00000000	0000	0000
.data	0000D958	00006000	0000D600	00004E00	00000000	00000000	0000	0000

pestudio 9.38 - Malware Initial Assessment - www.winitor.com (read-only)

file settings about

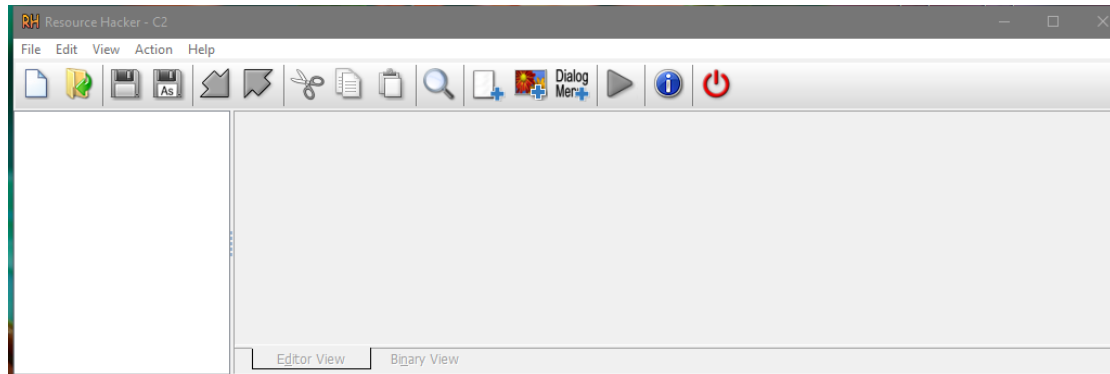
c:\users\n9er\desktop\c2

- indicators (mitre > technique)
- footprints (count > 8)
- virustotal (status > error)
- dos-header (size > 64 bytes)
- dos-stub (size > 144 bytes)
- rich-header (tooling > Visual Studio 6.0 M)
- file-header (executable > 32-bit)
- optional-header (subsystem > GUI)
- directories (count > 2)
- sections (count > 3)
- libraries (KERNEL32.dll)
- imports (flag > 37)
- exports (n/a)
- thread-local-storage (n/a)
- .NET (n/a)

property	value	value	value
section	section[0]	section[1]	section[2]
name	.text	.rdata	.data
footprint > sha256	FBDA15215FBB9BEF6366928...	046928A0786BDA700E015F6...	3753565619F03E459B99DFA
entropy	6.476	6.038	7.949
file-ratio (98.63%)	21.92 %	3.42 %	73.29 %
raw-address (begin)	0x00000400	0x00004400	0x00004E00
raw-address (end)	0x00004400	0x00004E00	0x00012400
raw-size (73728 bytes)	0x00004000 (16384 bytes)	0x00000A00 (2560 bytes)	0x0000D600 (54784 bytes)
virtual-address	0x00001000	0x00005000	0x00006000
virtual-size (74152 bytes)	0x00003F06 (16134 bytes)	0x0000094A (2378 bytes)	0x0000D958 (55640 bytes)
characteristics	0x60000020	0x40000040	0xC0000040
write	-	-	x
execute	v	-	-

9- Count of resource:

- There are zero resources in file C2



Chapter III

C3


1- Files' Fingerprints (MD5, SHA1):

md5 ---> 4d05488fec7d3fb63248ca9652b48cbb

sha1 ---> 5877f71c48ae3f5f36f77e78ec86e4c7a7f1fba7

MD5:	4d05488fec7d3fb63248ca9652b48cbb
SHA1:	5877f71c48ae3f5f36f77e78ec86e4c7a7f1fba7

2- The first 3 result in virustotal:

 VIRUSTOTAL

SUMMARY

DETECTION

DETAILS

RELATIONS

BEHAVIOR

[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ

Do you want to automate checks?

Acronis (Static ML)	✓ Undetected
AhnLab-V3	✓ Undetected
Alibaba	✓ Undetected
Antiy-AVL	✓ Undetected

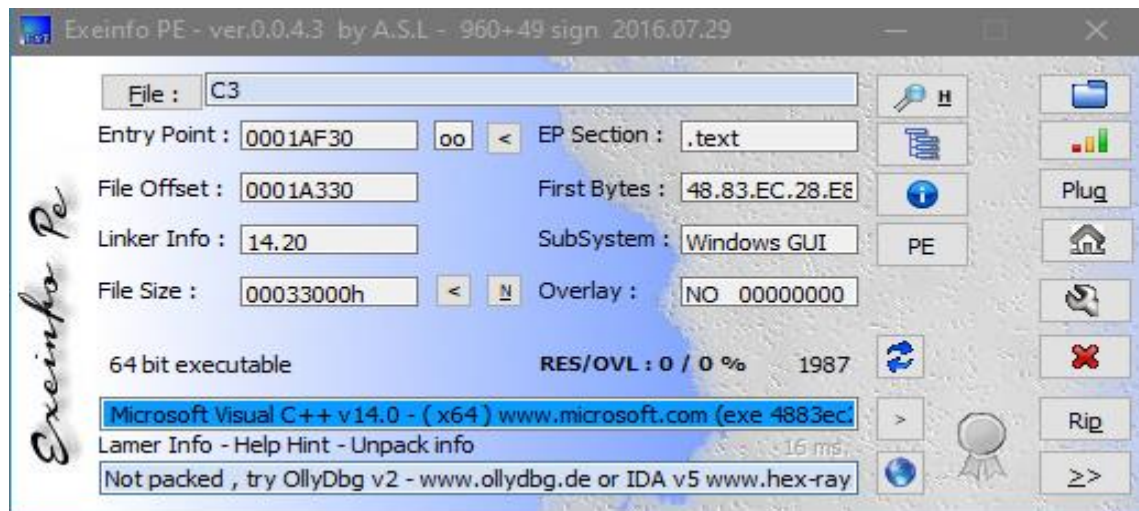
3- Text strings containing flags to mark the file as malicious or harmless:

هل هو ضار	عمله	String
غير ضار	EnterCriticalSection تستخدم لدخول قسم الحماية المتزامنة (critical section) في برنامج يعمل على نظام التشغيل Windows.	EnterCriticalSection
غير ضار	LeaveCriticalSection تستخدم للخروج من قسم الحماية المتزامنة (critical section) في برنامج يعمل على نظام التشغيل Windows.	LeaveCriticalSection
غير ضار	CreateSemaphoreEx تستخدم لإنشاء كائن سمافور (semaphore object) في برنامج يعمل على نظام التشغيل Windows.	CreateSemaphoreEx
غير ضار	InitializeCriticalSection تستخدم لتهيئة قسم الحماية المتزامنة (critical section) في برنامج يعمل على نظام التشغيل Windows.	InitializeCriticalSection
غير ضار	SetEvent تستخدم لتعيين حالة الحدث إلى "مفتوح" وإشعار العمليات المنتظرة على حدوث الحدث وهي غير ضارة.	SetEvent
غير ضار	DeleteCriticalSection تستخدم لحذف قسم الحماية المتزامنة (critical section) بعد الانتهاء من استخدامه في برنامج يعمل على نظام التشغيل Windows.	DeleteCriticalSection

c:\users\sa\desktop\c3	label (472)	group (13)	technique (16)	value
indicators (libraries > flag)	import	synchronization	-	CreateSemaphoreEx
footprints (count > 17)	import	synchronization	-	TryEnterCriticalSection
virustotal (error)	import	synchronization	-	LeaveCriticalSection
dos-header (size > 64 bytes)	import	synchronization	-	WaitForSingleObject
dos-stub (size > 192 bytes)	import	synchronization	-	ReleaseSemaphore
rich-header (tooling > Visual Studio 2015)	import	synchronization	-	InitializeCriticalSection
file-header (executable > 64-bit)	import	synchronization	-	ResetEvent
optional-header (subsystem > GUI)	import	synchronization	-	SetEvent
directories (count > 10)	import	synchronization	-	EnterCriticalSection
sections (count > 7)	import	synchronization	-	ReleaseMutex
libraries (group > registry)	import	synchronization	-	DeleteCriticalSection
imports (flag > 180)	import	synchronization	-	CreateMutex
exports (duplicate > 33)	import	synchronization	-	CreateEvent
thread-local-storage (n/a)	import	synchronization	-	WaitForMultipleObjectsEx
.NET (n/a)	import	synchronization	-	ReleaseSRWLockExclusive
resources (count > 3)	import	synchronization	-	AcquireSRWLockExclusive
strings (count > 4874)	import	synchronization	-	WakeAllConditionVariable
debug (streams > 3)	import	synchronization	-	SleepConditionVariableSR
manifest (level > aslInvoker)	import	synchronization	-	OpenEvent
version (FileDescription > WMI Performance I	import	services	T1569 System Services	CloseServiceHandle
certificate (n/a)	import	services	T1569 System Services	OpenSCManager
overlay (n/a)	import	services	T1543 Create or Modify System Proc...	OpenService
	import	services	T1569 System Services	QueryServiceConfig
	import	services	T1569 System Services	QueryServiceStatus

4- was file has been packed or compressed (Packed)?

- BY Exeinfo PE the file C3 not packed



5- Used libraries:

- There is 34 libraries in File C3

The screenshot shows a file analysis tool interface. On the left, a tree view displays various file headers and sections. On the right, a table lists the libraries used by the file.

library (34)	duplicate (0)	flag (4)	first-thunk-original (INT)	first-thunk (IAT)	type (2)
msvcrt.dll	-	-	0x0002EDC0	0x00020400	implicit
api-ms-win-core...	-	-	0x0002EAD8	0x00020118	implicit
api-ms-win-core...	-	-	0x0002ECC8	0x00020308	implicit
api-ms-win-core...	-	x	0x0002EC08	0x00020248	implicit
api-ms-win-core...	-	-	0x0002EBA8	0x000201E8	implicit
api-ms-win-secu...	-	x	0x0002EDA8	0x000203E8	implicit
api-ms-win-core...	-	-	0x0002EA70	0x000200B0	implicit
api-ms-win-core...	-	-	0x0002EAF8	0x00020138	implicit
api-ms-win-core...	-	-	0x0002ECA8	0x000202E8	implicit
api-ms-win-core...	-	-	0x0002EAE8	0x00020128	implicit

libraries	Short Description
msvcrt.dll	Microsoft C++ Runtime Library
ntdll.dll	NT Layer
api-ms-win-security-base-l1-1-0.dll	ApiSet Stub Library

Additional details:

ntdll.dll

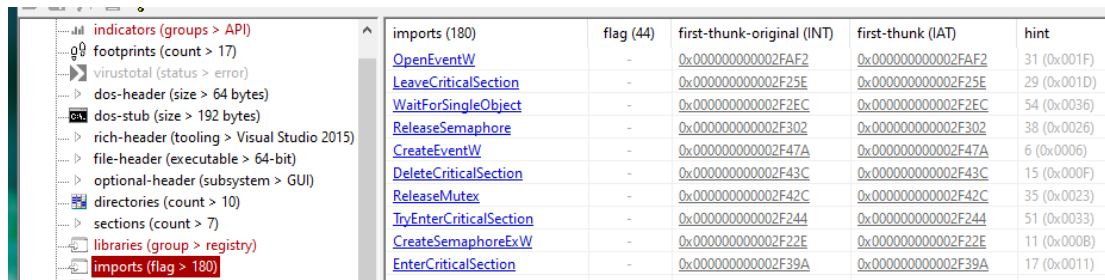
The **ntdll.dll** is a crucial component of the Windows operating system. It plays a vital role in the execution of various system processes and provides essential functions for the smooth operation of your computer. However, encountering errors related to ntdll.dll can be frustrating and disruptive to your workflow. In this article, we will explore what ntdll.dll is, common error messages associated with it, and effective methods to fix these errors. <https://malwaretips.com/>

api-ms-win-security-base-l1-1-0.dll

api-ms-win-security-base-l1-1-0.dll is a dynamic link library (DLL) file that is part of the Microsoft Windows operating system. It contains essential functions related to security and base-level operations within the Windows security subsystem. The "api-ms-win-security-base-l1-1-0.dll" file provides a set of application programming interfaces (APIs) that allow software developers to access and utilize various security features and functionalities provided by the Windows operating system. These functions may include authentication, authorization, access control, and other security-related tasks. The DLL file is crucial for the proper functioning of security-related applications and services on a Windows system.

6- Import Function:

- There are 180 imports functions in file C3



imports (180)	flag (44)	first-thunk-original (INT)	first-thunk (IAT)	hint
OpenEventW	-	0x000000000002FAF2	0x000000000002FAF2	31 (0x001F)
LeaveCriticalSection	-	0x000000000002F25E	0x000000000002F25E	29 (0x001D)
WaitForSingleObject	-	0x000000000002F2EC	0x000000000002F2EC	54 (0x0036)
ReleaseSemaphore	-	0x000000000002F302	0x000000000002F302	38 (0x0026)
CreateEventW	-	0x000000000002F47A	0x000000000002F47A	6 (0x0006)
DeleteCriticalSection	-	0x000000000002F43C	0x000000000002F43C	15 (0x000F)
ReleaseMutex	-	0x000000000002F42C	0x000000000002F42C	35 (0x0023)
TryEnterCriticalSection	-	0x000000000002F244	0x000000000002F244	51 (0x0033)
CreateSemaphoreExW	-	0x000000000002F22E	0x000000000002F22E	11 (0x000B)
EnterCriticalSection	-	0x000000000002F39A	0x000000000002F39A	17 (0x0011)
CreateMutexW	-	0x000000000002E46A	0x000000000002E46A	10 (0x000A)

Import Fun	Short Description
WaitForSingleObject	Wait for object completion
ReleaseSemaphore	Release semaphore resource.
SetEvent	Set event signal

Additional details:

WaitForSingleObject

The WaitForSingleObject function is used to wait until the specified object is in the signaled state or until the specified timeout interval elapses. It is commonly used to synchronize threads or to wait for a specific event or resource to become available.

```
C++ Copy  
  
DWORD WaitForSingleObject(  
    [in] HANDLE hHandle,  
    [in] DWORD  dwMilliseconds  
);
```

ReleaseSemaphore

The **ReleaseSemaphore** function is used to release a semaphore object, allowing other threads or processes waiting on the semaphore to proceed. It increments the semaphore's count by a specified amount.

```
C++ Copy  
  
BOOL ReleaseSemaphore(  
    [in]          HANDLE hSemaphore,  
    [in]          LONG   lReleaseCount,  
    [out, optional] LPLONG lpPreviousCount  
);
```

SetEvent

The **SetEvent** function is used to set the state of the specified event object to signaled, allowing threads or processes waiting on the event to proceed.

```
C++ Copy  
  
BOOL SetEvent(  
    [in] HANDLE hEvent  
);
```


7- Export Function:

- There are 33 export function in file C3

Export Fun	Short Description
CHPtrArray	Dynpamic pointer array
CHString	String object manipulation
CHPtrArray	Dynpamic pointer array

<div><div>indicators (groups > API)</div><div>g0 footprints (count > 17)</div><div>virustotal (status > error)</div><div>> dos-header (size > 64 bytes)</div><div>> dos-stub (size > 192 bytes)</div><div>> rich-header (tooling > Visual Studio 2015)</div><div>> file-header (executable > 64-bit)</div><div>> optional-header (subsystem > GUI)</div><div>> directories (count > 10)</div><div>> sections (count > 7)</div><div>> libraries (group > registry)</div><div>> imports (flag > 180)</div><div>> exports (duplicate > 33)</div></div>	<div>function-name (RVA)</div> <div>.rdata:0x0002BC4F</div> <div>.rdata:0x0002BC66</div> <div>.rdata:0x0002BC81</div> <div>.rdata:0x0002BC98</div> <div>.rdata:0x0002BCB1</div> <div>.rdata:0x0002BCCA</div> <div>.rdata:0x0002BCE3</div> <div>.rdata:0x0002BCFD</div> <div>.rdata:0x0002BD12</div> <div>.rdata:0x0002BD2C</div> <div>.rdata:0x0002BD48</div> <div>.rdata:0x0002BD5F</div>	<div>duplicate (33)</div> <div>x</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>x</div> <div>-</div> <div>-</div>	<div>anonymous (0)</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div>	<div>gap (0)</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div>	<div>forwarded (0)</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div> <div>-</div>
--	--	--	---	---	---

Additional details:

CHPtrArray is a class that represents a dynamic array of pointers. It provides functionality for managing and manipulating an array of pointers to objects or data.

```
C++Kopieren  
  
void * GetAt(  
    int nIndex  
);
```

CHString is a class that represents a string object. It provides methods for working with strings, including operations such as concatenation, comparison, and manipulation.

8- Section:

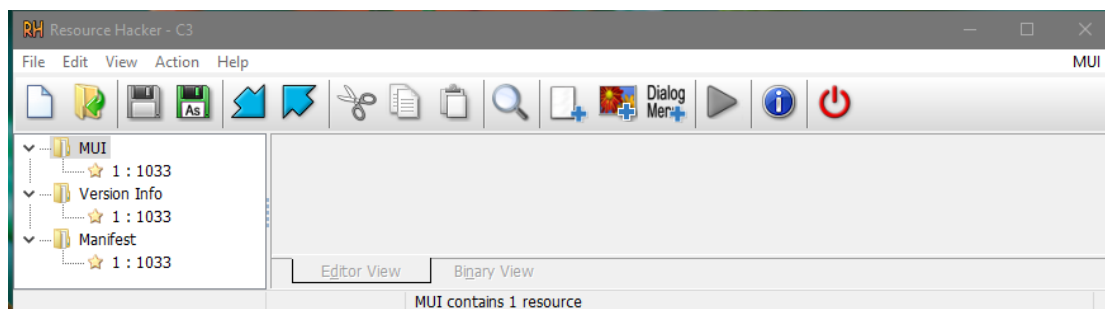
- There are 7 section in file C3

sec	Section [0]	Section [1]	Section [2]	Section [3]	Section [4]	Section [4]	Section [6]
Name	.text	.rdata	.data	.pdata	.didat	.rsrc	.reloc
Raw-size in bytes	122368 bytes	69120 bytes	4096 bytes	8192 bytes	512 bytes	2560 bytes	1024 bytes
Virtual size in bytes	121919 bytes	69090 bytes	6112 bytes	7836 bytes	296 bytes	2080 bytes	1004 bytes
Entry point .txt	0x0001AF30	---	----	---	----	---	----
Raw add begin	0x00000400	0x0001E200	0x0002F000	0x00030000	0x00032000	0x00032200	0x00032C00
Raw add end	0x0001E200	0x0002F000	0x00030000	0x00032000	0x00032200	0x00032C00	0x00033000

property	value	value	value
section	section[0]	section[1]	section[2]
name	.text	.rdata	.data
footprint > sha256	0B32D20B17EFAE389479374...	9528E6A31FB8C9A38AB04D...	397DF079F0B7C22246F86B2...
entropy	6.085	4.539	4.168
file-ratio (99.51%)	58.58 %	33.09 %	1.96 %
raw-address (begin)	0x00000400	0x0001E200	0x0002F000
raw-address (end)	0x0001E200	0x0002F000	0x00030000
raw-size (207872 bytes)	0x0001DE00 (122368 bytes)	0x00010E00 (69120 bytes)	0x00001000 (4096 bytes)
virtual-address	0x00001000	0x0001F000	0x00030000
virtual-size (208337 bytes)	0x0001DC3F (121919 bytes)	0x00010DE2 (69090 bytes)	0x000017E0 (6112 bytes)

9- Count of resource:

- There are three resources in file C3



name	instance (3)	signature	location	size (1830 bytes)	file-ratio (0.4)
MUI	1	MUI	.rsrc:0x00032958	200	0.10 %
version	1	version	.rsrc:0x000325A0	948	0.45 %
manifest	1	manifest	.rsrc:0x000322F0	682	0.33 %

Chapter IV

C4




1- Files' Fingerprints (MD5, SHA1):

md5 ----> 047c5dba99838a5d056ed4ade6fa28dd

sha1 ----> 54daa3d6701db2239965d743afffa4e29ec1dfde

MD5:	047c5dba99838a5d056ed4ade6fa28dd
SHA1:	54daa3d6701db2239965d743afffa4e29ec1dfde

2- The first 3 result in virustotal:



[Join the VT Community](#) and enjoy additional community insights and crowdsourced detections, plus an API key to [automate checks](#).

Security vendors' analysis ⓘ

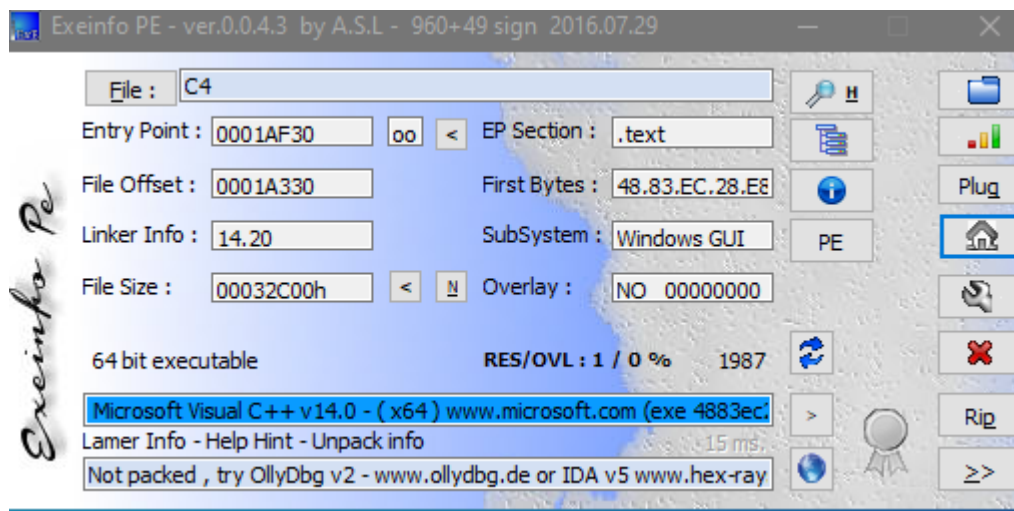
Do you want to automate checks?

SecureAge	❗ Malicious
Acronis (Static ML)	✅ Undetected
AhnLab-V3	✅ Undetected
Alibaba	✅ Undetected
ALYac	✅ Undetected
Antiy-AVL	✅ Undetected
...	...
AVIRA	✅ Undetected
AVG	✅ Undetected
AVP	✅ Undetected

3-Text strings containing flags to mark the file as malicious or harmless:

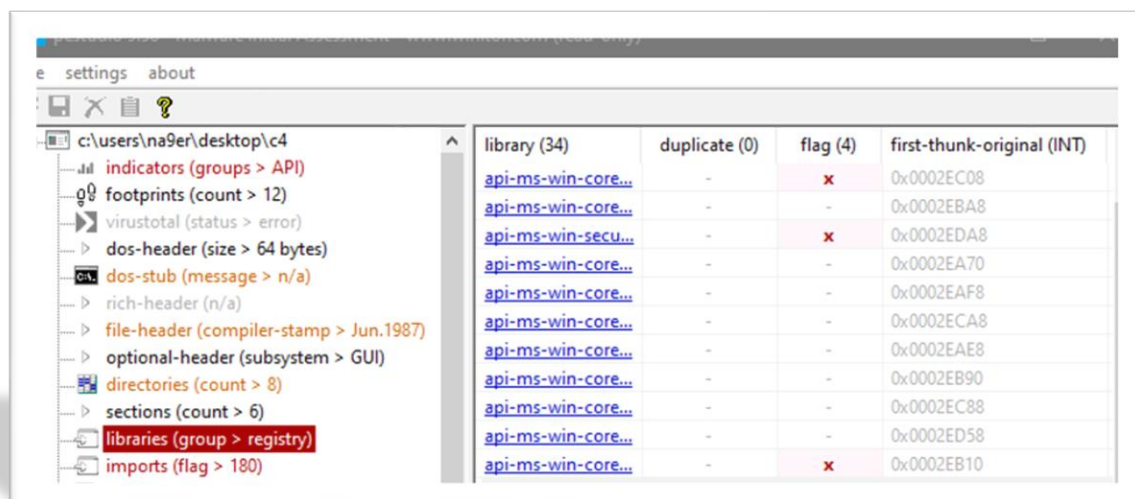
4-was file has been packed or compressed (Packed)?

- BY Exeinfo PE the file C4 not packed



5-Used libraries:

- There is 34 libraries in File C4



libraries	Short Description
oleaut32.dll	oleaut32 library
api-ms-win-core-com-l1-1-0.dll	ApiSet Stub Library
api-ms-win-core-memory-l1-1-0.dll	ApiSet Stub Library

Additional details:

oleaut32.dll

oleaut32.dll is a dynamic link library (DLL) file that is an integral part of the Microsoft Windows operating system. It stands for "Object Linking and Embedding Automation Extensions 32-bit." This DLL file contains functions and interfaces that enable software developers to create and manipulate objects, automate tasks, and facilitate inter-process communication within the Windows environment.

oleaut32.dll provides a set of Application Programming Interfaces (APIs) known as the Automation interfaces. These interfaces allow applications to interact with other applications and components, enabling features like scripting, data exchange, and automation.

api-ms-win-core-com-l1-1-0.dll

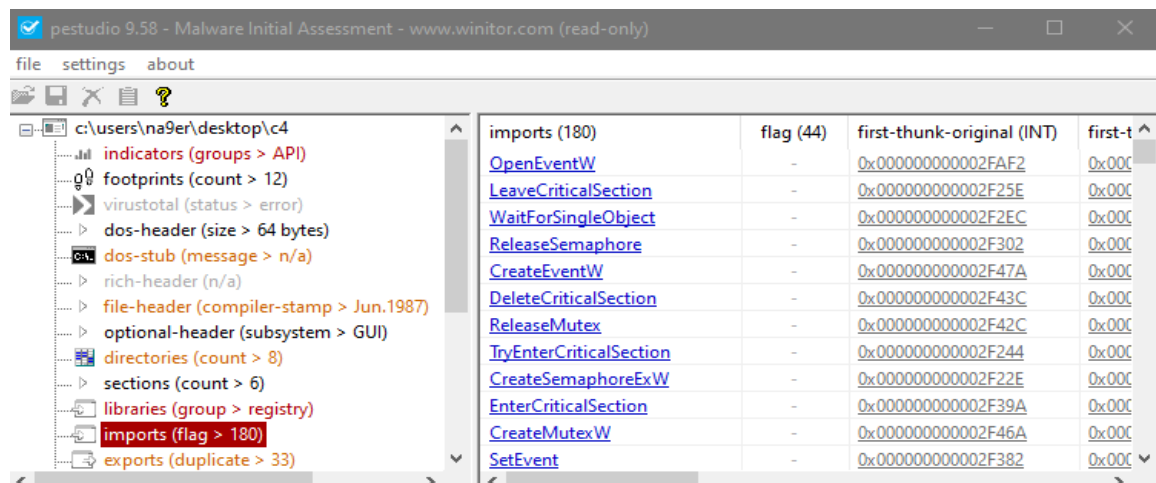
is a dynamic link library (DLL) file that is part of the Microsoft Windows operating system. It contains essential functions

related to Component Object Model (COM) and COM-based operations within the Windows core subsystem. COM is a binary-interface standard used in Windows for software components to communicate and interact with each other. It enables interprocess communication, object creation, and method invocation between software components, regardless of the programming language they are written in.

6- Import Function:

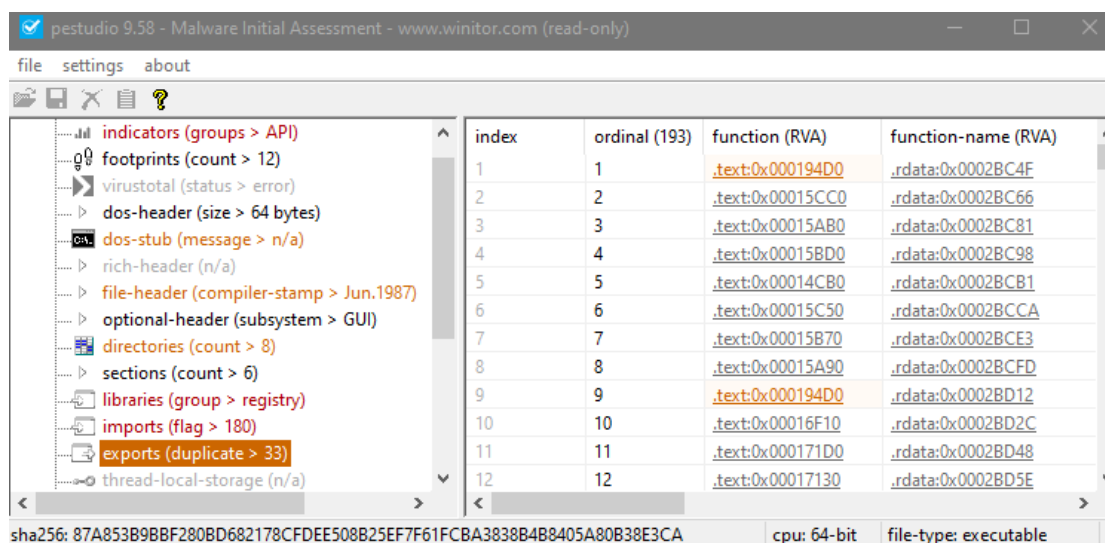
- There are 180 imports functions in file C4
WaitForSingleObject
ReleaseSemaphore
SetEvent

The file C4 the Same as file C3 in import functions



7- Export Function:

- There are 33 export function in file C4



Export Fun	Short Description
CHPtrArray::CHPtrArray(void)	Initialize CHPtrArray instance.
CRegistrySearch::CRegistrySearch	Copy CRegistrySearch instance.
CHString::~~CHString(void)	Delete CHString instance

Additional details:

CHPtrArray

This function is a constructor for the **CHPtrArray** class. It creates a new instance of the class and initializes it.

CRegistrySearch

This function is a copy constructor for the **CRegistrySearch** class. It creates a new instance of the class by making a copy of an existing instance.

CHString

This function is a destructor for the **CHString** class. It is responsible for cleaning up and releasing any resources held by an instance of the class when it is destroyed.

8- Section:

- There are 6 section in file C4

sec	Section [0]	Section [1]	Section [2]	Section [3]	Section [4]	Section [5]
Name	.text	.rdata	.data	.pdata	.didat	.rsrc
Raw-size in bytes	122368 bytes	69120 bytes	4096 bytes	8192 bytes	512 bytes	2560 bytes
Virtual size in bytes	122880 bytes	69632 bytes	8192 bytes	8192 bytes	4096 bytes	2080 bytes
Entry point .txt	0x0001AF30	---	----	---	----	---
Raw add begin	0x00000400	0x0001E200	0x0002F000	0x00030000	0x00032000	0x00032200
Raw add end	0x0001E200	0x0002F000	0x00032000	0x00032200	0x00032200	0x00032C00

pestudio 9.58 - Malware Initial Assessment - www.wintor.com (read-only)

file settings about

c:\users\nae9er\desktop\c4

- indicators (groups > API)
- footprints (count > 12)
- virustotal (status > error)
- dos-header (size > 64 bytes)
- dos-stub (message > n/a)
- rich-header (n/a)
- file-header (compiler-stamp > Jun.1987)
- optional-header (subsystem > GUI)
- directories (count > 8)
- sections (count > 6)
- libraries (group > registry)
- imports (flag > 180)
- exports (duplicate > 33)

property	value	value	value
section	section[0]	section[1]	section[2]
name	.text	.rdata	.data
footprint > sha256	0B32D20B17E7FAE389479374...	78D03A6EF9C93ECEEE15F34...	397DF079F0B7C22246F86B2...
entropy	6.085	4.533	4.168
file-ratio (99.51%)	58.87 %	33.25 %	1.97 %
raw-address (begin)	0x00000400	0x0001E200	0x0002F000
raw-address (end)	0x0001E200	0x0002F000	0x00030000
raw-size (206848 bytes)	0x0001DE00 (122368 bytes)	0x00010E00 (69120 bytes)	0x00001000 (4096 bytes)
virtual-address	0x00001000	0x0001F000	0x00030000
virtual-size (215072 bytes)	0x0001E000 (122880 bytes)	0x00011000 (6932 bytes)	0x00002000 (8192 bytes)
characteristics	0x60000020	0x40000040	0xC0000040

9- Count of resource:

- There are three resources in file C4

Resource Hacker - C4

file Edit View Action Help

MUI: 1: 1033

00032958 CD FE CD FE C8 00 00 00 00 01 00 00 00 00 00

00032968 11 00 00 00 00 00 00 02 00 00 00 3F FE 96 AE

00032978 FE 72 89 E6 52 66 70 AC 13 BD AC 84 AC 9D 5A 49

00032988 90 17 72 29 2C 26 97 1A 00 E8 82 1A 00 00 00 00

00032998 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

000329A8 00 00 00 00 88 00 00 00 0E 00 00 00 98 00 00 00

Editor View Binary View

8 / 32958 1:1 Selection - Offset: 0 Length: 0