Practical Malware Analysis & Triage
Malware Analysis Report

Werflt RCE Malware

Jun 20023 | HuskyHacks | v1.0

Table of Contents

Werflt Reverse shell Malware
Jun 2023
v1.0

Executive Summary

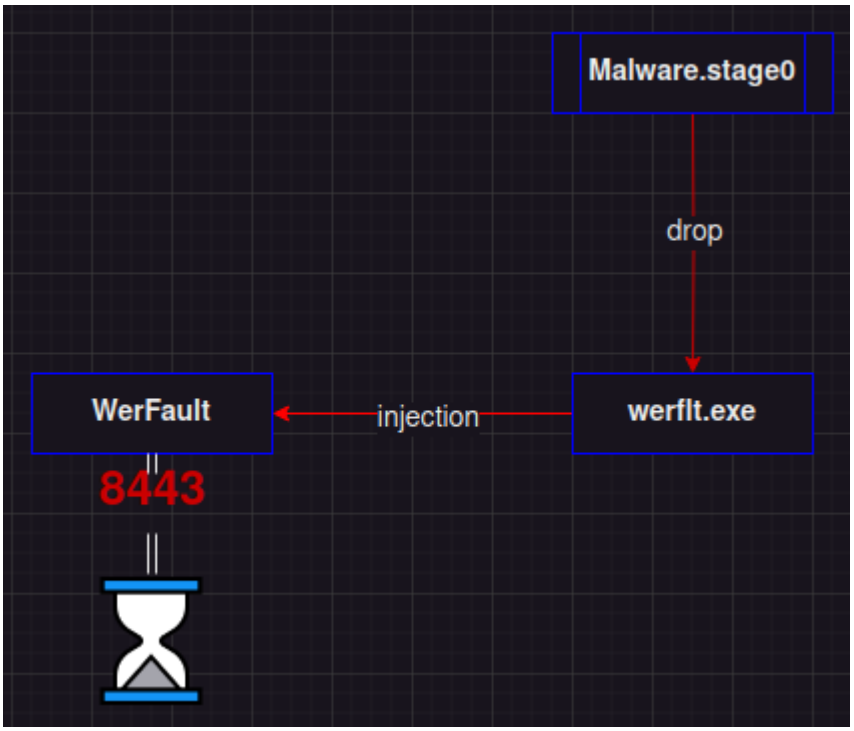
SHA256 hash	FCA62097B364B2F0338C5E4C5BAC86134CEDFFA4F8DDF27EE9901734128952E3

Werflt is a malware sample that consists of process injection, basically inject into **WerFault** (genuine windows binary) to spawn a local reverse shell.
It is a C++ compiled that runs on the x32 Windows operating system, that write a new executable on C:\Users\Public directory, named “werflt.exe”.

YARA signature rules are attached in Appendix A.

High-Level Technical Summary

Malware.stage0 consists of two parts: an stage 0 dropper and an process inection. It first write a new binary on the host then inject into a trusted service (Werfault) finally Werfault open a connection on 8443 port.



Werflt Reverse shell Malware
Jun 2023
v1.0

Malware Composition

DemoWare consists of the following components:

File Name	SHA256 Hash
Malware.stage0.exe	FCA62097B364B2F0338C5E4C5BAC86134CEDFFA4F8DDF27EE9901734128952E3
werflt.exe	0516009622B951C6C08FD8D81A856EAAB70C02E6BC58D066BBDFAFE8C6EDABEA

Malware.stage0.exe:

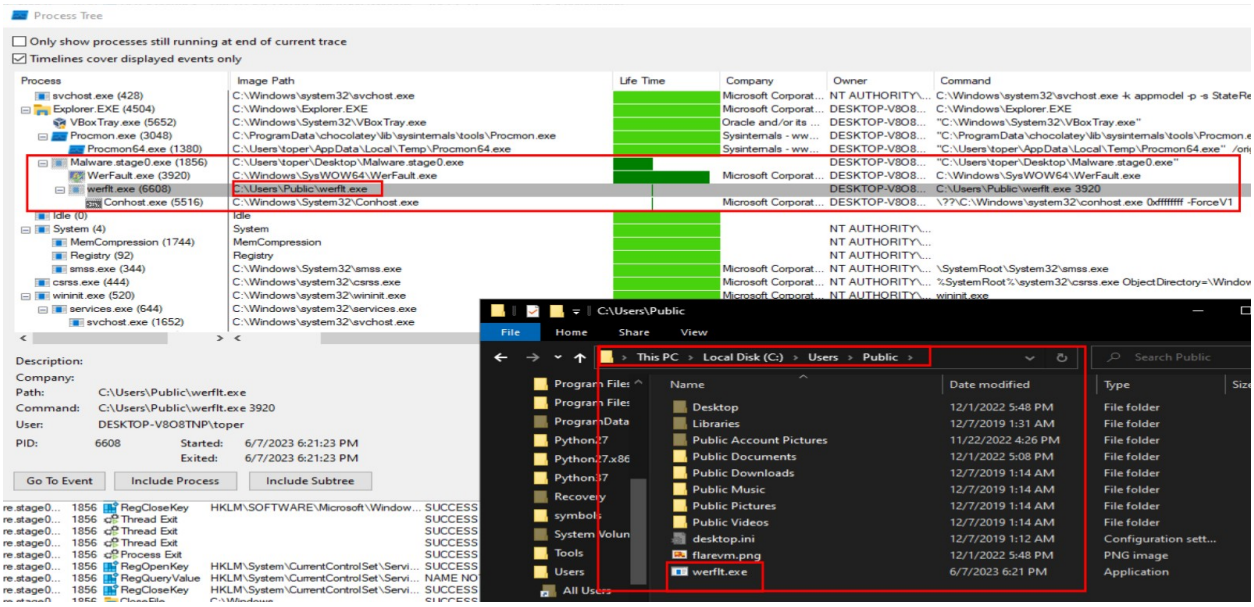
The initial executable that runs after user execution.

werflt.exe:

Binary dropped after the initial execution from Malware.stage0.exe.

Basic Dynamic Analysis

After the binary execution we can see some interesting indicators.

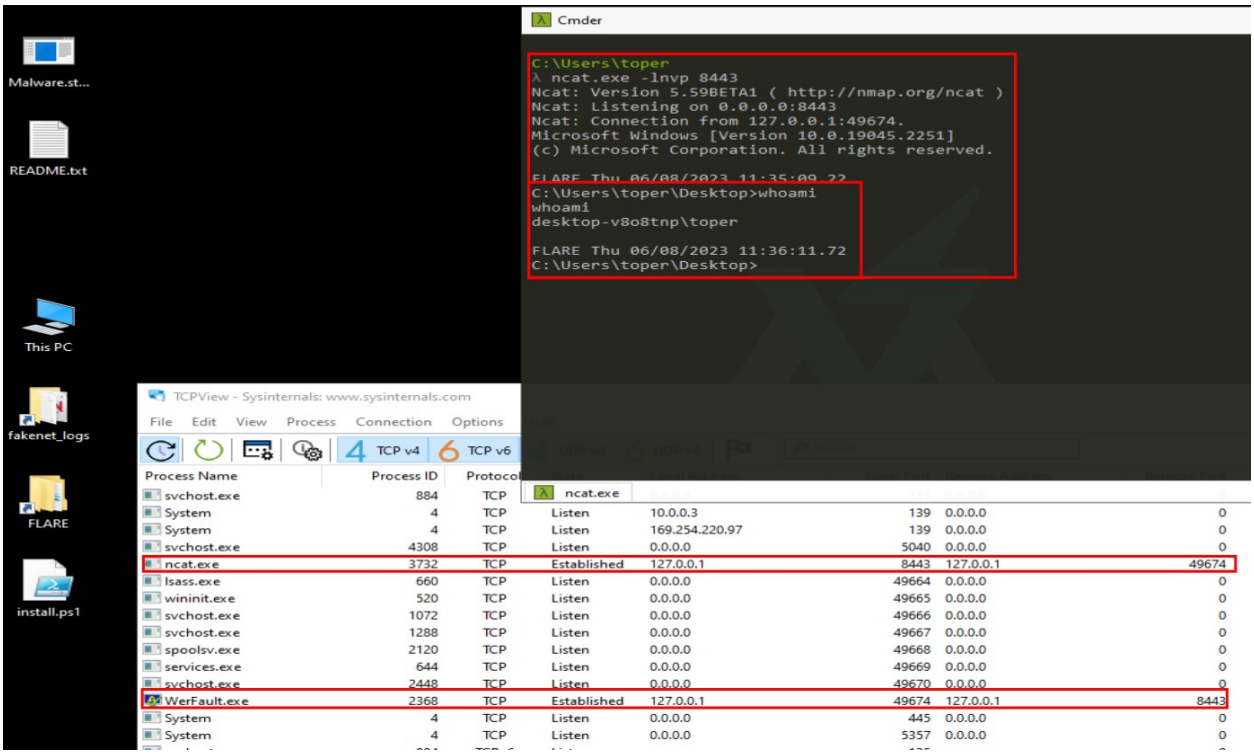


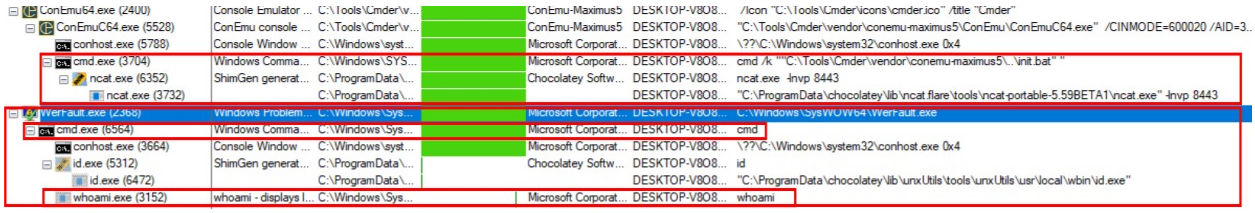
- In the picture above we can see some indicators:
  - Execution of WerFault (A genuine Windows component)
  - Werflt.exe file creation on **C:\Users\Public**

And with the TCPView we can see that there is a local request from **WerFault.exe** to a strange port 8443.

services.exe	644	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	1/10/2023 2:50:19 PM	services.exe
svchost.exe	2448	TCP	Listen	0.0.0.0	49670	0.0.0.0	0	1/10/2023 2:50:20 PM	PolicyAgent
WerFault.exe	6768	TCP	Syn Sent	127.0.0.1	49809	127.0.0.1	8443	6/7/2023 6:17:04 PM	WerFault.exe
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	1/10/2023 2:50:19 PM	System
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0	1/10/2023 2:50:20 PM	System
svchost.exe	884	TCPv6	Listen	::	135	::	0	1/10/2023 7:50:17 PM	RpcSs

After **Malware.stage0.exe** we saw that WerFault tried to connect on local port 8443, so I left a netcat waiting for connections on port 8443 and after that I received a reverse shell, bellow we can notice that behavior.





Basic Static Analysis

- Virtual Size 42.612 bytes

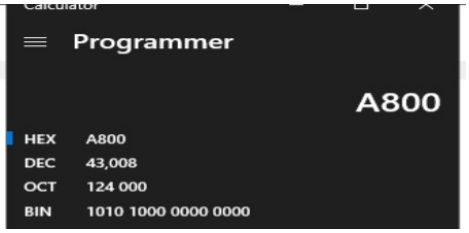
That value (42.612 bytes) is related to the data on disk when the binary is run.

pFile	Data	Description	Value
00000178	2E 74 65 78	Name	.text
0000017C	74 00 00 00		
00000180	0000A674	Virtual Size	
00000184	00001000	RVA	
00000188	0000A800	Size of Raw Data	
0000018C	00000400	Pointer to Raw Data	
00000190	00000000	Pointer to Relocations	
00000194	00000000	Pointer to Line Numbers	
00000198	0000	Number of Relocations	
0000019A	0000	Number of Line Numbers	
0000019C	60500060	Characteristics	

- Size of Raw Data 43.008 bytes

That value (43.008) is related to the the data written on disk.

pFile	Data	Description	Value
00000178	2E 74 65 78	Name	.text
0000017C	74 00 00 00		
00000180	0000A674	Virtual Size	
00000184	00001000	RVA	
00000188	0000A800	Size of Raw Data	
0000018C	00000400	Pointer to Raw Data	
00000190	00000000	Pointer to Relocations	
00000194	00000000	Pointer to Line Numbers	
00000198	0000	Number of Relocations	
0000019A	0000	Number of Line Numbers	
0000019C	60500060	Characteristics	



With that information we can assume that the binary is packed, because the large difference of values and because without internet connection is created **werflt.exe** binary.

- Below we can see when was compiled, the file type and the architecture.

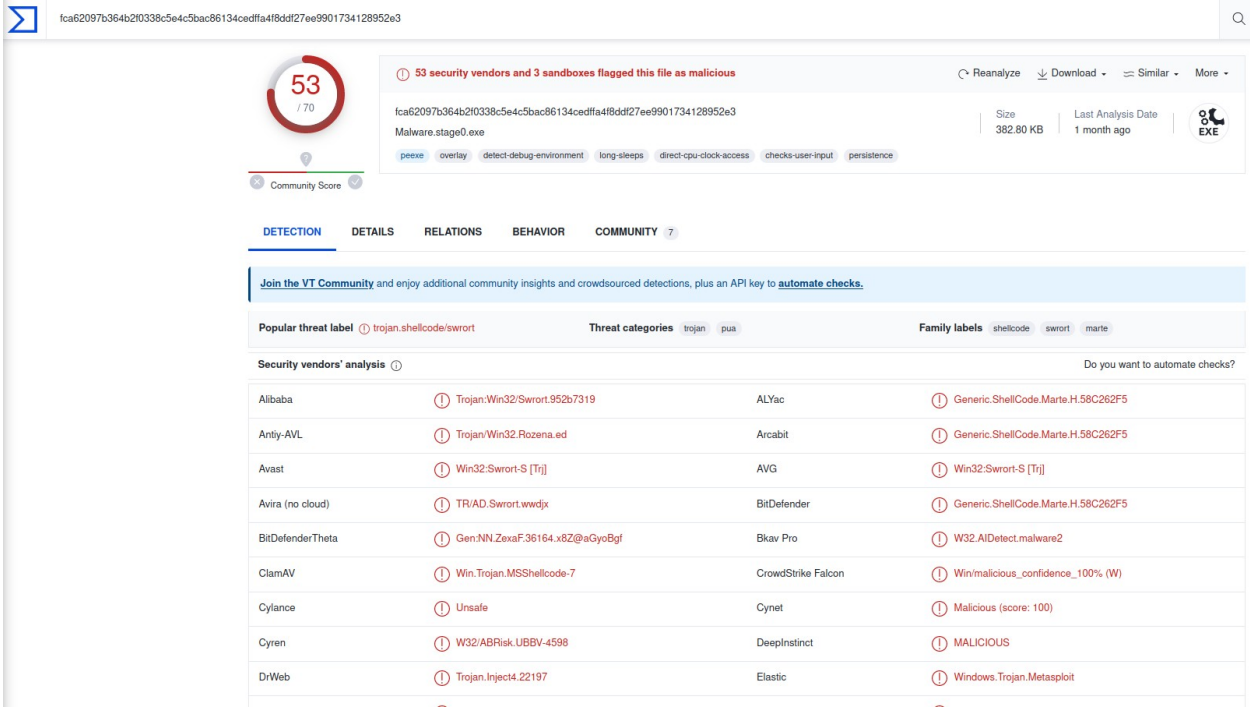
file-type	executable
cpu	32-bit
subsystem	GUI
compiler-stamp	Thu Oct 07 17:43:04 2021 | UTC

- Strings
  The most interesting strings caught from the binary.

size (bytes)	location	flag (18)	label (5151)	group (11)	value (10824)
33	0x0000BDA7	-	file	-	@C:\Windows\SysWOW64\WerFault.exe
27	0x0000BDE7	-	file	-	@C:\Users\Public\werflt.exe
85	0x0000D404	-	file	-	C:\Users\Administrator\source\repos\CRTInjectorConsole\Release\CRTInjectorConsole.pdb

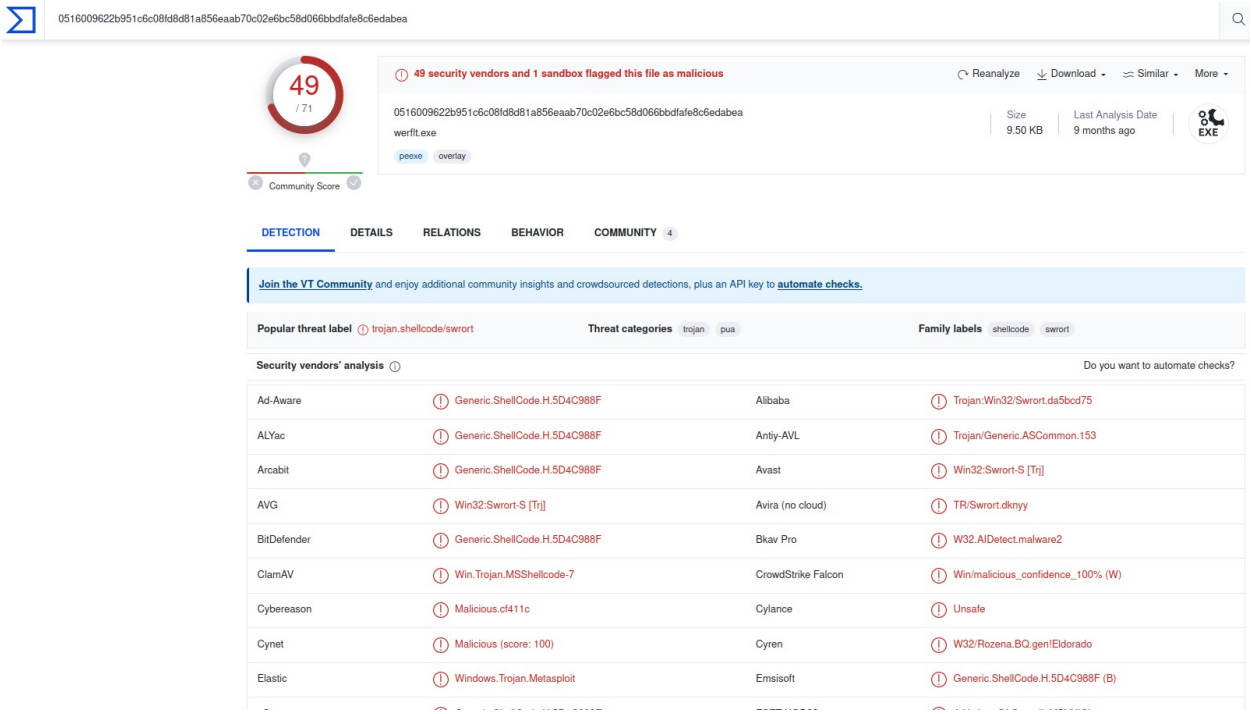
- Virus Total

Below we can see the Virus Total score from the first binary (Malware.stage0.exe):
fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3



We can see some trojan references at the image.

Second binary (werflt.exe):
0516009622B951C6C08FD8D81A856EAAB70C02E6BC58D066BBDFAFE8C6EDABEA



Advanced Static Analysis

```
[0x00401000]
   ;-- section..text:
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
1 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
2 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
3 push esi                        ; LPVOID lpBaseAddress
push edi                          ; HANDLE hProcess
call dword [WriteProcessMemory]   ; 0x402000 ; BOOL WriteProcessMemory(HANDLE hProcess, LPVOID l...
push 0
push 0
push 0
4 push esi
push 0
push 0                            ; LPSECURITY_ATTRIBUTES lpThreadAttributes
push edi                          ; HANDLE hProcess
call dword [CreateRemoteThread]   ; 0x402010 ; HANDLE CreateRemoteThread(HANDLE hProcess, LPSECU...
5 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
```

In the image above we can see some interesting API calls that is a common process injection behavior.

1. OpenProcess;
2. VirtualAllocEx;
3. WriteProcessMemory;
4. CreateRemoteThread.

Advanced Dynamic Analysis

Was not necessary.

Indicators of Compromise

Network Indicators

- Open connection on 8443 port.

Host-based Indicators

- Werflt.exe has been created;
- c:users/public directory where the binary was written;
- WerFault process injection.

Rules & Signatures

A. Yara Rules

```
rule stage0_werflt {

    meta:
        last_updated = "2023-06-08"
        author = "Gustavo Jatene"
        description = "Detection for Malware.stage0"

    strings:
        // Fill out identifying strings and other criteria
        $string1 = "@C:\Windows\SysWOW64\WerFault.exe"
        $string2 = "@C:\Users\Public\werflt.exe"
        $string3 = "C:\Users\Administrator\source\repos\
CRTInjectorConsole\Release\CRTInjectorConsole.pdb"
        $PE_magic_byte = "MZ"

    condition:
        // Fill out the conditions that must be met to identify the
binary
        $PE_magic_byte at 0 and
        ($string1 and $string2 and $string3)
}
```