

Practical Malware Analysis & Triage

Malware Analysis Report

Werflt RCE Malware

Jun 20023 | HuskyHacks | v1.0



Table of Contents

Table of Contents.....	2
Executive Summary.....	3
High-Level Technical Summary.....	4
Malware Composition.....	5
Basic Dynamic Analysis.....	6
Basic Static Analysis.....	8
Advanced Static Analysis.....	12
Advanced Dynamic Analysis.....	13
Indicators of Compromise.....	14
Network Indicators.....	14
Host-based Indicators.....	14
Rules & Signatures.....	15



Executive Summary

SHA256 hash	FCA62097B364B2F0338C5E4C5BAC86134CEDFFA4F8DDF27EE9901734128952E3
-------------	--

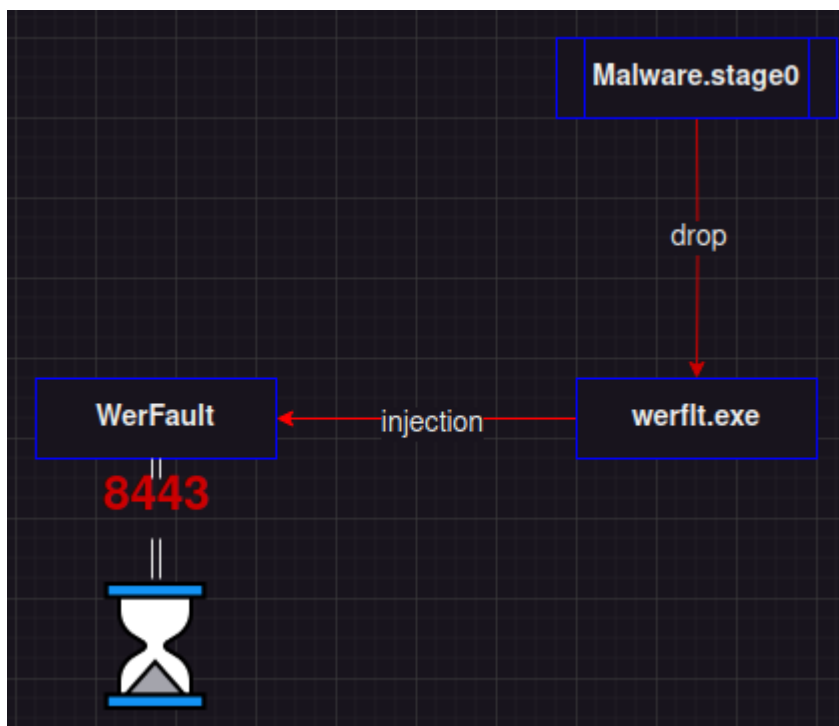
Werflt is a malware sample that consists of process injection, basically inject into **WerFault** (genuine windows binary) to spawn a local reverse shell. It is a C++ compiled that runs on the x32 Windows operating system, that write a new executable on C:\Users\Public directory, named "werflt.exe".

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 injection. It first write a new binary on the host then inject into a trusted service (Werfault) finally Werfault open a connection on 8443 port.





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.

The screenshot displays two windows from a Windows operating system. The top window is the 'Process Tree' view, showing a list of running processes. The bottom window is a File Explorer showing the contents of the 'C:\Users\Public' directory.

Process Tree Indicators:

Process	Image Path	Life Time	Company	Owner	Command
svchost.exe (428)	C:\Windows\system32\svchost.exe		Microsoft Corporat...	NT AUTHORITY\...	C:\Windows\system32\svchost.exe -k appmodel -p -s StateRe
Explorer.EXE (4504)	C:\Windows\Explorer.EXE		Microsoft Corporat...	DESKTOP-V808...	C:\Windows\Explorer.EXE
VBox Tray.exe (5652)	C:\Windows\System32\VBoxTray.exe		Oracle and/or its ...	DESKTOP-V808...	C:\Windows\System32\VBoxTray.exe
Procmon.exe (3048)	C:\ProgramData\chocolatey\lib\sysinternals\tools\Procmon.exe		Sysinternals - ww...	DESKTOP-V808...	C:\ProgramData\chocolatey\lib\sysinternals\tools\Procmon.exe
Procmon64.exe (1380)	C:\Users\toper\AppData\Local\Temp\Procmon64.exe		Sysinternals - ww...	DESKTOP-V808...	C:\Users\toper\AppData\Local\Temp\Procmon64.exe
Malware stage0.exe (1856)	C:\Users\toper\Desktop\Malware stage0.exe			DESKTOP-V808...	C:\Users\toper\Desktop\Malware stage0.exe
WerFault.exe (3920)	C:\Windows\SysWOW64\WerFault.exe		Microsoft Corporat...	DESKTOP-V808...	C:\Windows\SysWOW64\WerFault.exe
werflt.exe (6608)	C:\Users\Public\werflt.exe			DESKTOP-V808...	C:\Users\Public\werflt.exe 3920
Conhost.exe (5516)	C:\Windows\System32\Conhost.exe		Microsoft Corporat...	DESKTOP-V808...	C:\Windows\System32\Conhost.exe 0xffff -ForceV1

File Explorer Indicators:

The File Explorer window shows the 'C:\Users\Public' directory. The 'werflt.exe' file is highlighted, indicating its creation in the public directory.

- 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	RocSs



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, below we can notice that behavior.

The screenshot displays a Windows desktop with several open applications. In the top right, a Command Prompt window shows the netcat listener running on port 8443. It receives a connection from 127.0.0.1:49674, and the user 'toper' runs 'whoami', returning 'desktop-v8o8tnp\toper'. Below this, a TCPView window from Sysinternals shows a list of processes and their network connections. The 'ncat.exe' process (PID 3732) is highlighted with a red box, showing an established connection to 127.0.0.1:8443. The 'WerFault.exe' process (PID 2368) is also highlighted, showing a connection to 127.0.0.1:8443. At the bottom, a task manager window shows a list of processes, with 'ncat.exe' (PID 3732) and 'WerFault.exe' (PID 2368) highlighted with red boxes.

```
C:\Users\toper> ncat.exe -l -np 8443
Ncat: Version 5.59BETA1 ( http://nmap.org/ncat )
Ncat: Listening on 0.0.0.0:8443
Ncat: Connection from 127.0.0.1:49674.
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

FLARE Thu 06/08/2023 11:35:09.22
C:\Users\toper\Desktop> whoami
whoami
desktop-v8o8tnp\toper
FLARE Thu 06/08/2023 11:36:11.72
C:\Users\toper\Desktop>
```

Process Name	Process ID	Protocol	Local Address	Local Port	Remote Address	Remote Port	State
svchost.exe	884	TCP	Listen	10.0.0.3	139	0.0.0.0	0
System	4	TCP	Listen	169.254.220.97	139	0.0.0.0	0
svchost.exe	4	TCP	Listen	0.0.0.0	5040	0.0.0.0	0
svchost.exe	4308	TCP	Listen	0.0.0.0	8443	127.0.0.1	49674
lsass.exe	660	TCP	Listen	0.0.0.0	49664	0.0.0.0	0
wininit.exe	520	TCP	Listen	0.0.0.0	49665	0.0.0.0	0
svchost.exe	1072	TCP	Listen	0.0.0.0	49666	0.0.0.0	0
svchost.exe	1288	TCP	Listen	0.0.0.0	49667	0.0.0.0	0
spoolsv.exe	2120	TCP	Listen	0.0.0.0	49668	0.0.0.0	0
services.exe	644	TCP	Listen	0.0.0.0	49669	0.0.0.0	0
svchost.exe	2448	TCP	Listen	0.0.0.0	49670	0.0.0.0	0
WerFault.exe	2368	TCP	Established	127.0.0.1	49674	127.0.0.1	8443
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0
System	4	TCP	Listen	0.0.0.0	5357	0.0.0.0	0

Process Name	Process ID	Process Name	Process ID	Process Name	Process ID	Process Name	Process ID
ConEmu64.exe (2400)	2400	Console Emulator ...	C:\Tools\ConEmu\...	ConEmu-Maximus5	DESKTOP-V808...	/icon "C:\Tools\ConEmu\icons\conemu.ico" /title "ConEmu"	
ConEmu64.exe (5528)	5528	ConEmu console ...	C:\Tools\ConEmu\...	ConEmu-Maximus5	DESKTOP-V808...	"C:\Tools\ConEmu\vendor\conemu-maximus5\ConEmu\ConEmu64.exe" /CINMODE=600020 /AID=3...	
conhost.exe (5788)	5788	Console Window ...	C:\Windows\sys...	Microsoft Corporat...	DESKTOP-V808...	\??C:\Windows\system32\conhost.exe 0x4	
cmd.exe (3704)	3704	Windows Comm...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-V808...	cmd /k "C:\Tools\ConEmu\vendor\conemu-maximus5\unit.bat"	
ncat.exe (6352)	6352	ShimGen generat...	C:\ProgramData\...	Chocolatey Softw...	DESKTOP-V808...	ncat.exe -l -np 8443	
ncat.exe (3732)	3732	ShimGen generat...	C:\ProgramData\...	Chocolatey Softw...	DESKTOP-V808...	"C:\ProgramData\chocolatey\lib\ncat\ncat-portable-5.59BETA1\ncat.exe" -l -np 8443	
WerFault.exe (2368)	2368	Windows Problem...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-V808...	C:\Windows\System32\WerFault.exe	
cmd.exe (6564)	6564	Windows Comm...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-V808...	cmd	
conhost.exe (3664)	3664	Console Window ...	C:\Windows\sys...	Microsoft Corporat...	DESKTOP-V808...	\??C:\Windows\system32\conhost.exe 0x4	
id.exe (5312)	5312	ShimGen generat...	C:\ProgramData\...	Chocolatey Softw...	DESKTOP-V808...	id	
id.exe (6472)	6472	ShimGen generat...	C:\ProgramData\...	Chocolatey Softw...	DESKTOP-V808...	"C:\ProgramData\chocolatey\lib\unx\utils\tools\unx\usr\local\wbin\id.exe"	
whoami.exe (3152)	3152	whoami - displays...	C:\Windows\Sys...	Microsoft Corporat...	DESKTOP-V808...	whoami	

Werflt Reverse shell Malware
Jun 2023
v1.0



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	<u>executable</u>
cpu	<u>32-bit</u>
subsystem	<u>GUI</u>
compiler-stamp	<u>Thu Oct 07 17:43:04 2021 UTC</u>

- Strings
The most interesting strings caught from the binary.

size (bytes)	location	flag (18)	label (5151)	group (11)	value (10824)
33	0x00008DA7	-	file	-	@C:\Windows\SysWOW64\WerFault.exe
27	0x00008DE7	-	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

53 / 70

53 security vendors and 3 sandboxes flagged this file as malicious

fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3

Malware.stage0.exe

Size: 382.80 KB | Last Analysis Date: 1 month ago

peexe overlay detect-debug-environment long-sleeps direct-cpu-clock-access checks-user-input persistence

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 7

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

Popular threat label: trojan.shellcode/swort Threat categories: trojan, pus Family labels: shellcode, swort, marte

Security vendors' analysis

Vendor	Detection	Vendor	Detection
Alibaba	Trojan.Win32/Swort.952b7319	ALYac	Generic.ShellCode.Marte.H.58C262F5
Antiy-AVL	Trojan/Win32.Rozena.ed	Arcabit	Generic.ShellCode.Marte.H.58C262F5
Avast	Win32:Swort-S [Trj]	AVG	Win32:Swort-S [Trj]
Avira (no cloud)	TR/AD.Swort.wwdjx	BitDefender	Generic.ShellCode.Marte.H.58C262F5
BitDefenderTheta	Gen:NN.ZexaF.36164.x6Z@aGyoBgf	Bkav Pro	W32.AIDetect.malware2
ClamAV	Win.Trojan.MSShellcode-7	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cylance	Unsafe	Cynet	Malicious (score: 100)
Cyren	W32/ABRisk.UBBV-4598	DeepInstinct	MALICIOUS
DrWeb	Trojan.Inject4.22197	Elastic	Windows.Trojan.Metasploit

We can see some trojan references at the image.



Second binary (werflt.exe): **0516009622B951C6C08FD8D81A856EAAB70C02E6BC58D066BBDFAFE8C6E DABEA**

0516009622b951c6c08fd8d81a856eaab70c02e6bc58d066bbdfafe8c6edabea

49
/ 71

49 security vendors and 1 sandbox flagged this file as malicious

Reanalyze Download Similar More

0516009622b951c6c08fd8d81a856eaab70c02e6bc58d066bbdfafe8c6edabea
werflt.exe
Size: 9.50 KB
Last Analysis Date: 9 months ago
EXE

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 4

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

Popular threat label: trojan.shellcode/swort Threat categories: trojan, pua Family labels: shellcode, swort

Security vendors' analysis

Ad-Aware	Generic.ShellCode.H.5D4C988F	Alibaba	Trojan.Win32/Swort.da5bcd75
ALYac	Generic.ShellCode.H.5D4C988F	Anity-AVL	Trojan.Generic.ASCommon.153
Arcabit	Generic.ShellCode.H.5D4C988F	Avast	Win32/Swort-S [Trj]
AVG	Win32/Swort-S [Trj]	Avira (no cloud)	TR/Swort.dknyy
BitDefender	Generic.ShellCode.H.5D4C988F	Bkav Pro	W32.AIDetect.malware2
ClamAV	Win.Trojan.MSShellcode-7	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.c411c	Cylance	Unsafe
Cyren	Malicious (score: 100)	Cyren	W32/Rozena.BQ.gen!Eldorado
Elastic	Windows.Trojan.Metasploit	Emsisoft	Generic.ShellCode.H.5D4C988F (B)

Werflt Reverse shell Malware
Jun 2023
v1.0



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
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 0x1fffffff ; DWORD dwDesiredAccess
call dword [OpenProcess] ; 0x402004 ; HANDLE OpenProcess(DWORD dwDesiredAccess, BOOL bI...
push 0x40 ; 'e' ; 64
push 0x3000 ; 325
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
```

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)  
}
```