Malware Analysis Report

Stage0 Dropper

Dec 2022

Table of Contents

Executive Summary

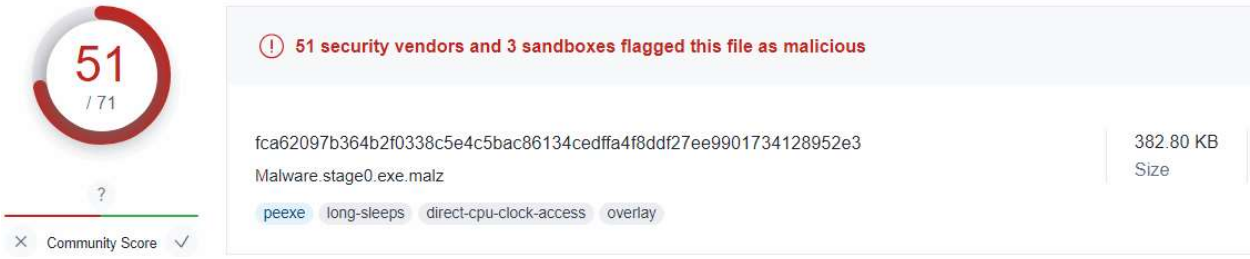
SHA256 hash	fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3

Stage0 is a file dropper malware sample first identified on December 10, 2022. VirusTotal scored this sample 51/71 malicious shell code. It is a 32-bit dropper for x86 architecture that writes to memory for injection into trusted Microsoft binary *WerFault.exe* to spawn a reverse shell on the Windows 10 operating system. This reverse shell can drop additional payloads and/or serve as a live command & control (C2) application.

YARA signature rules are attached in Appendix A.

Basic Static Analysis

VirusTotal results:



Basic Properties

MD5	6d8895c63a77ebe5e49b656bdefdb822
SHA-1	de8fb0deb6a0ac1f621950270f0ee312357401d7
SHA-256	fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3
Vhash	0350f76d155c0d5d1d051az172flz1fz
Authentihash	635004c83285bfbee8f4e08a9d78a30130a15c4c10aa5e39af5fefb472a36753
Imphash	4ac3a68b027325fa15901334d5667567
SSDEEP	6144:vgumhJWXPXqq8K4mBw/1MWYWqEkmz30WR6Pac/2ySi3WnjCTVtbo:I1hJWXPttjCqQHnLv4CfwmeTv0
TLSH	T19A844C90F692FEBAE8554BBD18F2530953AEE2C0E71DEB333520FD380556A5C42B3646
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
TrID	Win32 EXE PECompact compressed (generic) (45.7%) | Microsoft Visual C++ compiled executable (generic) (18.2%) | Win64 Executable (generic) (11.5%) | Win32 Dynamic Link Library (generic) (7.2%) | Win16 NE executable (generic) (5.5%)
DetectItEasy	PE32 | Compiler: Nim | Linker: GNU linker ld (GNU Binutils) (2.34) [GUI32]

Contacted IP Addresses (3)

IP	Detections	Autonomous System	Country
192.168.0.21	0 / 97	-	-
20.99.184.37	0 / 97	8075	US
23.216.147.76	0 / 97	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		

PEStudio results:

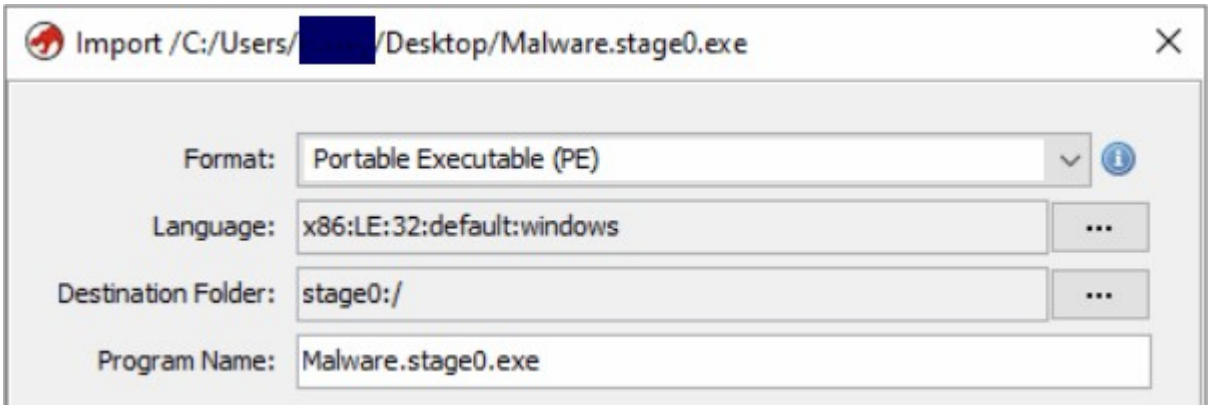
property	value
sha1	DE8FB0DEB6A0AC1F621950270F0EE312357401D7
sha256	FCA62097B364B2F0338C5E4C5BAC86134CEDFFA4F8DDF27EE9901734128952E3
md5-without-overlay	C49D3C36ADE8B1294506911E667CECB3
sha1-without-overlay	04B1FBA29B71E3EB464D51F25B1896F75472382C
sha256-without-overlay	51BDE147531F033A1C7F53A8F038DC5D305F997050182FCDB1603E25DE9448F6
first-bytes-hex	4D 5A 90 00 03 00 00 00 04 00 00 00 FF FF 00 00 B8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 00
first-bytes-text	M Z . . . . . @ . . . . .
file-size	391987 (bytes)
size-without-overlay	332800 (bytes)
entropy	6.116
imphash	n/a
signature	n/a
entry-point	83 EC 0C C7 05 F4 1B 41 00 01 00 00 00 E8 3E 8F 00 00 83 C4 0C E9 A6 FC FF FF 8D B6 00 00 00 00 83
file-version	n/a
description	n/a
file-type	**executable**
cpu	**32-bit**
subsystem	GUI
compiler-stamp	0x615F31A8 (Thu Oct 07 10:43:04 2021)

indicator (38)	detail	level
The file contains another file	signature: unknown, location: overlay, offset: 0x0005...	1
The file contains another file	signature: executable, location: .rdata, offset: 0x0000...	1
The file exposes thread-local-storage (TLS) callback(s)	count: 2	1
The count of libraries is suspicious	count: 0	1
The count of imports is suspicious	count: 0	1
The value of 'number-of-symbols' is suspicious	value: 0x0000085C	2
The file contains a virtualized section	section: .bss	2
The file references a group of API	type: console, count: 2	3
The file references a group of API	type: diagnostic, count: 7	3
The file references a group of API	type: memory, count: 14	3
The file references a group of API	type: data-exchange, count: 2	3
The file references a group of API	type: file, count: 12	3
The file references a group of API	type: execution, count: 23	3
The file references a group of API	type: synchronization, count: 10	3
The file references a group of API	type: exception, count: 7	3
The file references a group of API	type: reckoning, count: 9	3
The file references a group of API	type: dynamic-library, count: 3	3
The file references a group of hint	type: dos-message, count: 2	3
The file references a group of hint	type: file, count: 441	3
The file references a group of hint	type: utility, count: 7	3
The file references a group of hint	type: rtti, count: 1	3
The file references a group of hint	type: format-string, count: 3	3
The file references a group of hint	type: registry, count: 810	3

encoding (2)	size (bytes)	file-offset	blacklist (17)	hint (1264)	group (10)	value (10506)
ascii	18	0x0000D8A2	x	-	memory	WriteProcessMemory
ascii	14	0x0000F050	x	-	memory	VirtualProtect
ascii	14	0x00036618	x	-	memory	VirtualProtect
ascii	13	0x0000B8CC	x	-	execution	CreateProcess
ascii	13	0x0000B8DB	x	-	execution	SuspendThread
ascii	18	0x0000B903	x	-	execution	GetExitCodeProcess
ascii	11	0x0000D8B8	x	-	execution	OpenProcess
ascii	18	0x0000D8E6	x	-	execution	CreateRemoteThread
ascii	16	0x0000DC52	x	-	execution	TerminateProcess
ascii	19	0x0000DC9C	x	-	execution	GetCurrentProcessId
ascii	18	0x0000DCB2	x	-	execution	GetCurrentThreadId
ascii	19	0x0000EEE6	x	-	execution	GetCurrentProcessId
ascii	18	0x0000EEFC	x	-	execution	GetCurrentThreadId
ascii	16	0x0000EFF4	x	-	execution	TerminateProcess
ascii	16	0x0002D948	x	-	execution	TerminateProcess
ascii	19	0x0002D9BA	x	-	execution	GetCurrentProcessId
ascii	18	0x0002D9E7	x	-	execution	GetCurrentThreadId

encoding (2)	size (bytes)	file-offset	blacklist (17)	hint (1264)	group (10)	value (10506)
ascii	17	0x0000EED2	-	-	execution	GetCurrentProcess
ascii	5	0x0000EFEC	-	-	execution	Sleep
ascii	11	0x0000F008	-	-	execution	TlsGetValue
ascii	5	0x00016DBF	-	-	execution	Sleep
ascii	17	0x0002D91F	-	-	execution	GetCurrentProcess
ascii	11	0x0003E964	-	-	execution	TlsGetValue
ascii	24	0x0000DC04	-	-	exception	UnhandledExceptionFilter
ascii	27	0x0000DC20	-	-	exception	SetUnhandledExceptionFilter
ascii	27	0x0000EFCE	-	-	exception	SetUnhandledExceptionFilter
ascii	24	0x0000F016	-	-	exception	UnhandledExceptionFilter
ascii	27	0x00016DF3	-	-	exception	SetUnhandledExceptionFilter
ascii	27	0x0002D8B3	-	-	exception	SetUnhandledExceptionFilter
ascii	24	0x0002D8EE	-	-	exception	UnhandledExceptionFilter
ascii	15	0x0000DD0C	-	-	dynamic-l...	GetModuleHandle
ascii	14	0x0000EF22	-	-	dynamic-l...	GetProcAddress
ascii	11	0x0000EFA4	-	-	dynamic-l...	LoadLibrary
ascii	12	0x0000AE6B	-	-	diagnostic	GetLastError
ascii	13	0x0000AE78	-	-	diagnostic	FormatMessage
ascii	13	0x0000B839	-	-	diagnostic	FormatMessage
ascii	12	0x0000B852	-	-	diagnostic	GetLastError
ascii	12	0x0000EF12	-	-	diagnostic	GetLastError
ascii	12	0x0003667F	-	-	diagnostic	GetLastError
ascii	12	0x0003E983	-	-	diagnostic	GetLastError
ascii	10	0x0000B82E	-	-	data-exch...	CreatePipe
ascii	15	0x0000B874	-	-	data-exch...	CreateNamedPipe

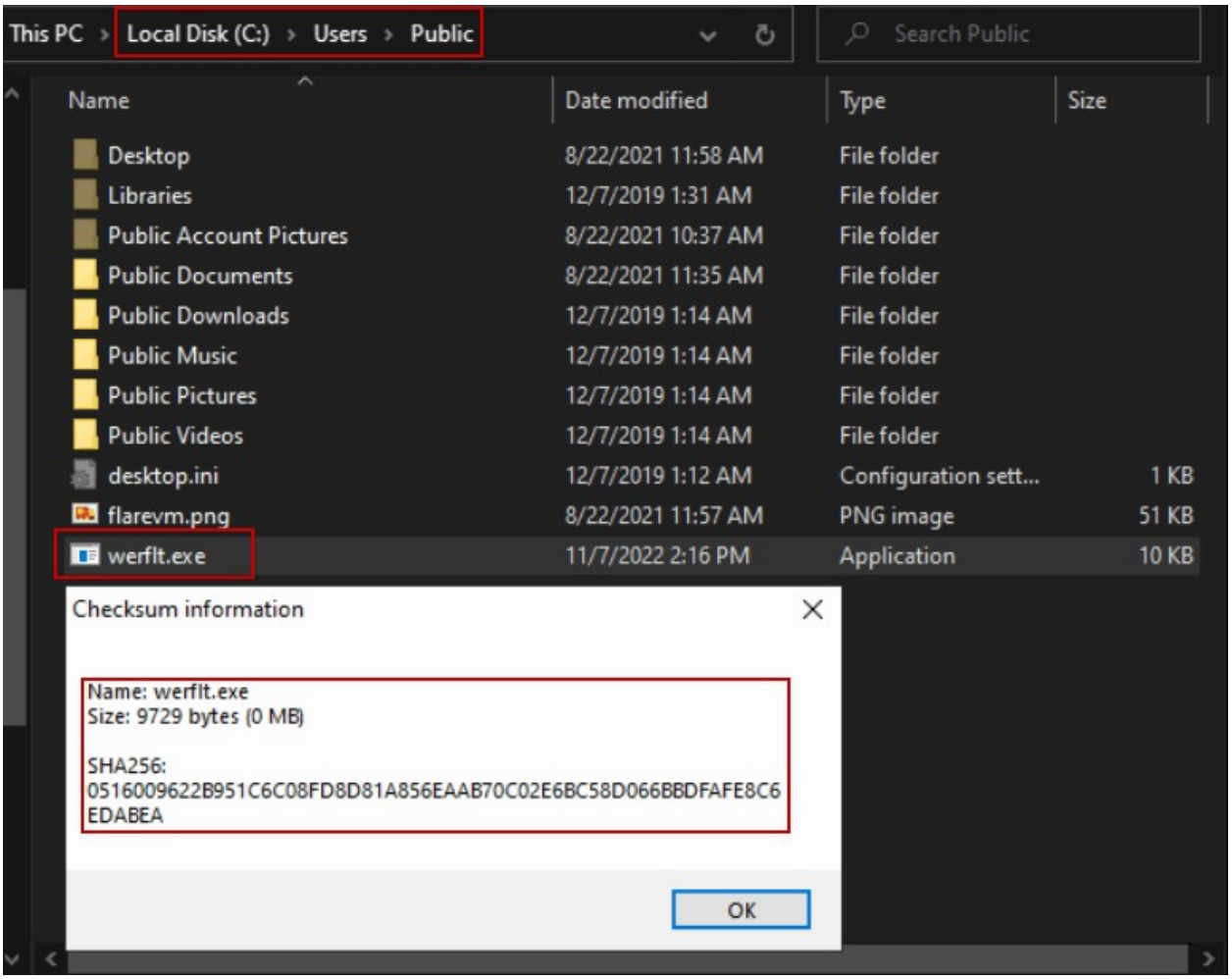
Ghidra results:



Ghidra failed to import the referenced libraries

Basic Dynamic Analysis

Networked detonation on FLARE vm yields a file creation to C:\Users\Public



TCPview results:

The *werflt.exe* binary runs as the known Microsoft error reporting program *WerFault.exe* and listens on the loopback address via port 8443.

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	
svchost.exe	900	TCP	Listen	0.0.0.0	135	0.0.0.0	0	11/5/2022
System	4	TCP	Listen	169.254.243.48	139	0.0.0.0	0	11/5/2022
System	4	TCP	Listen	192.168.149.132	139	0.0.0.0	0	11/7/2022
ncat.exe	264	TCP	Listen	0.0.0.0	1097	0.0.0.0	0	11/7/202
WerFault.exe	2484	TCP	Syn Sent	127.0.0.1	1098	127.0.0.1	8443	11/7/202
svchost.exe	4336	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	11/5/2022
services.exe	660	TCP	Listen	0.0.0.0	23473	0.0.0.0	0	11/5/2022

Advanced Static Analysis

Cutter results:

The Main function of *werflt.exe* indicates a “Create Remote Thread” process injection technique. The binary retrieves and assigns an existing Process ID to a variable:

```
[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
```

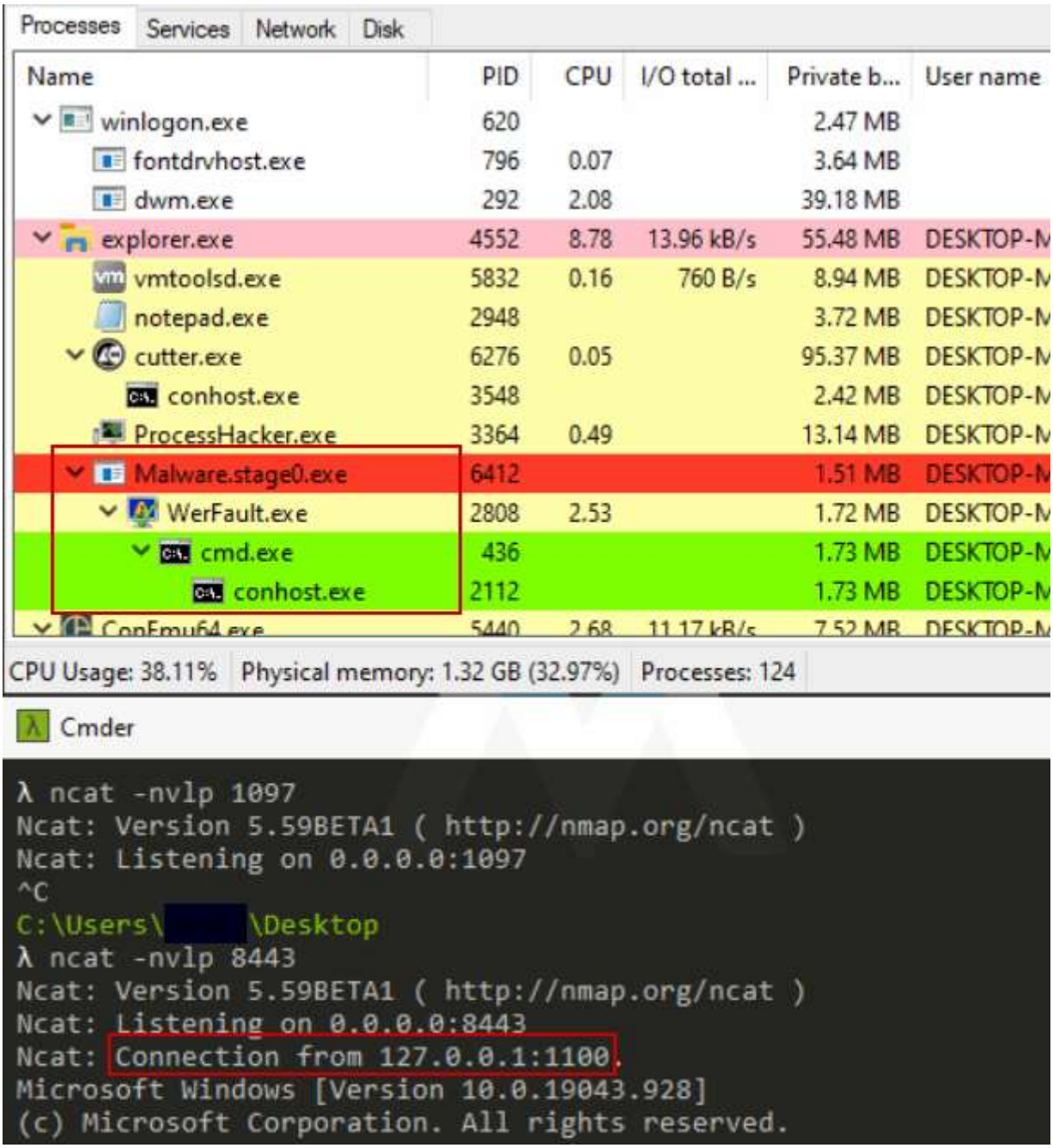
It opens this process with Write permissions and then allocates memory space with Read/Write/Execute permissions. It writes the contents of a variable to the allocated memory section and starts a thread within the process. It executes code from the allocated memory.

```
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]
```

Advanced Dynamic Analysis

Process Hacker 2 results:

We set up a netcat listener for port 8443 on FLARE while running iNetSim on REMnux and confirmed a reverse TCP shell spawned from legitimate process *WerFault.exe*.



Indicators of Compromise

Network Indicators

WerFault.exe listening on remote port 8443

Host-based Indicators

SHA256: fca62097b364b2f0338c5e4c5bac86134cedffa4f8ddf27ee9901734128952e3

WerFault.exe spawns child process cmd.exe, which in turn spawns conhost.exe

Appendix A: Rules & Signatures

YARA Signature Match - THOR APT Scanner

RULE: SUSP_Shellcode_Dec20_1
RULE_SET: Livehunt - Suspicious20 Indicators
RULE_TYPE: THOR APT Scanner's rule set only
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/SUSP_Shellcode_Dec20_1
DESCRIPTION: Detects shellcode sequences
RULE_AUTHOR: Florian Roth

RULE: SUSP_FilePath_Public_Oct21_1
RULE_SET: Livehunt - Suspicious5 Indicators
RULE_TYPE: Valhalla Rule Feed Only
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/SUSP_FilePath_Public_Oct21_1
DESCRIPTION: Detects a suspicious file path often found in malicious samples
RULE_AUTHOR: Florian Roth

RULE: HKTL_Shellter_Mar20
RULE_SET: Livehunt - Hacktools Indicators
RULE_TYPE: Valhalla Rule Feed Only
RULE_LINK: https://valhalla.nextron-systems.com/info/rule/HKTL_Shellter_Mar20
DESCRIPTION: Detects an executable that was modified by Shellter
REFERENCE: https://shellterproject.com/
RULE_AUTHOR: Max Altgelt