

# MALWARE ANALYSIS REPORT

## 1. Basic Information

Field	Value
Malware Name/Hash	91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac
Type	Trojan
File Name	WEXTRACT.EXE
File Size	420.00 KB
Date of Analysis	(29-07-2025)
Analyst Name	Suryansh Pandey
Intern Id	110
Platform Targeted	Windows
Sample Source	http://june12.5gbfree.com/fszz/gud.exe

Hashes

MD5: 1517814c4d44cc632abb52d2d6307f15

SHA1: 9ee0404b76fe5bda2692f049bb9fc78e17240708

SHA256: 91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac

SSDEEP: 6144:QjbeiyDBJNEeHfZEW6GH5W288L5ABAYRb+m112Mppeaibjz90645wZUS+:Qu1PzgGH5W28oANn112tLOE+

SSDEEP: e744:0jpe7yADp7MEeHfZEMeCH2M588f2VEVXLP+WT73HfBe97p]5a0e42a202+:0n7Lx0GH2M58oVWU773cFOE+

## 2. Static Analysis

Feature	Details
File Type	Win32 EXE
File Hashes	MD5: 1517814c4d44cc632abb52d2d6307f15 SHA-1: 9ee0404b76fe5bda2692f049bb9fc78e17240708
Strings Found	(offset 00039230: 1A 3B 2A BE 14 42 C5 E7 etc)
PEiD Packer	Microsoft Visual C++ SPx

Feature	Details
Located IPs	3.131.193.27
Sections Info	(.text, .exe, .vir)
Digital Signature	Unsigned
API reference	ExitWindowsEx@USER32.dll
YARA Rules	<a href="http://www.hexacorn.com/blog/2012/10/14/random-stats-from-1-2m-samples-pe-section-names/">http://www.hexacorn.com/blog/2012/10/14/random-stats-from-1-2m-samples-pe-section-names/</a>

Basic properties

MD5

1517814c4d44cc632abb52d2d6307f15

SHA-1

9ee0404b76fe5bda2692f049bb9fc78e17240708

SHA-256

91bfa2445d998425c81f30d293235429ca6a8c6c8f326536478952a2a6754aac

Vhash

0450366d1570e013z10054mz1f03dz

Authentihash

e8e59d053329175e4526a50f15c4abf35acb169a910b1311f55ee89489a00761

Imphash

0ebb3c09b06b1666d307952e824c8697

Rich PE header hash

87c02cf7ae3b70f2eeb1122540dff093

SSDEEP

6144:QJbeiyDBJNEeHfZEW6GH5W288L5ABAYRb+m112Mppealbjz90645wZUS+Qu1PzgGH5W28oANn112tLOE+

TLSH

T14A94F10652D5893BE0A137B048EE276316397CF46EB1E36B724475C9AC317C1AA7932F

File type

Win32 EXE executable windows win32 pe peexe

Magic

PE32 executable (GUI) Intel 80386, for MS Windows

TrID

Win32 MS Cabinet Self-Extractor (WExtract stub) (82.1%) | Win32 Executable MS Visual C++ (generic) (8.4%) | Win64 Executable (generic) (2.8%) | Win32 Dynamic Link Li...

DetectItEasy

PE32 | sfx: Microsoft Cabinet (6.00.2900.2180 (xpsp\_sp2\_rtm.040803-2158)) | Compiler: EP:Microsoft Visual C/C++ (2005) [EXE32] | Archive: Microsoft Cabinet File (1.03) [...]

Magika

PEBIN

File size

420.00 KB (430080 bytes)

PEID packer

Microsoft CAB SFX

F-PROT packer

SFX

1-4801 bytes

26X

1-4801 bytes

Microsoft CAB 26X

1-4801 bytes

430080 KB (430080 bytes)

1-4801 bytes

PEBIN

## ADVAPI32.dll

### Meta Data

```

{ 2 items
  "libref": { 2 items
    "name": "advapi32.dll"
    "suspicious": false
  }
  "reason": [ 1 item
    0: "LIBRARY_REFERENCE"
  ]
}
```

```
}
```

```
}
```

```
0: "LIBRARY_REFERENCE"
```

Extended details

Meta	Header	RichHeader	Characteristics	Verinfo	Sections	Resources	Imports	PdbData
Name		Value						
CompanyName		Microsoft Corporation						
FileDescription		Win32 Cabinet Self-Extractor						
FileVersion		6.00.2900.2180 (xpsp_sp2_rtm.040803-2158)						
InternalName		Wextract						
LegalCopyright		© Microsoft Corporation. All rights reserved.						
OriginalFilename		WEXTRACT.EXE						
ProductName		Microsoft® Windows® Operating System						
ProductVersion		6.00.2900.2180						

ProductVersion	6.00.2900.2180
ProductName	Microsoft® Windows® Operating System

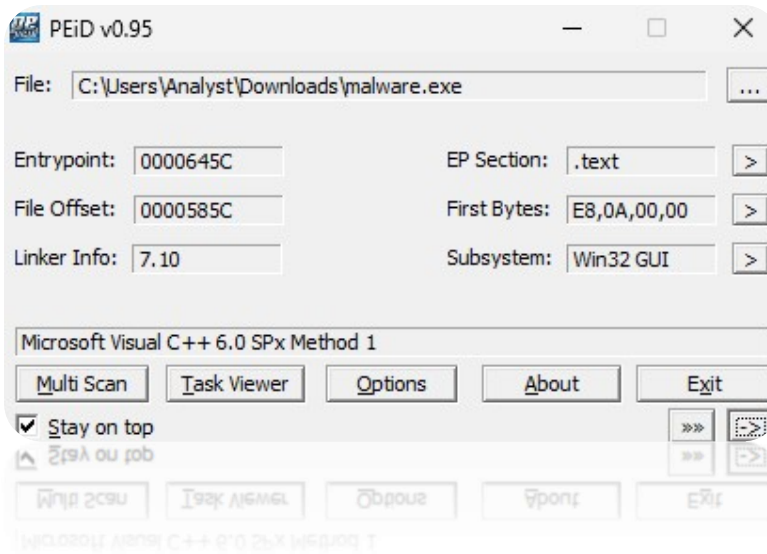
Extended details

Meta	Header	RichHeader	Characteristics	Verinfo	Sections	Resources	Imports	PdbData
ImageBase:		0x1000000						
EntrypointName:		.text						
EntrypointEntropy:		6.6						
EntrypointVA:		0x100645c						
CrcInFile:		0x69ccf						
CrcActual:		0x6b10a						
LinkerVersionMajor:		7						
LinkerVersionMinor:		10						
CompilerFlags:		IsASLR: false						
		IsNXCOMPAT: false						
		IsSEH: true						
		IsCFG: false						
		IsGS: false						
PointerToSymbolTable:		0x0						
NumberOfSymbols:		0x0						

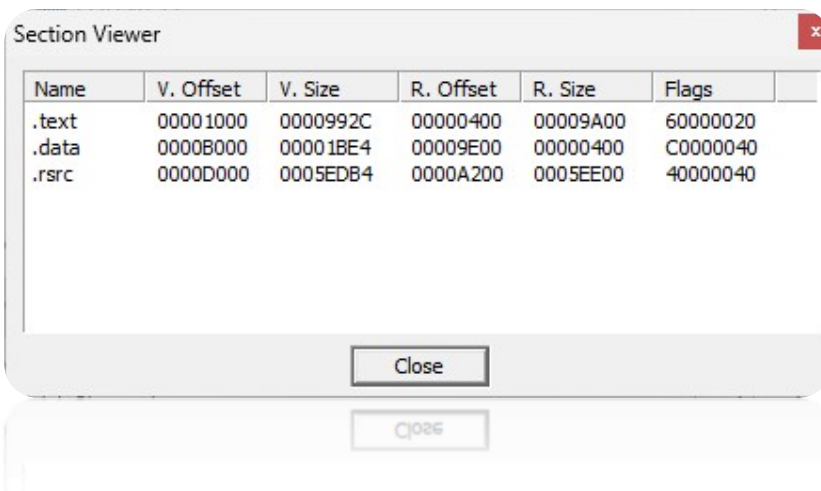
NumberOfSymbols:	0x0
PointerToSymbolTable:	0x0
IsASLR:	false
IsCFG:	false

## # PEid Tool (Screenshots)

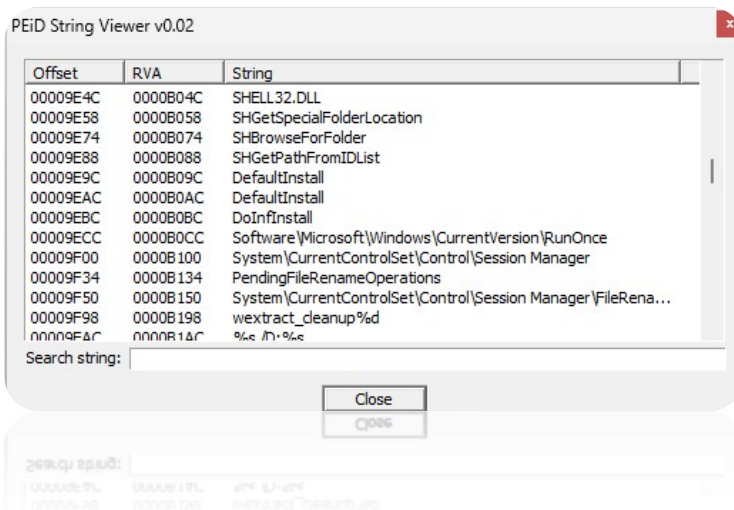
### 1. Basic Information



### 2. EP Section



### 3. Strings



#### 4. PE Details

The screenshot shows the 'PE Details' dialog box with two tabs: 'Basic Information' and 'Directory Information'.

**Basic Information**

EntryPoint:	0000645C	SubSystem:	0002
ImageBase:	01000000	NumberOfSections:	0003
SizeOfImage:	0006C000	TimeDateStamp:	41107BC1
BaseOfCode:	00001000	SizeOfHeaders:	00000400
BaseOfData:	0000B000	Characteristics:	010F
SectionAlignment:	00001000	Checksum:	00069CCF
FileAlignment:	00000200	SizeOfOptionalHeader:	00E0
Magic:	010B	NumOfRvaAndSizes:	00000010

**Directory Information**

	RVA	SIZE		
ExportTable:	00000000	00000000		
ImportTable:	00009CE4	0000008C	...	>
Resource:	0000D000	0005EDB4	...	>
TLSTable:	00000000	00000000		
Debug:	00001230	0000001C	...	>

Buttons: Close

#### 5. Extra Information

The screenshot shows the 'Extra Information' dialog box.

FileName: C:\Users\Analyst\Downloads\malware.exe

Detected: Microsoft Visual C++ 6.0 SPx Method 1

Scan Mode: Deep

Entropy: 6.56 (Maybe Packed) -

EP Check: Not Packed -

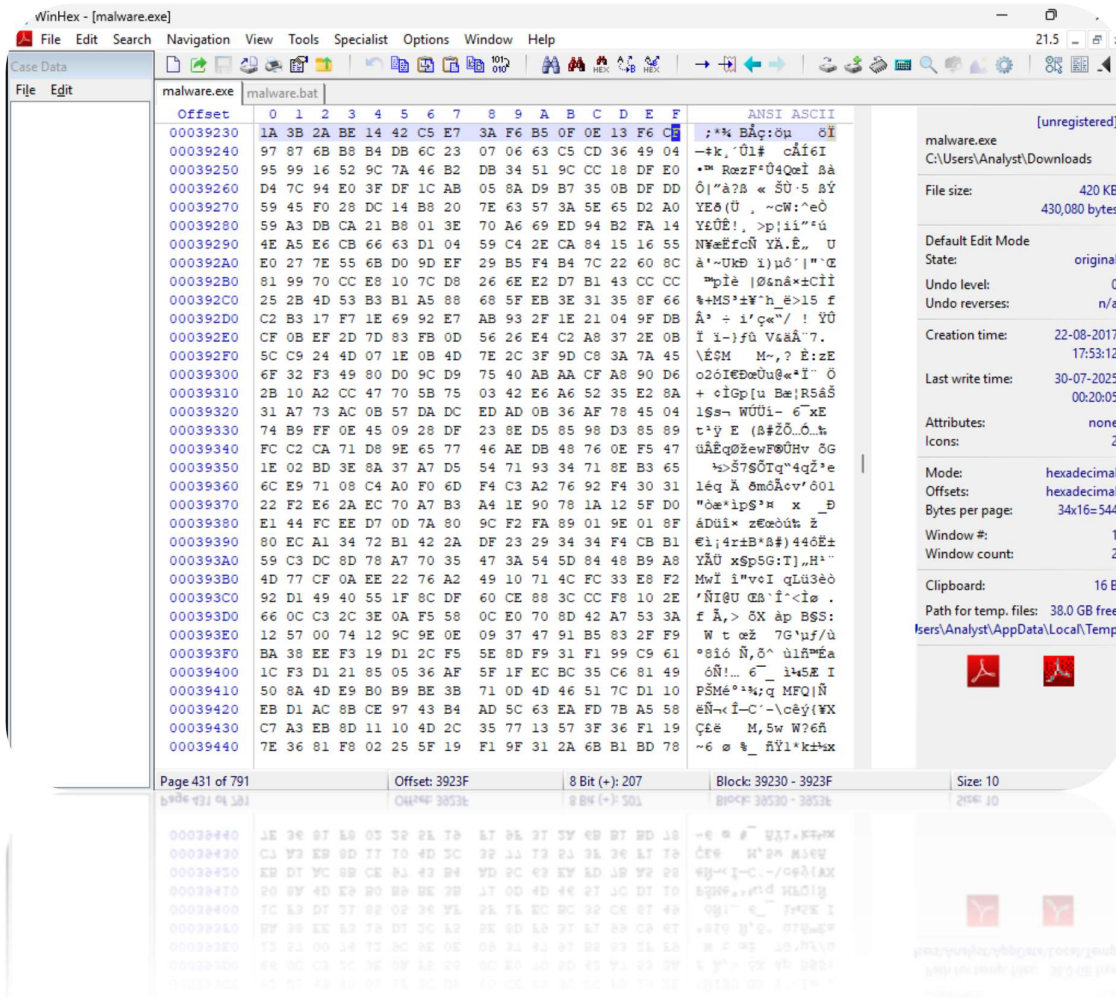
Fast Check: Packed -

Buttons: OK

## # IP Traffic



## # WinHex Tool (Screenshot)



## # Capabilities:

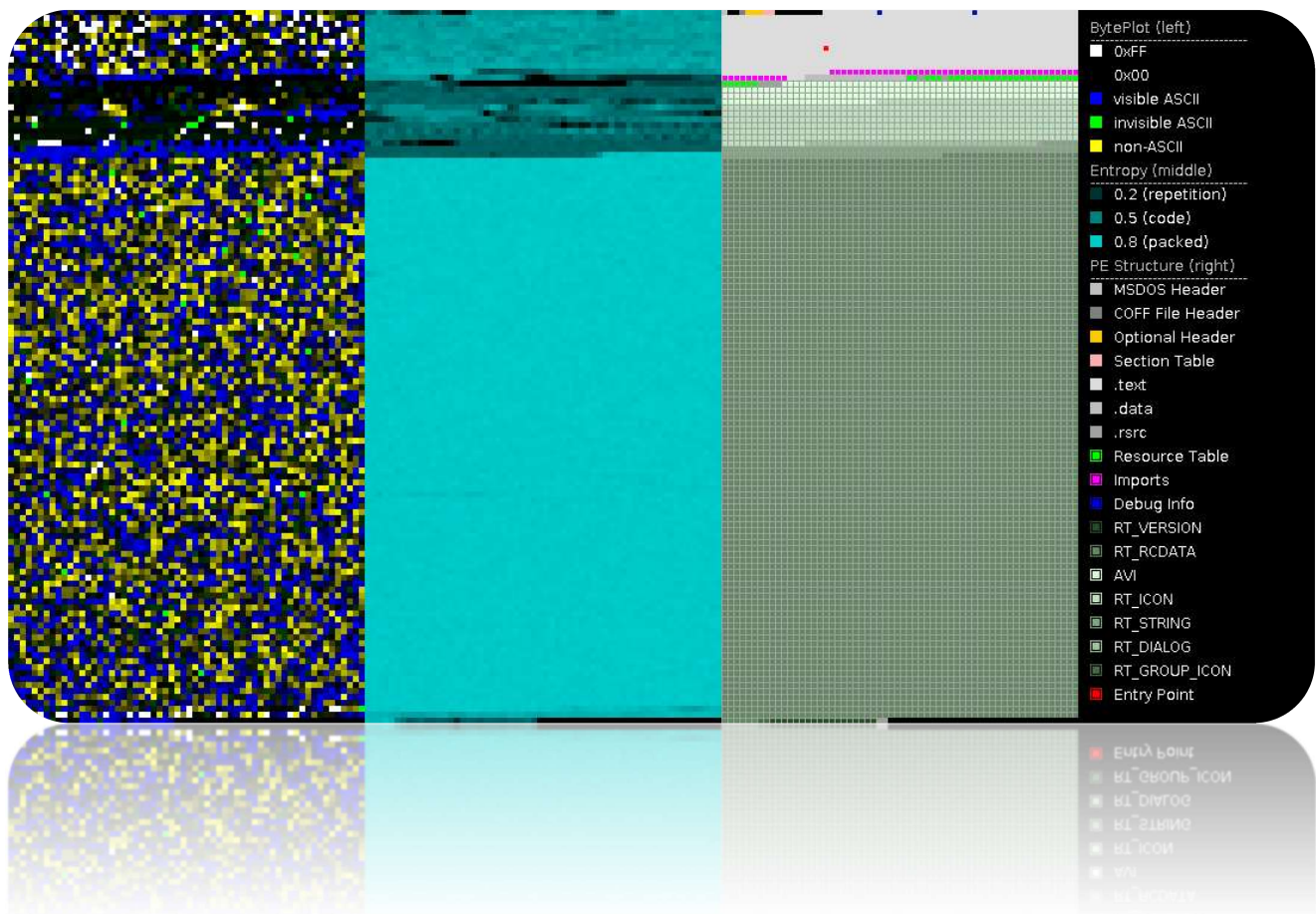
<b>Executable</b>	packaged as an IExpress self-extracting archive extract resource via kernel32 functions
<b>Data-Manipulation</b>	encode data using XOR
<b>Linking</b>	link function at runtime on Windows
<b>Persistence</b>	persist via Run registry key
<b>Host-Interaction</b>	get file version info create process on Windows set registry value shutdown system delete registry value set file attributes get system information on Windows compare security identifiers query or enumerate registry key enumerate files recursively set current directory terminate process get disk size get disk information delete file etc.



## # Graph



## # Visualization Input File (PortEx)

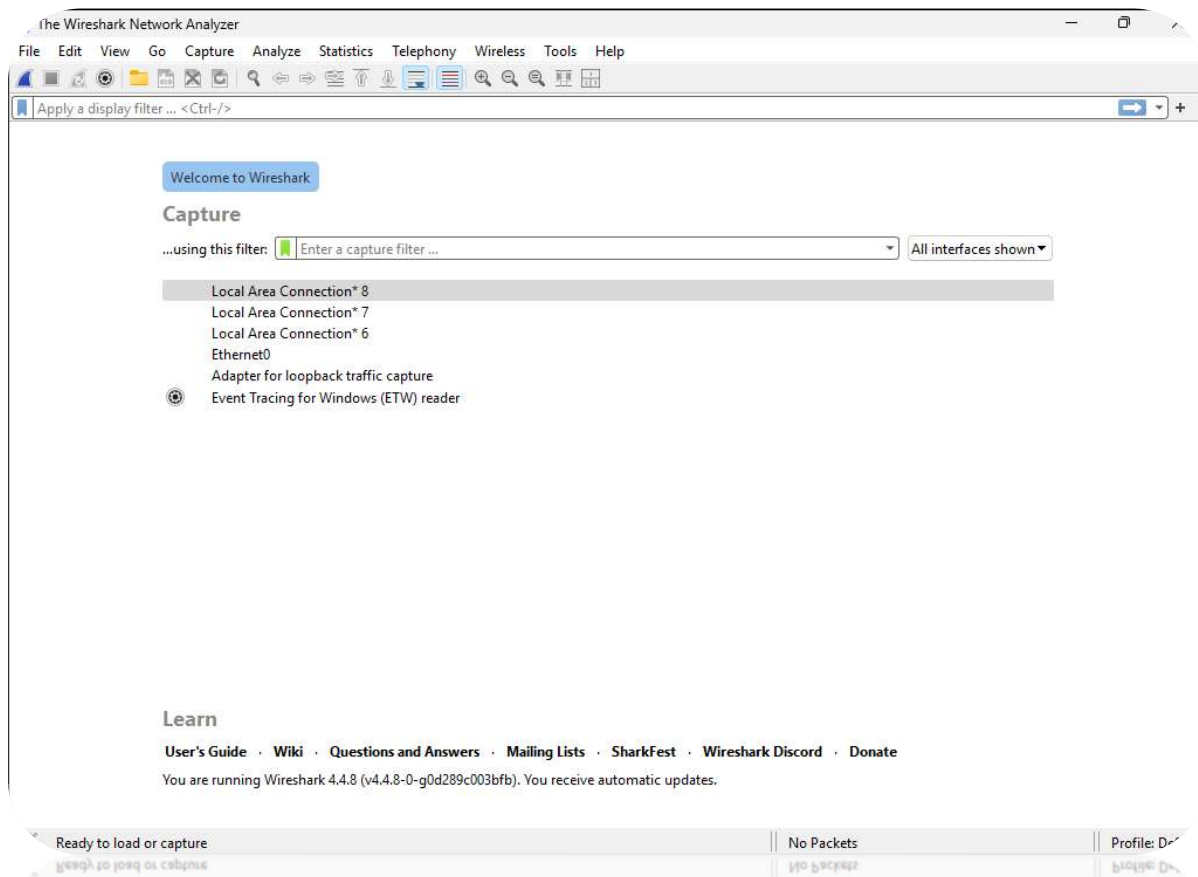




### 3. Dynamic Analysis

#### # Wireshark Tool (Screenshots)

##### 1. Before running malware



##### 2. After running malware

Measurement	Captured	Displayed
Packets	282	282 (100.0%)
Time span, s	352.836	352.836
Average pps	0.8	0.8
Average packet size, B	44	44
Bytes	12438	12438 (100.0%)
Average bytes/s	35	35
Average bits/s	282	282

ethernet0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
268	338.509382	VMware_27:ba:03	Broadcast	ARP	42	Who has 192.168.40.2? Tell 192.168.40.128
269	339.629611	VMware_27:ba:03	Broadcast	ARP	42	Who has 192.168.40.2? Tell 192.168.40.128
270	340.513270	VMware_27:ba:03	Broadcast	ARP	42	Who has 192.168.40.2? Tell 192.168.40.128
271	341.512784	VMware_27:ba:03	Broadcast	ARP	42	Who has 192.168.40.2? Tell 192.168.40.128
272	344.665040	VMware_27:ba:03	Broadcast	ARP	42	Who has 192.168.40.2? Tell 192.168.40.128
273	345.506802	VMware_27:ba:03	Broadcast	ARP	42	Who has 192.168.40.2? Tell 192.168.40.128
274	345.598245	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.40.2? Tell 192.168.40.1
275	346.513068	VMware_27:ba:03	Broadcast	ARP	42	Who has 192.168.40.2? Tell 192.168.40.128
276	346.916208	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.40.2? Tell 192.168.40.1
277	347.600000	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.40.2? Tell 192.168.40.1
278	348.597993	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.40.2? Tell 192.168.40.1
279	349.933478	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.40.2? Tell 192.168.40.1
280	350.585423	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.40.2? Tell 192.168.40.1
281	351.592722	VMware_c0:00:08	Broadcast	ARP	60	Who has 192.168.40.2? Tell 192.168.40.1
282	352.835967	VMware_27:ba:03	Broadcast	ARP	42	Who has 192.168.40.2? Tell 192.168.40.128

> Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on

> Ethernet II, Src: VMware\_27:ba:03 (00:0c:29:27:ba:03), Dst: Broadcast

> Address Resolution Protocol (request)

0000

ff ff ff ff ff ff 00 0c 29 27 ba 03 08 06 00 01

0010

08 00 06 04 00 01 00 0c 29 27 ba 03 c0 a8 28 80

0020

00 00 00 00 00 00 c0 a8 28 02

wireshark\_Ethernet0PJ4GA3.pcapng

Packets: 282 - Dropped: 0 (0.0%)

Profile: D...

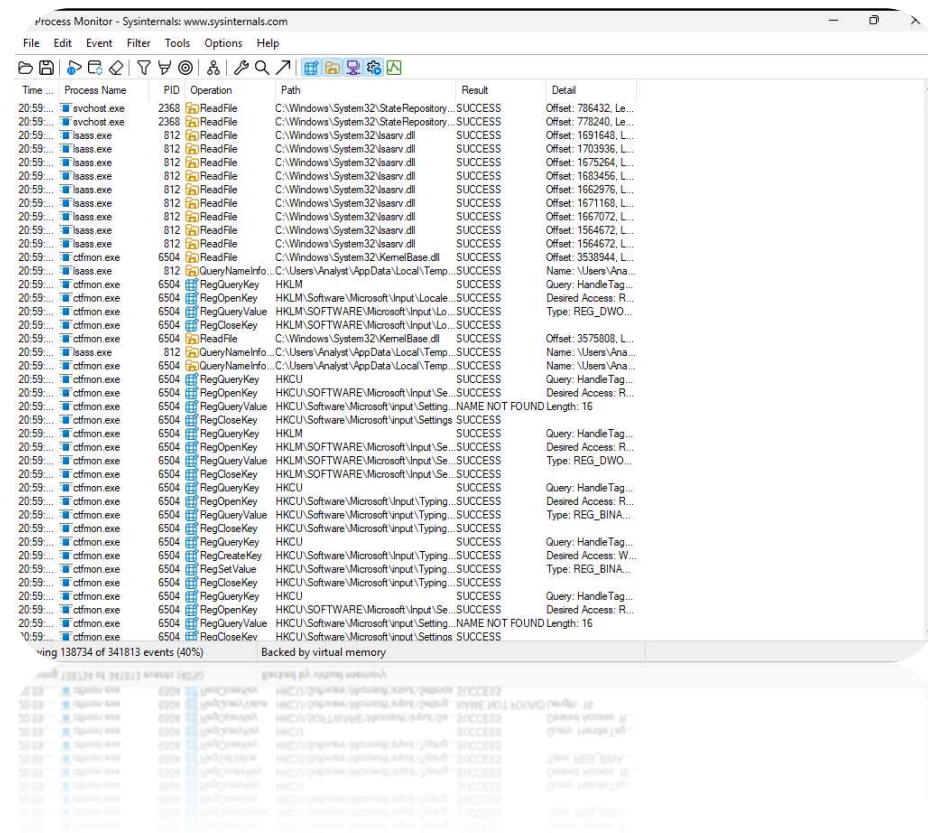
wireshark\_Ethernet0PJ4GA3.pcapng

Packets: 282 - Dropped: 0 (0.0%)

Profile: D...

# # Process Monitor Tool (Screenshots)

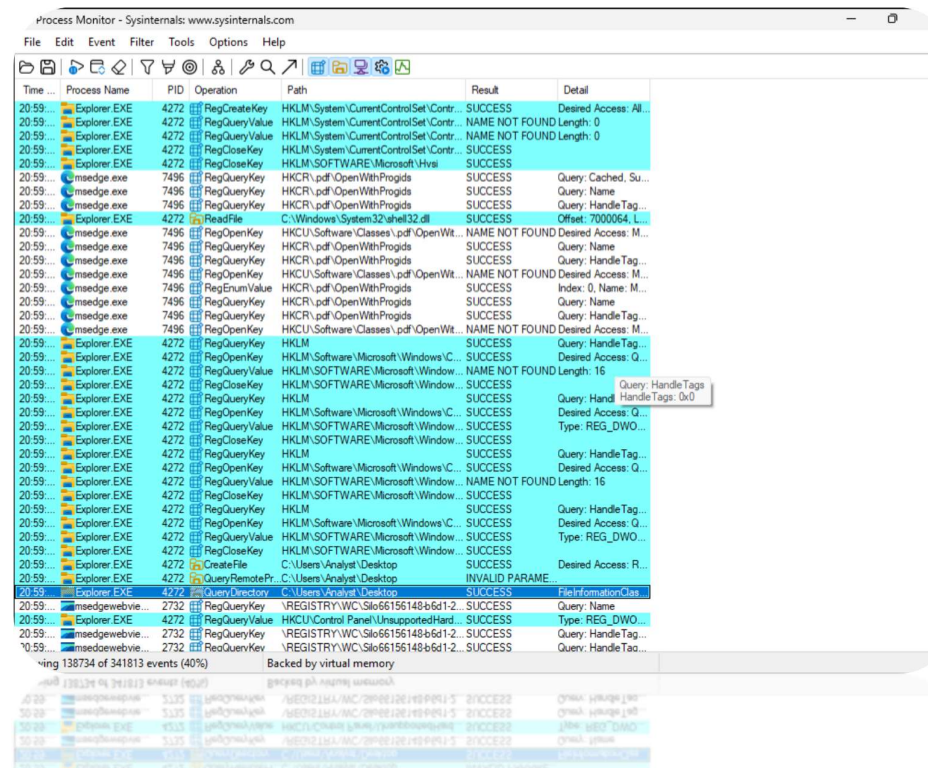
## 1. Before running malware



The screenshot shows the Process Monitor tool interface with the following table of events:

Time	Process Name	PID	Operation	Path	Result	Detail
20:59:...	svchost.exe	2368	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 786432, Le...
20:59:...	svchost.exe	2368	ReadFile	C:\Windows\System32\StateRepository...	SUCCESS	Offset: 778240, Le...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1691648, L...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1703936, L...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1675264, L...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1683456, L...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1662976, L...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1671168, L...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1667072, L...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1564672, L...
20:59:...	lsass.exe	812	ReadFile	C:\Windows\System32\lsassv.dll	SUCCESS	Offset: 1564672, L...
20:59:...	cfmon.exe	6504	ReadFile	C:\Users\Analyst\AppData\Local\Temp...	SUCCESS	Offset: 3538944, L...
20:59:...	cfmon.exe	6504	QueryNameInfo	C:\Users\Analyst\AppData\Local\Temp...	SUCCESS	Name: \Users\Ana...
20:59:...	cfmon.exe	6504	RegQueryValue	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Query: HandleTag...
20:59:...	cfmon.exe	6504	RegOpenKey	HKLM\Software\Microsoft\Input\Locale...	SUCCESS	Desired Access: R...
20:59:...	cfmon.exe	6504	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	Type: REG_DWO...
20:59:...	cfmon.exe	6504	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Lo...	SUCCESS	
20:59:...	cfmon.exe	6504	ReadFile	C:\Windows\System32\KernelBase.dll	SUCCESS	Offset: 3575808, L...
20:59:...	lsass.exe	812	QueryNameInfo	C:\Users\Analyst\AppData\Local\Temp...	SUCCESS	Name: \Users\Ana...
20:59:...	cfmon.exe	6504	RegQueryValue	HKCU\Software\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
20:59:...	cfmon.exe	6504	RegOpenKey	HKCU\Software\Microsoft\Input\Se...	SUCCESS	Desired Access: R...
20:59:...	cfmon.exe	6504	RegQueryValue	HKCU\Software\Microsoft\Input\Setting...	NAME NOT FOUND Length: 16	
20:59:...	cfmon.exe	6504	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	
20:59:...	cfmon.exe	6504	RegQueryKey	HKLM\Software\Microsoft\Input\Se...	SUCCESS	Query: HandleTag...
20:59:...	cfmon.exe	6504	RegOpenKey	HKLM\Software\Microsoft\Input\Se...	SUCCESS	Desired Access: R...
20:59:...	cfmon.exe	6504	RegQueryValue	HKLM\Software\Microsoft\Input\Se...	SUCCESS	Type: REG_DWO...
20:59:...	cfmon.exe	6504	RegCloseKey	HKLM\Software\Microsoft\Input\Se...	SUCCESS	
20:59:...	cfmon.exe	6504	RegQueryKey	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	Query: HandleTag...
20:59:...	cfmon.exe	6504	RegOpenKey	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	Desired Access: R...
20:59:...	cfmon.exe	6504	RegQueryValue	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	Type: REG_BINA...
20:59:...	cfmon.exe	6504	RegCloseKey	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	
20:59:...	cfmon.exe	6504	RegQueryKey	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	Query: HandleTag...
20:59:...	cfmon.exe	6504	RegCreateKey	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	Desired Access: W...
20:59:...	cfmon.exe	6504	RegSetValue	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	Type: REG_BINA...
20:59:...	cfmon.exe	6504	RegCloseKey	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	
20:59:...	cfmon.exe	6504	RegQueryKey	HKCU\Software\Microsoft\Input\Typing...	SUCCESS	Query: HandleTag...
20:59:...	cfmon.exe	6504	RegOpenKey	HKCU\Software\Microsoft\Input\Se...	SUCCESS	Desired Access: R...
20:59:...	cfmon.exe	6504	RegQueryValue	HKCU\Software\Microsoft\Input\Setting...	NAME NOT FOUND Length: 16	
20:59:...	cfmon.exe	6504	RegCloseKey	HKCU\Software\Microsoft\Input\Settings	SUCCESS	

## 2. After running malware



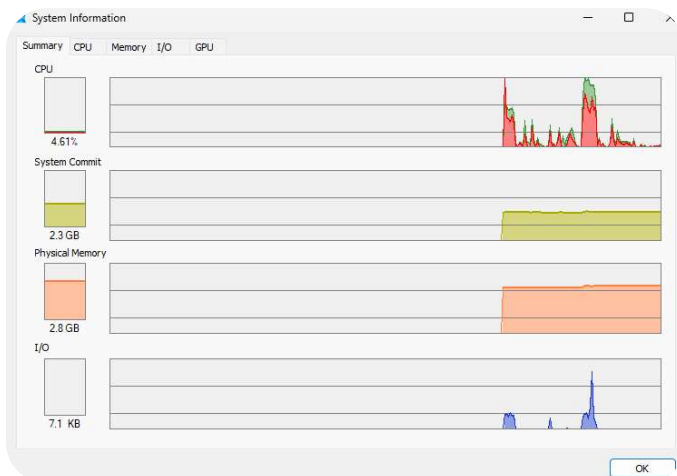
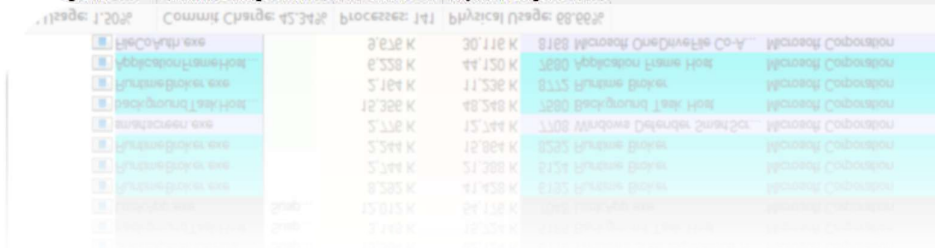
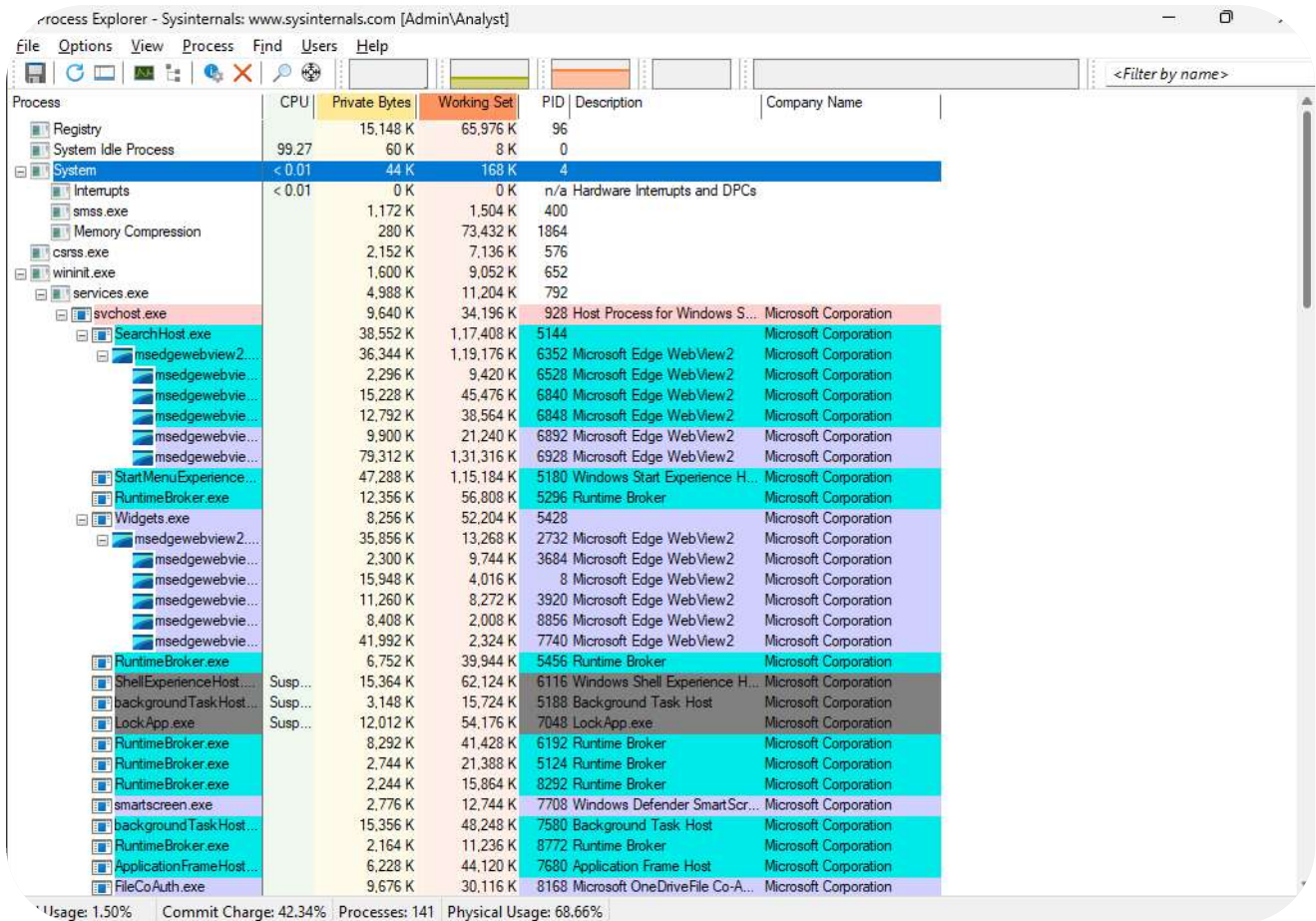
The screenshot shows the Process Monitor tool interface with the following table of events:

Time	Process Name	PID	Operation	Path	Result	Detail
20:59:...	Explorer.EXE	4272	RegCreateKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	Desired Access: All...
20:59:...	Explorer.EXE	4272	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 0	
20:59:...	Explorer.EXE	4272	RegQueryValue	HKLM\System\CurrentControlSet\Contr...	NAME NOT FOUND Length: 0	
20:59:...	Explorer.EXE	4272	RegCloseKey	HKLM\System\CurrentControlSet\Contr...	SUCCESS	
20:59:...	msedge.exe	7496	RegQueryKey	HKCU\Software\Microsoft\Hydra...	SUCCESS	Query: Cached, Su...
20:59:...	msedge.exe	7496	RegQueryKey	HKCR\pdf\OpenWithProgs	SUCCESS	Query: Name
20:59:...	msedge.exe	7496	RegQueryKey	HKCR\pdf\OpenWithProgs	SUCCESS	Query: HandleTag...
20:59:...	Explorer.EXE	4272	ReadFile	C:\Windows\System32\shell32.dll	SUCCESS	Offset: 7000064, L...
20:59:...	msedge.exe	7496	RegOpenKey	HKCU\Software\Classes\pdf\OpenWith...	NAME NOT FOUND Desired Access: M...	
20:59:...	msedge.exe	7496	RegQueryKey	HKCR\pdf\OpenWithProgs	SUCCESS	Query: Name
20:59:...	msedge.exe	7496	RegQueryKey	HKCR\pdf\OpenWithProgs	SUCCESS	Query: HandleTag...
20:59:...	msedge.exe	7496	RegOpenKey	HKCU\Software\Classes\pdf\OpenWith...	NAME NOT FOUND Desired Access: M...	
20:59:...	msedge.exe	7496	RegEnumValue	HKCR\pdf\OpenWithProgs	SUCCESS	Index: 0, Name: M...
20:59:...	msedge.exe	7496	RegQueryKey	HKCR\pdf\OpenWithProgs	SUCCESS	Query: Name
20:59:...	msedge.exe	7496	RegQueryKey	HKCR\pdf\OpenWithProgs	SUCCESS	Query: HandleTag...
20:59:...	msedge.exe	7496	RegOpenKey	HKCU\Software\Classes\pdf\OpenWith...	NAME NOT FOUND Desired Access: M...	
20:59:...	Explorer.EXE	4272	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
20:59:...	Explorer.EXE	4272	RegOpenKey	HKLM\Software\Microsoft\Windows\Co...	SUCCESS	Desired Access: Q...
20:59:...	Explorer.EXE	4272	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND Length: 16	
20:59:...	Explorer.EXE	4272	RegQueryKey	HKLM	SUCCESS	Query: Handl...
20:59:...	Explorer.EXE	4272	RegOpenKey	HKLM\Software\Microsoft\Windows\Co...	SUCCESS	Desired Access: Q...
20:59:...	Explorer.EXE	4272	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWO...
20:59:...	Explorer.EXE	4272	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
20:59:...	Explorer.EXE	4272	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
20:59:...	Explorer.EXE	4272	RegOpenKey	HKLM\Software\Microsoft\Windows\Co...	SUCCESS	Desired Access: Q...
20:59:...	Explorer.EXE	4272	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	NAME NOT FOUND Length: 16	
20:59:...	Explorer.EXE	4272	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
20:59:...	Explorer.EXE	4272	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
20:59:...	Explorer.EXE	4272	RegOpenKey	HKLM\Software\Microsoft\Windows\Co...	SUCCESS	Desired Access: Q...
20:59:...	Explorer.EXE	4272	RegQueryValue	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	Type: REG_DWO...
20:59:...	Explorer.EXE	4272	RegCloseKey	HKLM\SOFTWARE\Microsoft\Window...	SUCCESS	
20:59:...	Explorer.EXE	4272	CreateFile	C:\Users\Analyst\Desktop	SUCCESS	Desired Access: R...
20:59:...	Explorer.EXE	4272	QueryRemotePro...	C:\Users\Analyst\Desktop	INVALID PARAM...	
20:59:...	msedge.exe	2732	RegQueryDirectory	C:\Users\Analyst\Desktop	SUCCESS	FileInformationClas...
20:59:...	msedge.exe	2732	RegQueryKey	\REGISTRY\WC\Slo66156148-b6d1-2...	SUCCESS	Query: Name
20:59:...	msedge.exe	2732	RegQueryValue	HKCU\Control Panel\UnsupportedHard...	SUCCESS	Type: REG_DWO...
20:59:...	msedge.exe	2732	RegQueryKey	\REGISTRY\WC\Slo66156148-b6d1-2...	SUCCESS	Query: HandleTag...
20:59:...	msedge.exe	2732	RegQueryKey	\REGISTRY\WC\Slo66156148-b6d1-2...	SUCCESS	Query: HandleTag...

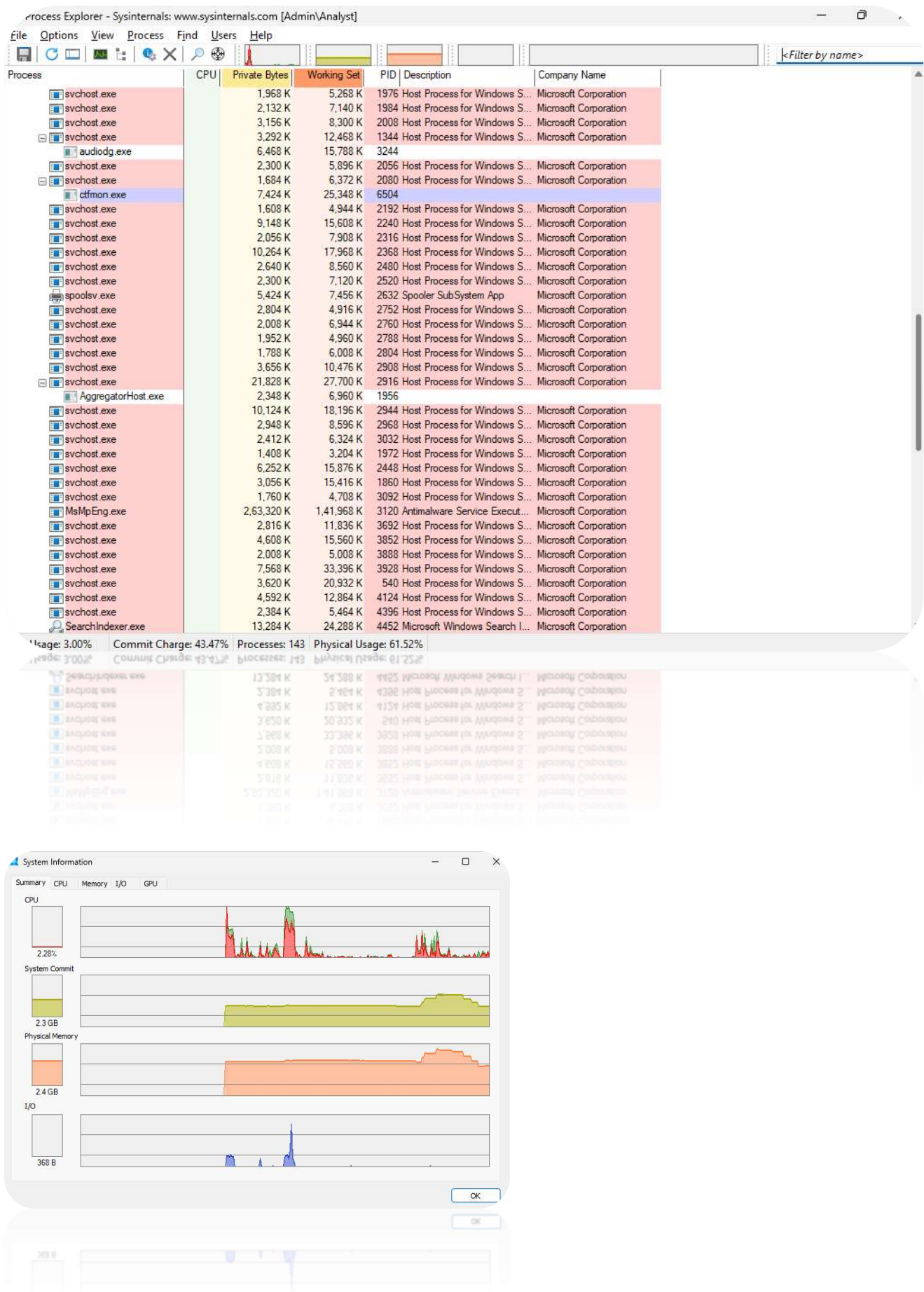


# # Process Explorer Tool (Screenshots)

## 1. Before running malware



## 2. After running malware



## # TCP View Tool (Screenshots)

## 1. Before running malware

File Edit View Process Connection Options Help

TCP v4 TCP v6 UDP v4 UDP v6

Search

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time
fakenet.exe	8000	TCP	Listen	0.0.0.0	21	0.0.0.0	0	02-08-2025 20:41
fakenet.exe	8000	TCP	Listen	0.0.0.0	25	0.0.0.0	0	02-08-2025 20:41
fakenet.exe	8000	TCP	Listen	0.0.0.0	80	0.0.0.0	0	02-08-2025 20:41
fakenet.exe	8000	TCP	Listen	0.0.0.0	110	0.0.0.0	0	02-08-2025 20:41
svchost.exe	436	TCP	Listen	0.0.0.0	135	0.0.0.0	0	02-08-2025 20:34
System	4	TCP	Listen	192.168.40.128	139	0.0.0.0	0	02-08-2025 20:42
fakenet.exe	8000	TCP	Listen	0.0.0.0	443	0.0.0.0	0	02-08-2025 20:41
fakenet.exe	8000	TCP	Listen	0.0.0.0	1337	0.0.0.0	0	02-08-2025 20:41
svchost.exe	4124	TCP	Listen	0.0.0.0	5040	0.0.0.0	0	02-08-2025 20:34
fakenet.exe	8000	TCP	Listen	0.0.0.0	6667	0.0.0.0	0	02-08-2025 20:41
fakenet.exe	8000	TCP	Listen	0.0.0.0	38926	0.0.0.0	0	02-08-2025 20:41
lsass.exe	812	TCP	Listen	0.0.0.0	49664	0.0.0.0	0	02-08-2025 20:34
wininit.exe	652	TCP	Listen	0.0.0.0	49665	0.0.0.0	0	02-08-2025 20:34
svchost.exe	1268	TCP	Listen	0.0.0.0	49666	0.0.0.0	0	02-08-2025 20:34
svchost.exe	1612	TCP	Listen	0.0.0.0	49667	0.0.0.0	0	02-08-2025 20:34
spoolsv.exe	2632	TCP	Listen	0.0.0.0	49668	0.0.0.0	0	02-08-2025 20:34
services.exe	792	TCP	Listen	0.0.0.0	49669	0.0.0.0	0	02-08-2025 20:34
svchost.exe	2316	TCP	Syn Sent	192.168.40.128	57756	192.0.2.123	80	02-08-2025 20:55
svchost.exe	2316	TCP	Syn Sent	192.168.40.128	57757	192.0.2.123	80	02-08-2025 20:55
msedgeview2.exe	6848	TCP	Syn Sent	192.168.40.128	57758	192.0.2.123	443	02-08-2025 20:55
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0	02-08-2025 20:34
svchost.exe	436	TCPv6	Listen	::	135	::	0	02-08-2025 20:34
System	4	TCPv6	Listen	::	445	::	0	02-08-2025 20:34
lsass.exe	812	TCPv6	Listen	::	49664	::	0	02-08-2025 20:34
wininit.exe	652	TCPv6	Listen	::	49665	::	0	02-08-2025 20:34
svchost.exe	1268	TCPv6	Listen	::	49666	::	0	02-08-2025 20:34
svchost.exe	1612	TCPv6	Listen	::	49667	::	0	02-08-2025 20:34
spoolsv.exe	2632	TCPv6	Listen	::	49668	::	0	02-08-2025 20:34
services.exe	792	TCPv6	Listen	::	49669	::	0	02-08-2025 20:34
fakenet.exe	8000	UDP	Listen	0.0.0.0	53	*	0	02-08-2025 20:41

Summary: 51 Established, 26 Listening, 0 Time Wait, 0 Close Wait, 2 sec Update, States: (All)

Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time
svchost.exe	8000	TCP	Listen	0.0.0.0	21	0.0.0.0	0	02-08-2025 20:41
svchost.exe	436	TCPv6	Listen	::	135	::	0	02-08-2025 20:34
svchost.exe	5825	TCPv6	Listen	::	135	::	0	02-08-2025 20:34
svchost.exe	1612	TCPv6	Listen	::	135	::	0	02-08-2025 20:34
svchost.exe	1268	TCPv6	Listen	::	135	::	0	02-08-2025 20:34
svchost.exe	8000	TCPv6	Listen	::	135	::	0	02-08-2025 20:34

## 2. After running malware

[illegible]



## 4. Risk Classification

- **Risk Level:** High
- **Threat Type:** Remote-Access Trojan with credential stealing potential

## 5. Mitigation and Recommendations

- Block external communication to IP **3.131.193.27** and related domains.
- Delete the file and any spawned artifacts.
- Remove malicious registry entries.
- Reimage system if integrity cannot be ensured.
- Update endpoint protection signatures.

## 6. Conclusion

- The analysed sample **WEXTRACT.EXE** is a **Windows-based Trojan** with SHA256 hash **91bfa2...6754aac**. It was delivered via a suspicious external URL and is capable of performing a range of malicious activities. **Static analysis** revealed the executable was unsigned, packed using Microsoft Visual C++, and contained several suspicious capabilities such as persistence via registry, **file manipulation, process injection, and host interrogation**. **Dynamic analysis** confirmed that the malware initiates network communication (observed via **Wireshark**), interacts with the Windows registry, and launches or injects processes post-execution. The average packet size and consistent communication post-execution strongly suggest **C2 (Command and Control) behaviour**. Tools like **Process Monitor** and **TCPView** also indicated significant process and network activity that were not present before execution.