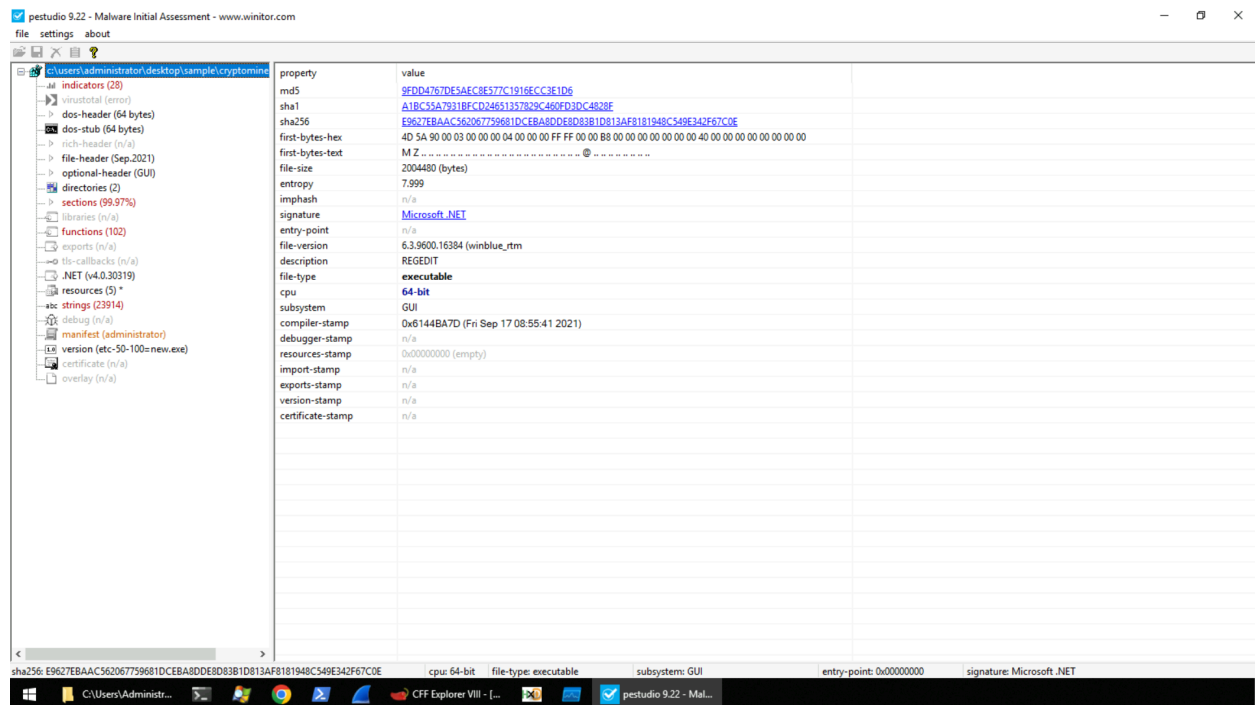


FlareVM Arsenal Tools (Malware Analysis)

Analyse using PEStudio

PEStudio is particularly useful for malware analysis, reverse engineering, and security research, as it helps analysts understand the structure and behavior of executable files without executing them.



The Main Tab provides an overview of the file being analyzed. This tab is the starting point for inspecting the properties and characteristics of a Windows executable. It is designed to give us a quick snapshot of critical information about the file, so we can start the analysis.

PEStudio also displays the initial bytes of the file in hexadecimal format. For instance, if the first bytes are '4D 5A', this confirms that the file is a Windows Executable. While users typically recognize files by their extensions, like '.exe', the operating system identifies file types based on the byte patterns in their headers. A Windows executable will always start with '4D 5A' in hex, which corresponds to 'MZ' in ASCII.

Additionally, PEStudio lists the file's entropy, which is useful for determining whether the malware is packed. Packed malware is often obfuscated to make it harder for analysts to quickly understand its functionality. Entropy is measured on a scale from 0 to 8, with higher values indicating a greater likelihood that the malware is packed. Values between 7 and 8 strongly suggest that the sample is packed, indicating that unpacking the malware will be necessary to extract useful indicators of compromise (IoCs).

file-size	2004480 (bytes)
entropy	7.999

The indicators tab, this highlights data within the sample that may be malicious.

pestudio 9.22 - Malware Initial Assessment - www.winitor.com

file settings about

c:\users\administrator\desktop\sample\cryptomine

indicators (28)

indicator (28)	detail	level
The file references string(s)	type: blacklist, count: 1	1
The address of the entry-point is suspicious	address: 0x00000000	1
The file execution privilege has been found	level: administrator	1
The file-ratio of the .NET resources is high	ratio: 99.48 %	2
The original name of the file has been detected	name: etc-50-100=new.exe	3
The manifest identity has been found	name: Program.app	3
The file references a group of API	type: execution, count: 8	3
The file references a group of API	type: obfuscation, count: 2	3
The file references a group of API	type: file, count: 4	3
The file references a group of API	type: memory, count: 2	3
The file references a group of API	type: cryptography, count: 10	3
The file references a group of hint	type: format-string, count: 17	3
The file references a group of hint	type: utility, count: 7	3
The file references a group of hint	type: file, count: 21	3
The file references a group of hint	type: base64, count: 2	3
The .NET file is strongly-named	status: no	3
The .NET file references Managed Methods	count: 35	3
The file score is not available	The operation timed out	4
The file contains a rich-header	status: no	4
The file uses Control Flow Guard (CFG) as software security defense	status: no	4
The file opts for Data Execution Prevention (DEP) as software security defense	status: yes	4
The file opts for Address Space Layout Randomization (ASLR) as software security defense	status: yes	4
The file subsystem has been found	type: GUI	4
The file contains a Manifest	status: yes	4
The file contains a digital Certificate	status: no	4
The file-ratio of the section(s) has been determined	ratio: 99.97%	4
The file references string(s)	type: ascii, count: 23859	4
The file references string(s)	type: unicode, count: 44	4

sha256: E9627EBAAC562067799681DCEBA8DDE8D83B1D813AF8181948C549E342F67C0E cpu: 64-bit file-type: executable subsystem: GUI entry-point: 0x00000000 signature: Microsoft .NET

The image above demonstrates how PeStudio has detected several indicators and categorized them on a scale from 1 to 3, with 1 representing a highly likely malicious indicator. In this case, PeStudio has flagged certain suspicious strings, sections, and imports, as well as identified another file within the sample. This information is valuable because PeStudio provides tabs on the left for strings, sections, and imports, enabling further exploration of these potentially harmful indicators.

pestudio 9.22 - Malware Initial Assessment - www.winitor.com

file settings about

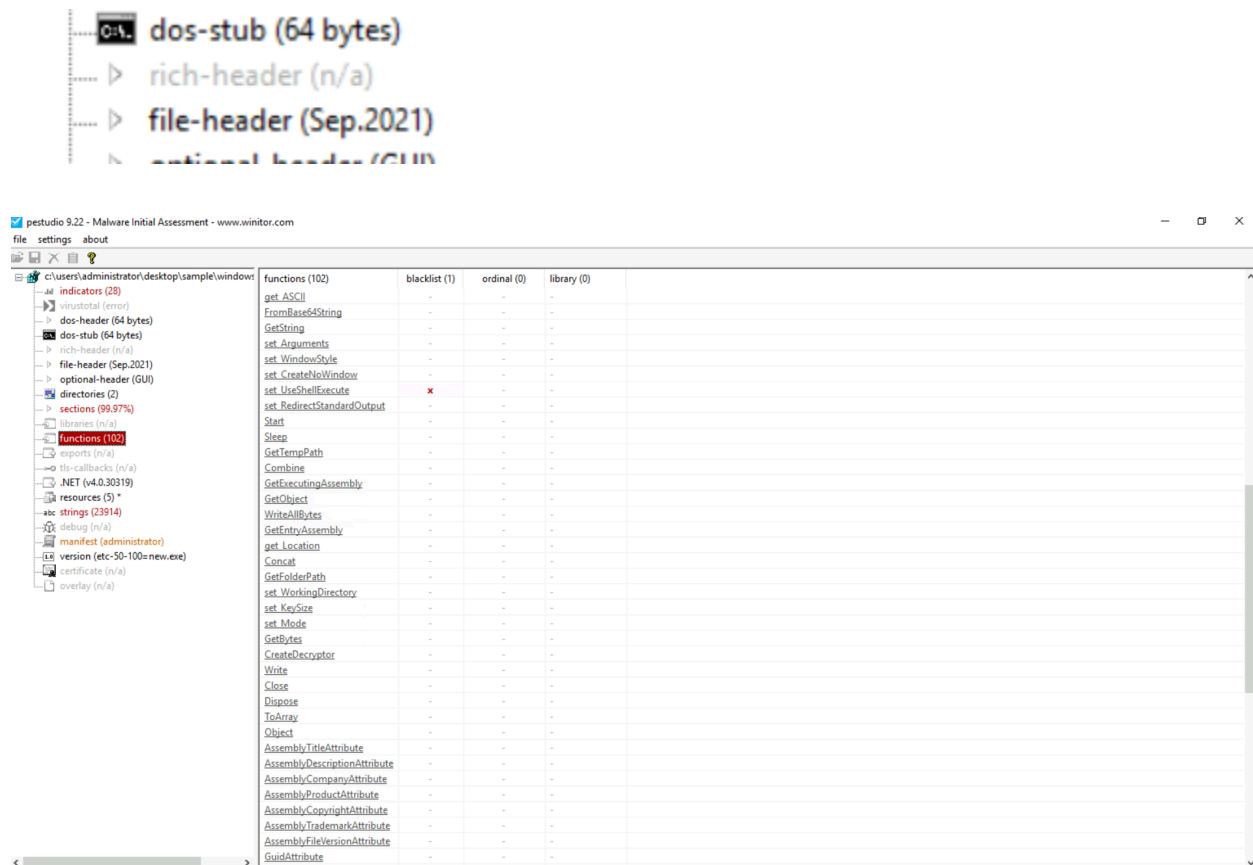
c:\users\administrator\desktop\sample\cryptomine

indicators (28)

property	value	value
name	.text	.rsrc
md5	S20D2B9C8CD340CEB84DD...	02999421402483CC3B9F536...
entropy	8.000	4.139
file-ratio (99.97%)	99.82 %	0.15 %
raw-address	0x00000020	0x01E8A00
raw-size (2003968 bytes)	0x001E8800 (2000896 bytes)	0x000000C00 (3072 bytes)
virtual-address	0x0000000040002000	0x00000000401EC000
virtual-size (2003596 bytes)	0x001E870C (2000652 bytes)	0x000000B80 (2944 bytes)
entry-point	0x00000000	0x00000000
characteristics	0x60000020	0x40000040
writable	-	-
executable	x	-
shareable	-	-
discardable	-	-
initialized-data	-	x
uninitialized-data	-	-
unreadable	-	-
self-modifying	-	-
virtualized	-	-
file	n/a	n/a

sha256: E9627EBAAC562067799681DCEBA8DDE8D83B1D813AF8181948C549E342F67C0E cpu: 64-bit file-type: executable subsystem: GUI entry-point: 0x00000000 signature: Microsoft .NET

The '.text' section contains executable code, looking at the columns of the section names we can see an 'x' next to the permission pane indicating that this section has executable permissions. The '.rdata' and '.data' sections store data, and PeStudio has identified that the data section is writable. The '.idata' section stores the Import Address Table, the IAT is covered later in the article. The '.rsrc' section stores resources that can be used by the malware such as strings and additional files.



In malware analysis, set_UseShellExecute is often used to determine whether the malicious executable should be launched using the Windows shell (true), allowing it to inherit shell environment settings, or directly (false), which can be used to control and redirect output, potentially hiding its behavior.

Using FLOSS for Malware Analysis: Run FLOSS on the sample: `bash Copy floss sample.exe`
Look for suspicious strings in the output, such as: IP addresses (e.g., 192.168.1.1) Domains (e.g., malicious-site.com) File paths (e.g., C:\Windows\Temp\) Keywords related to malware (e.g., dropper, payload) Investigate: Once you have these strings, you can research whether they correspond to known malware infrastructure or patterns, giving insight into the malware's behavior.

```
PS C:\Users\Administrator\Desktop\Sample > Floss.exe windows.exe > floss.txt
WARNING: floss: .NET language-specific string extraction is not supported yet
WARNING: floss: FLOSS does NOT attempt to deobfuscate any strings from .NET binaries
INFO: floss: disabled string deobfuscation
INFO: floss: extracting static strings
INFO: floss: finished execution after 0.50 seconds
INFO: floss: rendering results
```

For example we use windows.exe as malware files. We use `> floss.txt` to convert the result into a text file.



We can open the file and the result will be similar to the previous analysis using PEStudio.

Analyse using process explorer

Process Explorer - Sysinternals: www.sysinternals.com [WIN-7B50GHBP51\Administrator] (Administrator)

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System	100.00	56 K	8 K	0		
System Idle Process	< 0.01	188 K	148 K	4		
System	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe	< 0.01	496 K	1,184 K	428	Windows Session Manager	Microsoft Corporation
csrss.exe		2,452 K	5,336 K	500	Client Server Runtime Process	Microsoft Corporation
csrss.exe		1,676 K	4,612 K	656	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,416 K	6,416 K	676	Windows Start-Up Application	Microsoft Corporation
services.exe		4,744 K	9,464 K	792	Services and Controller app	Microsoft Corporation
svchost.exe		884 K	3,676 K	920	Host Process for Windows S...	Microsoft Corporation
svchost.exe		6,664 K	21,920 K	940	Host Process for Windows S...	Microsoft Corporation
ShellExperienceHost.exe	Susp...	10,012 K	55,976 K	4008	Windows Shell Experience H...	Microsoft Corporation
SearchUI.exe	Susp...	26,508 K	70,784 K	4920	Search and Cortana applicati...	Microsoft Corporation
RuntimeBroker.exe		5,224 K	19,572 K	4988	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		5,436 K	16,484 K	5100	Runtime Broker	Microsoft Corporation
RuntimeBroker.exe		2,976 K	14,972 K	5124	Runtime Broker	Microsoft Corporation
VimProVSE.exe		2,568 K	8,732 K	4160	VMH Provider Host	Microsoft Corporation
svchost.exe		4,680 K	11,024 K	448	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,624 K	10,400 K	604	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,708 K	11,128 K	1028	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	32,832 K	46,572 K	1040	Host Process for Windows S...	Microsoft Corporation
lsidpdp.exe		2,644 K	11,128 K	2832	RDP Clipboard Monitor	Microsoft Corporation
svchost.exe		1,960 K	9,628 K	1096	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,252 K	5,088 K	1280	Host Process for Windows S...	Microsoft Corporation
svchost.exe		10,308 K	14,300 K	1288	Host Process for Windows S...	Microsoft Corporation
svchost.exe	< 0.01	1,648 K	11,624 K	1296	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,380 K	5,580 K	1392	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,828 K	7,556 K	1456	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,500 K	11,284 K	1464	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,280 K	5,556 K	1472	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,784 K	7,580 K	1480	Host Process for Windows S...	Microsoft Corporation
svchost.exe		3,276 K	7,132 K	1540	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,080 K	7,308 K	1572	Host Process for Windows S...	Microsoft Corporation
svchost.exe		1,952 K	8,392 K	1596	Host Process for Windows S...	Microsoft Corporation
svchost.exe		4,776 K	13,980 K	1640	Host Process for Windows S...	Microsoft Corporation
taskhostw.exe		4,492 K	13,908 K	3888	Host Process for Windows T...	Microsoft Corporation
cmd.exe	< 0.01	2,064 K	3,548 K	5824	Windows Command Processor	Microsoft Corporation
conhost.exe		6,664 K	2,452 K	5852	Console Window Host	Microsoft Corporation
svchost.exe		3,692 K	10,412 K	1672	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,332 K	7,740 K	1696	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,000 K	8,644 K	1704	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,116 K	11,856 K	1788	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,360 K	8,192 K	1860	Host Process for Windows S...	Microsoft Corporation
svchost.exe		2,228 K	7,480 K	1868	Host Process for Windows S...	Microsoft Corporation

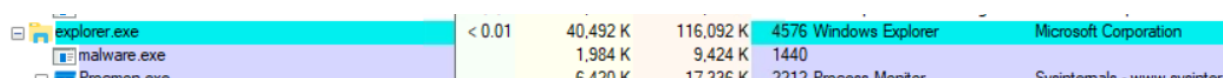
CPU Usage: 0.00% | Commit Charge: 13.57% | Processes: 104 | Physical Usage: 28.54%

Process Explorer is a powerful tool from Sysinternals (now owned by Microsoft) that provides detailed information about the processes running on a system, including those initiated by

Muhammad Hisyam

Github - Cybersecurity Notes

potentially malicious software. It's widely used in malware analysis because it can help analysts identify suspicious activities, understand the behavior of malware, and track down malicious processes or services running on a system.

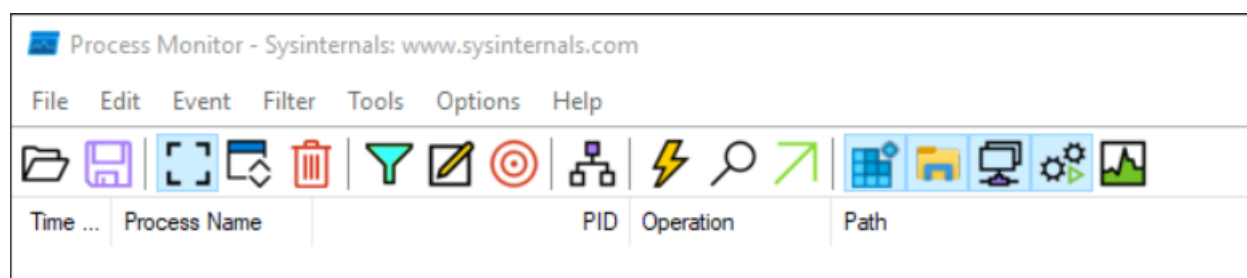


Process Name	CPU	Private Memory	Working Set	PID	Company Name
explorer.exe	< 0.01	40,492 K	116,092 K	4576	Windows Explorer
malware.exe	1,984 K	9,424 K	1440		
smss.exe	6,420 K	17,336 K	2212		Process Monitor

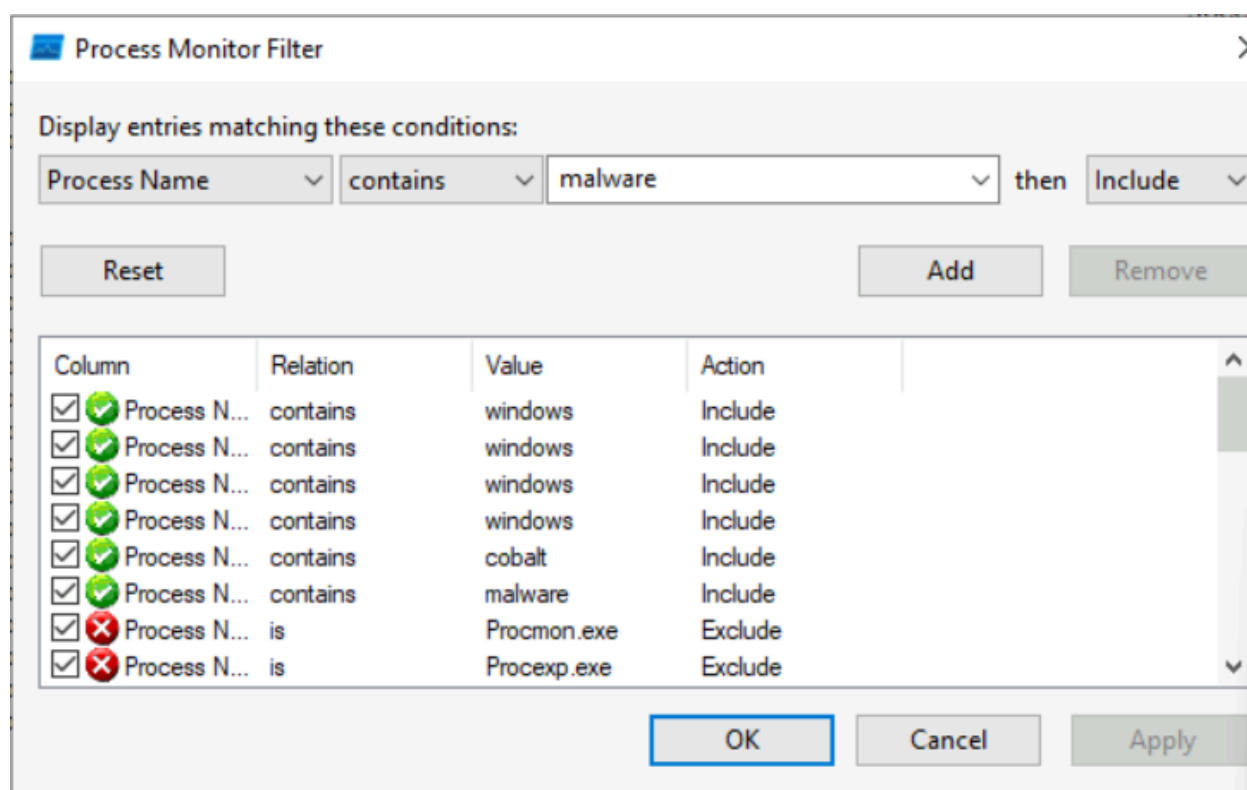
1. View Running Processes and Their Details: Process Explorer shows a detailed list of all processes, including those that might not show up in the regular Task Manager. This includes information such as:
 - Process name
 - PID (Process ID)
 - CPU, memory, and disk usage
 - Parent-child relationships between processes
 - Path to executable file
2. Malware often hides or disguises its presence by injecting into legitimate processes, so Process Explorer can help you spot unusual or unexpected processes.
3. Check the Digital Signature of Processes: If a process is signed with a valid digital certificate, Process Explorer will display the signing information. In malware analysis, if you see a process without a signature or with a suspicious or forged signature, that's often a red flag.
4. Analyze Process Tree: Process Explorer allows you to view the hierarchy of processes (parent-child relationships). This is useful when malware spawns multiple processes. For instance, a malware dropper might spawn a malicious process as a child of a legitimate one. Examining the process tree can help track the origin of the malware.
5. Check for Suspicious Process Names: Malware often uses deceptive names to blend in with legitimate processes. By carefully reviewing the process list, you can spot processes with unusual or random names, or processes running from strange locations (like temporary directories or the user's AppData folder).
6. Inspect Loaded DLLs: Malware often injects malicious code into other processes by loading DLLs (Dynamic Link Libraries). You can right-click on any process in Process Explorer and select Properties to see a list of DLLs loaded by that process. This is essential in identifying injected malicious code or trojanized DLLs.
7. Check Network Connections: You can view network activity by selecting a process and examining its TCP/IP or UDP connections. If a process is communicating with suspicious external IP addresses or domains (often associated with command-and-control servers), this could indicate malicious behavior.
 - Look for unusual ports or unfamiliar external IP addresses.
 - If malware is attempting to exfiltrate data or communicate with a C2 server, Process Explorer can help identify those connections.
8. Process Threads and Handles: Malware may spawn additional threads or create handles to resources (files, registry keys, etc.). Analyzing these threads and handles can provide insight into what the malware is doing (e.g., writing to disk, modifying the registry, etc.).

9. Search for Process Injection: Many types of malware use process injection techniques to hide in plain sight. You can look for suspicious behavior, such as when one process is loading code into another. Process Explorer allows you to inspect processes for signs of injected code or hidden threads.

Analyse using process monitor



To use the process monitor we can choose existing tools. We will use filter tools to select the applications that will be used in the analysis stage.



After we specified the filter, the result malware will be shown below.

Time ...	Process Name	PID	Operation	Path	Result	Detail
11:27...	malware.exe	1440	TCP Reconnect		SUCCESS	Length: 0, seqnum: 0, connid: 0
11:27...	malware.exe	1440	TCP Disconnect		SUCCESS	Length: 0, seqnum: 0, connid: 0
11:27...	malware.exe	1440	TCP Reconnect		SUCCESS	Length: 0, seqnum: 0, connid: 0
11:27...	malware.exe	1440	TCP Reconnect		SUCCESS	Length: 0, seqnum: 0, connid: 0