Lab - Finding Malware with Sysinternal's Process Explorer

Overview

In this lab, you will learn how to detect the presence of malware on an infected Windows computer using Sysinternal's Process Explorer.

Process Explorer is a tool that lets us access a lot of information about processes running on a Windows machine, offering features we can leverage to analyze and determine if something is malicious.

Lab Requirements

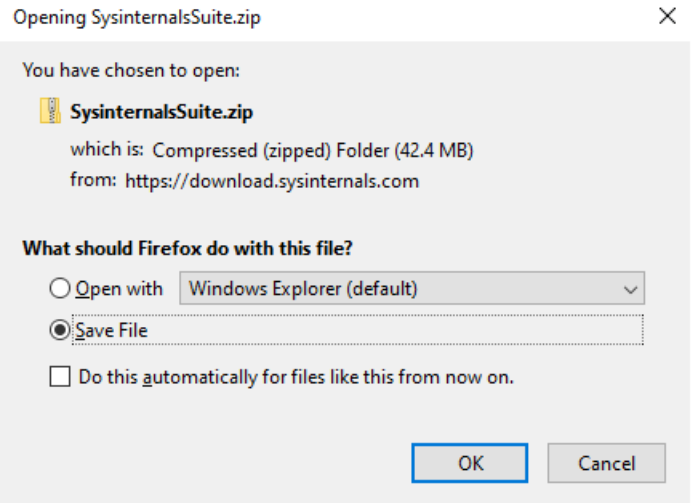
- One virtual install of Windows 10
- One download of the Windows Sysinternal Suite of tools saved to your Windows 10 virtual machine.

Download the Sysinternal suite of tools

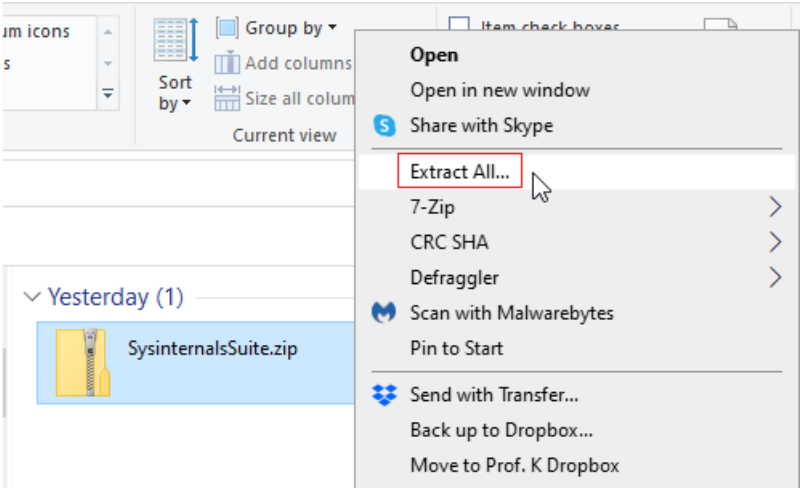
Copy and paste the following URL into the browser of your virtual machine.

https://download.sysinternals.com/files/SysinternalsSuite.zip

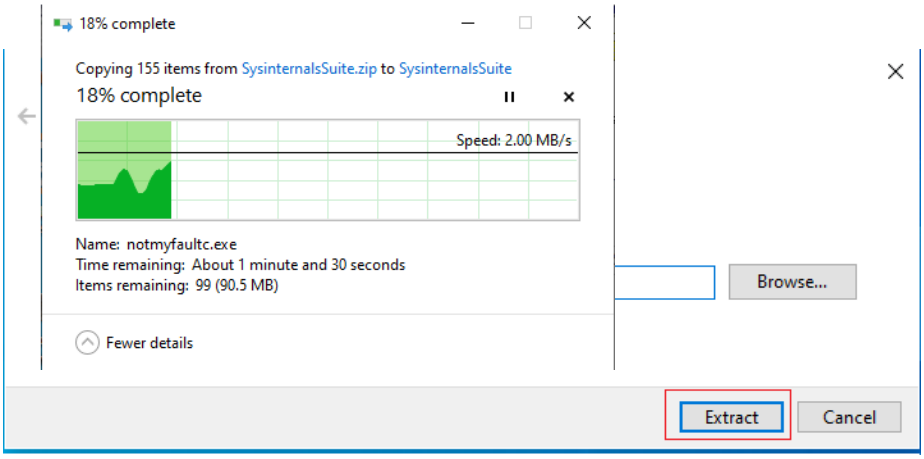
Save the file to the Download directory of your virtual machine.



From the saved location, right-click on the downloaded archive, and from the context menu, select extract all.

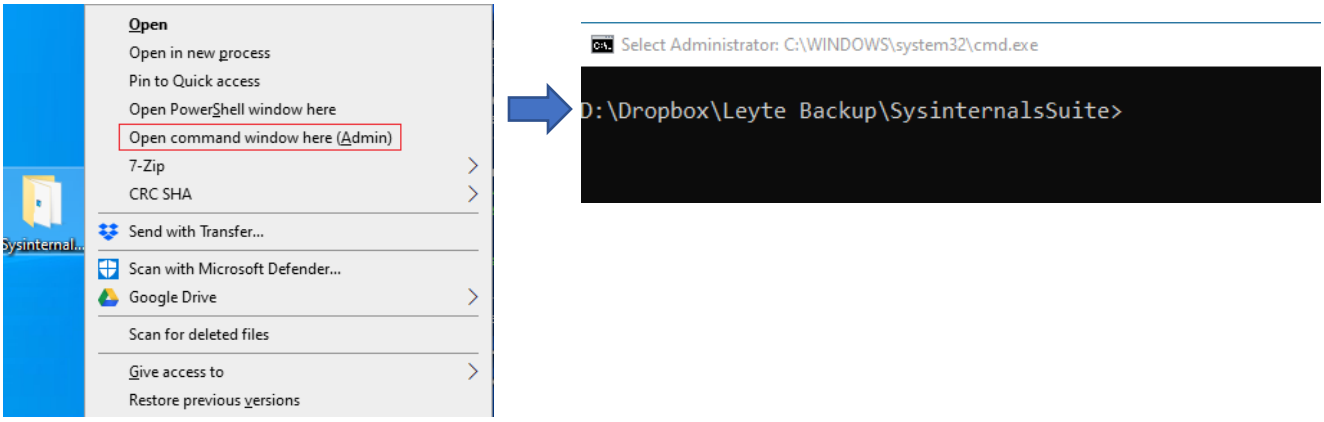


Save the extracted folder to the same location.



Find the extracted folder on your desktop. Next, hold down the shift key on your keyboard and right-click on the extracted folder. This brings up the extended context menu. From the top of the context menu, select **Open a command window here (Admin).**

This opens the folder in a terminal or command prompt window.



To see the contents of the folder, at the prompt type, **dir**.

```
Administrator: C:\WINDOWS\system32\cmd.exe

D:\Dropbox\Leyte Backup\SysinternalsSuite>dir
 Volume in drive D has no label.
 Volume Serial Number is 9A67-6423

 Directory of D:\Dropbox\Leyte Backup\SysinternalsSuite

03/09/2021  11:08 PM    <DIR>          .
03/09/2021  11:08 PM    <DIR>          ..
03/09/2021  11:08 PM         1,379,216 accesschk.exe
03/09/2021  11:08 PM           759,680 accesschk64.exe
03/09/2021  11:07 PM           174,968 AccessEnum.exe
03/09/2021  11:07 PM            50,379 AdExplorer.chm
03/09/2021  11:07 PM         1,162,120 ADExplorer.exe
03/09/2021  11:07 PM           617,352 ADExplorer64.exe
03/09/2021  11:07 PM           401,616 ADInsight.chm
03/09/2021  11:07 PM         5,106,056 ADInsight.exe
```

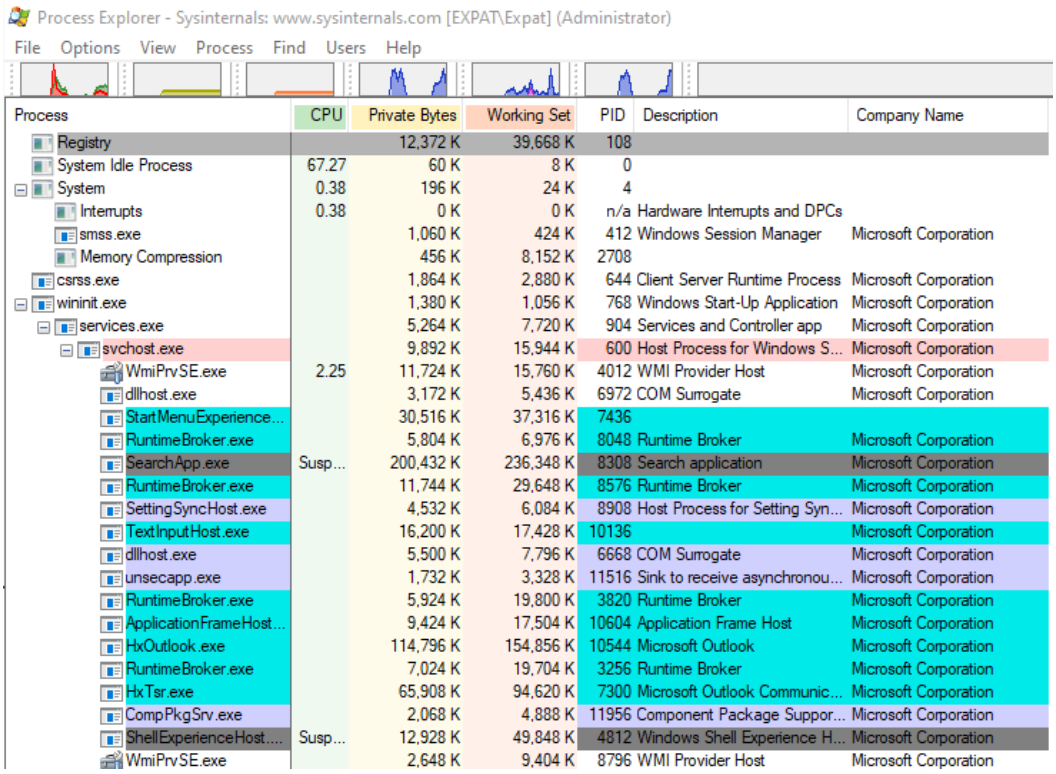
Scroll down through the list of tools until you find **procexp64.exe**

Highlight the name of the utility and use the Crtl+C key to copy the name. Scroll down to a new prompt, and using your right mouse button, click one time at the prompt to paste in the utility's name. Press enter to launch Process Explorer.

```
03/09/2021  11:07 PM         1,059,712 ZoomIt.exe
03/09/2021  11:07 PM           588,152 ZoomIt64.exe
             155 File(s)    114,949,440 bytes
               2 Dir(s)  288,182,284,288 bytes free

D:\Dropbox\Leyte Backup\SysinternalsSuite>procexp64.exe
```

After a short pause, Process Explorer opens.



Process Explorer - Sysinternals: www.sysinternals.com [EXPAT\Expat] (Administrator)

File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
Registry		12,372 K	39,668 K	108		
System Idle Process	67.27	60 K	8 K	0		
System	0.38	196 K	24 K	4		
Interrupts	0.38	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		1,060 K	424 K	412	Windows Session Manager	Microsoft Corporation
Memory Compression		456 K	8,152 K	2708		
csrss.exe		1,864 K	2,880 K	644	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,380 K	1,056 K	768	Windows Start-Up Application	Microsoft Corporation
services.exe		5,264 K	7,720 K	904	Services and Controller app	Microsoft Corporation
svchost.exe		9,892 K	15,944 K	600	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe	2.25	11,724 K	15,760 K	4012	WMI Provider Host	Microsoft Corporation
dllhost.exe		3,172 K	5,436 K	6972	COM Surrogate	Microsoft Corporation
StartMenuExperience...		30,516 K	37,316 K	7436		
RuntimeBroker.exe		5,804 K	6,976 K	8048	Runtime Broker	Microsoft Corporation
SearchApp.exe	Susp...	200,432 K	236,348 K	8308	Search application	Microsoft Corporation
RuntimeBroker.exe		11,744 K	29,648 K	8576	Runtime Broker	Microsoft Corporation
SettingSyncHost.exe		4,532 K	6,084 K	8908	Host Process for Setting Syn...	Microsoft Corporation
TextInputHost.exe		16,200 K	17,428 K	10136		Microsoft Corporation
dllhost.exe		5,500 K	7,796 K	6668	COM Surrogate	Microsoft Corporation
unsecapp.exe		1,732 K	3,328 K	11516	Sink to receive asynchronou...	Microsoft Corporation
RuntimeBroker.exe		5,924 K	19,800 K	3820	Runtime Broker	Microsoft Corporation
ApplicationFrameHost...		9,424 K	17,504 K	10604	Application Frame Host	Microsoft Corporation
HxOutlook.exe		114,796 K	154,856 K	10544	Microsoft Outlook	Microsoft Corporation
RuntimeBroker.exe		7,024 K	19,704 K	3256	Runtime Broker	Microsoft Corporation
HxTsr.exe		65,908 K	94,620 K	7300	Microsoft Outlook Communic...	Microsoft Corporation
CompPkgSrv.exe		2,068 K	4,888 K	11956	Component Package Suppor...	Microsoft Corporation
ShellExperienceHost....	Susp...	12,928 K	49,848 K	4812	Windows Shell Experience H...	Microsoft Corporation
WmiPrvSE.exe		2,648 K	9,404 K	8796	WMI Provider Host	Microsoft Corporation

Each process is assigned a specific color based on its type and state. We can use these colors to determine the process type. For example, "services" or "packed images."

Process Explorer's default configuration uses the following color scheme.

Path, Description, and Company Name

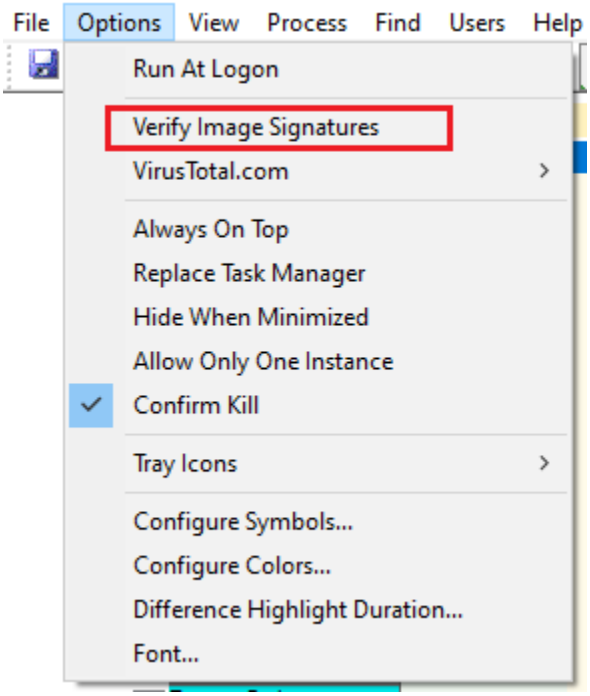
Most legitimate processes (except for system processes) will have a description and a company name. The absence of one or both should indicate suspicious behavior.

We can also see the path from which the process was launched. It's important to correlate the path and location with the name and the process itself. For example, a process named "DNS.EXE" running from the temp directory would probably not be a legitimate process.

Image Signature

Process explorer automatically provides a feature called "Verify Image Signatures," which can verify if an executable file or DLL used by a process has a trusted digital signature. Some malware developers will not bother to sign their code. Be on the lookup for unverified processes or DLLs.

The Verify Image Signatures option is not enabled by default. However, this option can be enabled on a process-by-process basis or globally via the "Options" menu.



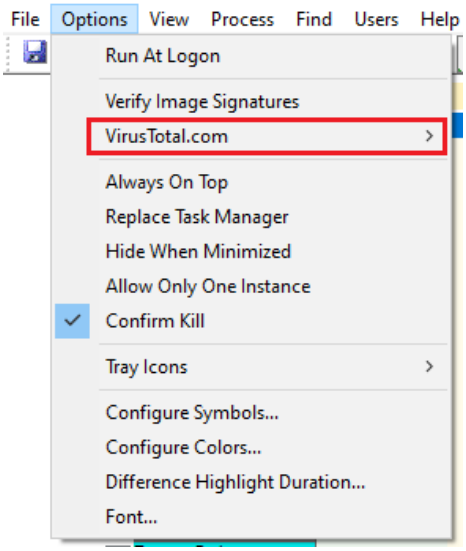
Virus Total

Process explorer integrates by default with Virus Total and can send the hashes of the executables and DLLs to check if any AV engines have flagged them.

For this feature to work, the machine being analyzed must have access to the internet. It is highly recommended that this feature be enabled as it can be of great help during analysis.

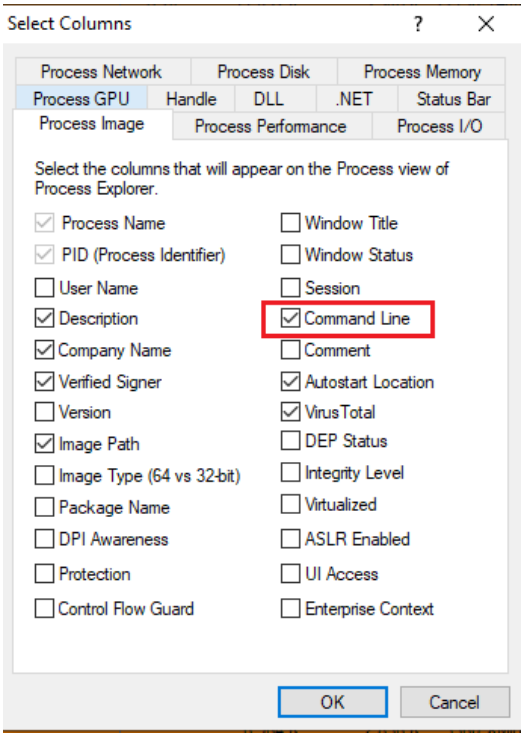
We can also submit unknown executables to VT for analysis if the scan result shows a status of unknown.

This feature is enabled via the "Options" menu.



Command Line

By default, Process Explorer doesn't show the command lines that launched a process. Adding the Command Line information can be enabled by selecting the "Select Columns" option from the "View" menu or by right-clicking on any column on the processes pane and selecting the "Select Columns" option.

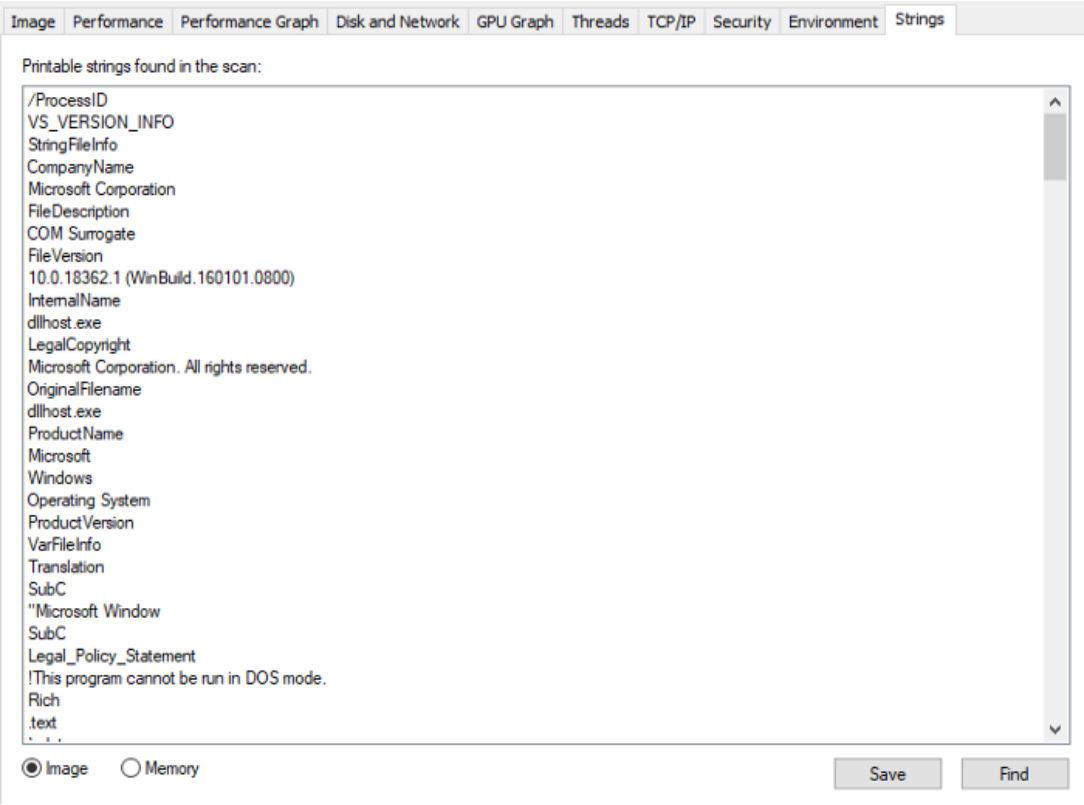


Identifying the command that launched a process can be very useful, especially if that malicious process contains arguments that we can use to determine the nature of the process.

When you start your analysis, you should add the Command Line to the Process Explorer display window.

Strings

Analyzing the strings of an executable has always been a powerful technique during static analysis, as they contain interesting indicators.



Process explorer lets us explore any process's strings by double-clicking on its name and navigating clicking the strings tab. We can inspect both on disk and in-memory strings (The in-memory strings only shows the part where the executable is mapped in memory), which in the case of packed or encrypted/encoded samples can sometimes be a gold mine of Indicators of Compromise (IOC).

Once we've determined that a process is malicious, we can look at its corresponding strings for further analysis.

TCP/IP

As the name suggests, this feature can quickly identify processes that have any active TCP connections (i.e., communicating via the network).

For example, if our initial indicator was a log showing communication between a machine and a C2 server and If the process is still communicating during our analysis, we can use this feature to locate it immediately.

DLLs

Process explorer lets us access any loaded DLL by pressing the "Ctrl+D" shortcut or selecting it from the results.

Name	Description	Company Name	Path	VirusTotal
nsi.dll	NSI User-mode interface DLL	Microsoft Corporation	C:\Windows\System32\nsi.dll	0/68
ntasn1.dll	Microsoft ASN.1 API	Microsoft Corporation	C:\Windows\System32\ntasn1.dll	0/64
ntdll.dll	NT Layer DLL	Microsoft Corporation	C:\Windows\System32\ntdll.dll	0/67

This can be combined with the Virus Total feature to submit the hashes of the DLL to check if the process is using a malicious file or an overview of the malware's possible capabilities.

Handles

When an application wants to access resources such as files or the registry, it must request them via the appropriate windows API responsible for handling the requested resource. Once this request is completed successfully, windows will allocate a handle and return its index in the process's handle table.

Process explorer lets us access all the open handles of a process by selecting a process and pressing "Ctrl+H."

Type	Name	Handle
Key	HKLM	0x00000000000000A4
Key	HKLM	0x00000000000000BC
Key	HKLM\SOFTWARE\Microsoft\Ole	0x00000000000000C0
Key	HKCU\Software\Classes\Local Settings\Software\Microsoft	0x00000000000000C8
Key	HKCU\Software\Classes\Local Settings	0x00000000000000CC
Key	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Options	0x0000000000000124
Key	HKCU\Software\Classes	0x0000000000000190
Key	HKCU\Software\Classes	0x00000000000001A4
Key	HKCU\Software\Classes	0x00000000000001AC
Key	HKCU\Software\Classes	0x00000000000001CC
Key	HKLM\SYSTEM\ControlSet001\Control\Session Manager	0x000000000000020C

This can be very helpful when analyzing malware dynamically and can help locate and identify IOC's and give us insight into its functionalities.

Summary –

In this lab, you learned how to detect the presence of malware on an infected Windows computer using Sysinternal's Process Explorer.

Process Explorer is a tool that lets us access a lot of information about processes running on a Windows machine, offering features we can leverage to analyze and determine if something is malicious.