Overview

This guide describes how to use Windows utilities to identify suspicious sample files and send them to the AVLab at Fortinet. The AVLab can further analyze the suspicious sample file, and provide you with the most appropriate solution.

When files are infected with ransomware, it is almost always impossible to reliably restore the affected files. After a device has been victim to a successful or undetected Zero Day infection or intrusion, it is highly recommended to restore the entire affected system from a clean backup. It is nearly impossible without proper forensic procedures to determine whether other components might have been installed during the breach because successfully executed malware can download and install additional components from a remote site.

It is highly recommend to obtain the third-party tools referenced in this guide from the Microsoft Sysinternals site at https://docs.microsoft.com/en-us/sysinternals/.

The third-party tools referenced in this guide have been tested on a device running a Windows 10 operating system.

This guide contains the following topics:

Installing and using Process Explorer to locate suspicious files

You can use the Process Explorer utility to view currently running processes on a host. Process Explorer is similar to Task Manager, but provides more detail about the current running process.

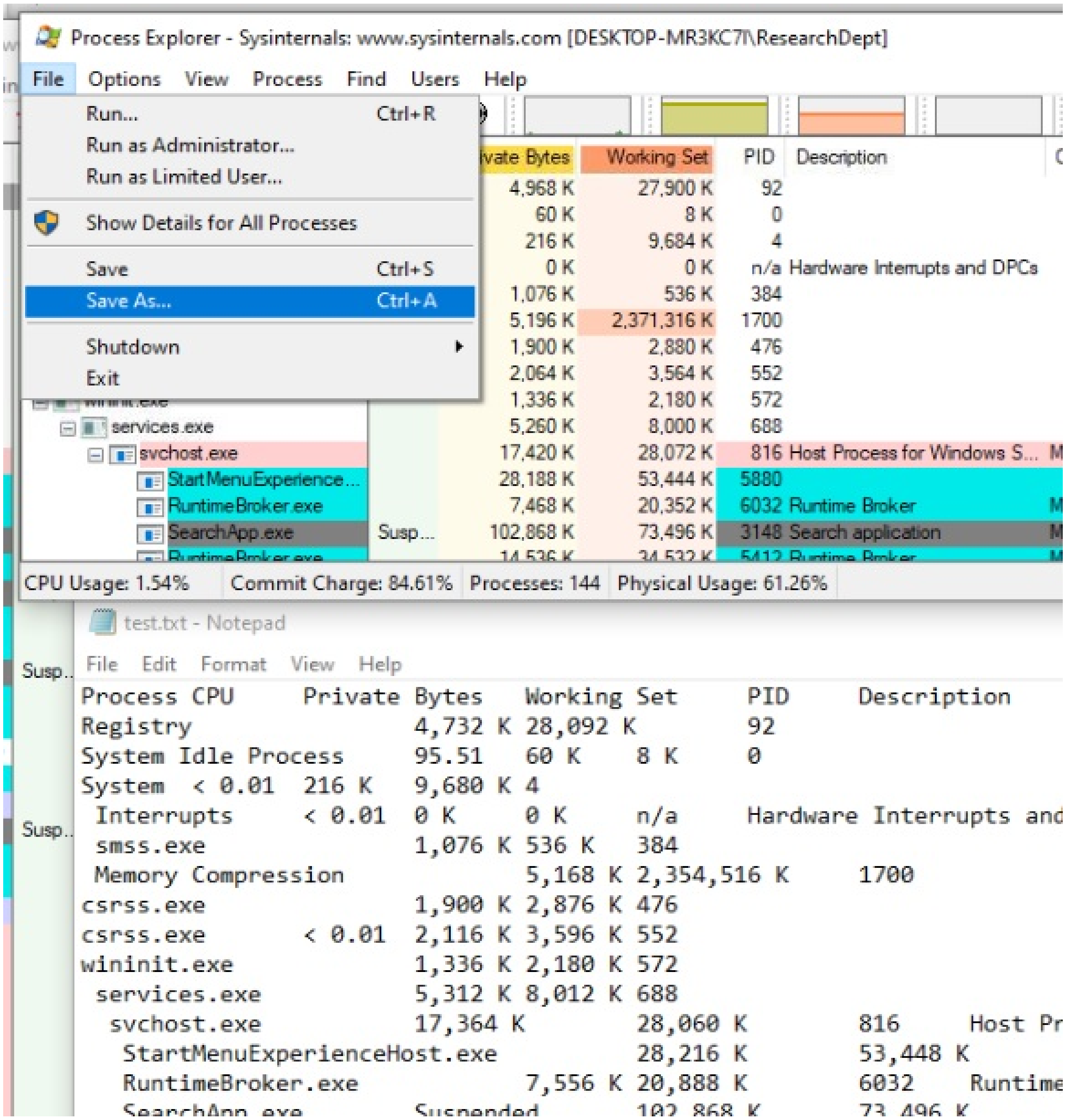
Process Explorer can be used to search for and locate suspicious files. A suspicious process can be any processes that are unfamiliar to you or your system administrator. The process name often indicates the name of the running application. You can consider any unfamiliar processes or applications suspicious.

To install Process Explorer:

1. Download the Process Explorer utility from Microsoft at https://docs.microsoft.com/en-us/sysinternals/downloads/process-explorer.
2. Install Process Explorer.

To use Process Explorer:

1. Open the Process Explorer utility, and search for suspicious processes.
2. If you cannot determine whether processes are suspicious, save the list of processes to a text file, and send the file to the AVLab:
   a. In Process Explorer, select *File* > *Save As*, and save the file as a *.txt* file.



```
vate Bytes   Working Set   PID   Description
   4,968 K      27,900 K    92
      60 K           8 K     0
     216 K       9,684 K     4
       0 K           0 K   n/a   Hardware Interrupts and DPCs
   1,076 K         536 K   384
   5,196 K   2,371,316 K  1700
   1,900 K       2,880 K   476
   2,064 K       3,564 K   552
   1,336 K       2,180 K   572
services.exe                       5,260 K      8,000 K   688
svchost.exe                       17,420 K     28,072 K   816 Host Process for Windows S...  M
StartMenuExperience...            28,188 K     53,444 K  5880
RuntimeBroker.exe                  7,468 K     20,352 K  6032 Runtime Broker                 M
SearchApp.exe            Susp...  102,868 K    73,496 K  3148 Search application             M
RuntimeBroker.exe                 14,536 K     34,532 K  5412 Runtime Broker                 M
```

CPU Usage: 1.54% | Commit Charge: 84.61% | Processes: 144 | Physical Usage: 61.26%

```
Process CPU     Private Bytes    Working Set     PID     Description
Registry                4,732 K 28,092 K        92
System Idle Process     95.51   60 K    8 K     0
System  < 0.01  216 K   9,680 K 4
 Interrupts     < 0.01  0 K     0 K     n/a     Hardware Interrupts and
 smss.exe               1,076 K 536 K   384
 Memory Compression             5,168 K 2,354,516 K     1700
csrss.exe               1,900 K 2,876 K 476
csrss.exe       < 0.01  2,116 K 3,596 K 552
wininit.exe             1,336 K 2,180 K 572
 services.exe           5,312 K 8,012 K 688
  svchost.exe           17,364 K        28,060 K        816     Host Pr
   StartMenuExperienceHost.exe          28,216 K        53,448 K
   RuntimeBroker.exe            7,556 K 20,888 K        6032    Runtime
   SearchApp.exe        Suspended       102,868 K       73,496 K
```

   b. Attach the log text file to the FortiCare ticket.
   c. Skip the last step in this procedure.
3. If you locate a suspicious process, use the Process Monitor utility to further analyze the file. See Installing and using Process Monitor to locate suspicious files on page 3.

Installing and using Process Monitor to locate suspicious files

You can use the Process Monitor utility to monitor in any registry, process, or thread activity in real-time.

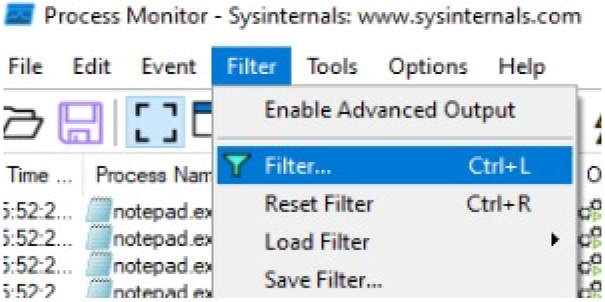
If you locate a potentially suspicious process by using the Process Explorer utility, you can use the Process Monitor utility to further analyzer the suspicious process.

To install Process Monitor:

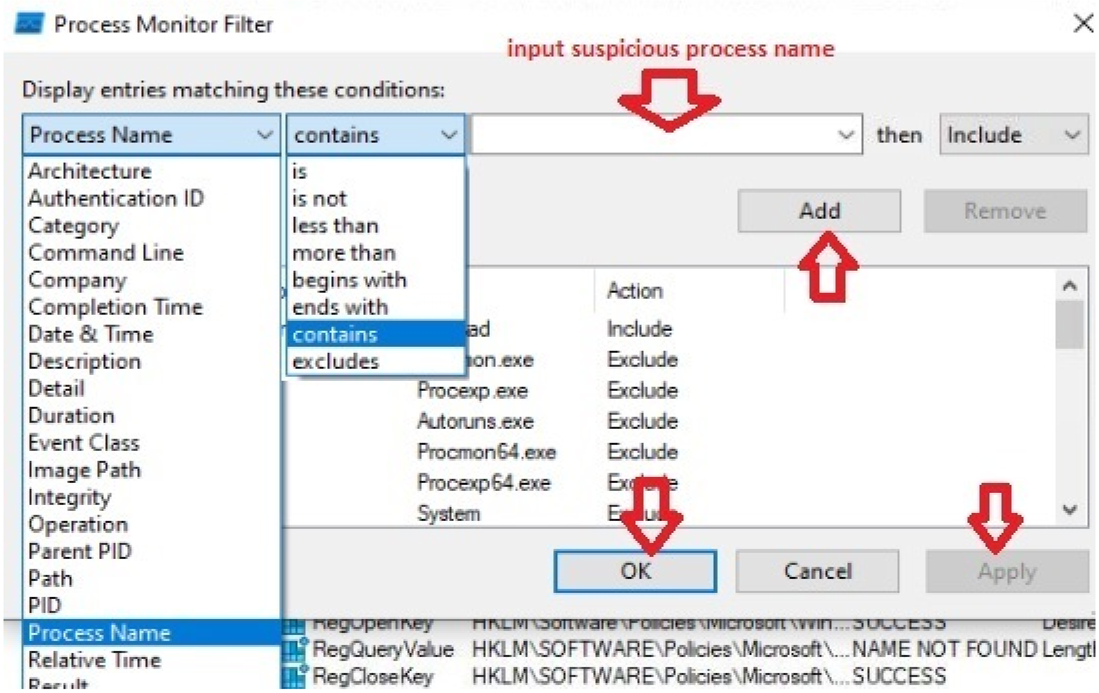
1. Download the Process Monitor utility from Microsoft at https://docs.microsoft.com/en-us/sysinternals/downloads/procmon.
2. Install Process Monitor.

To use Process Monitor:

1. Open the Process Monitor utility.
2. Go to *Filter* > *Filter*.



3. Monitor a process:
   a. Select *Process Name*, *contains*, and then type the name of suspicious process.
   b. Click *Add*, *Apply*, and *OK*.



Results for the process are displayed.

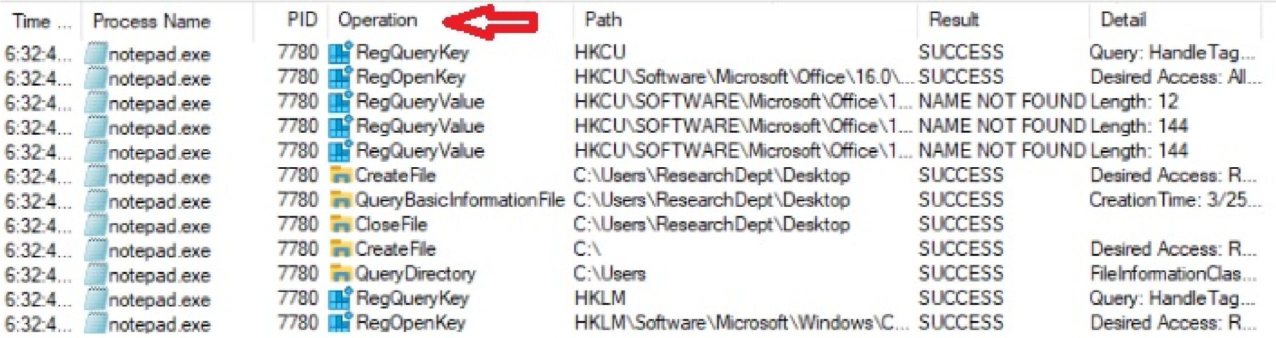
4. Review the process results:

   You can check the API functions being used by the suspicious process. Depending on the type of malware, various samples may indicate various suspicious API calls.

   Common calls that might be considered suspicious include:

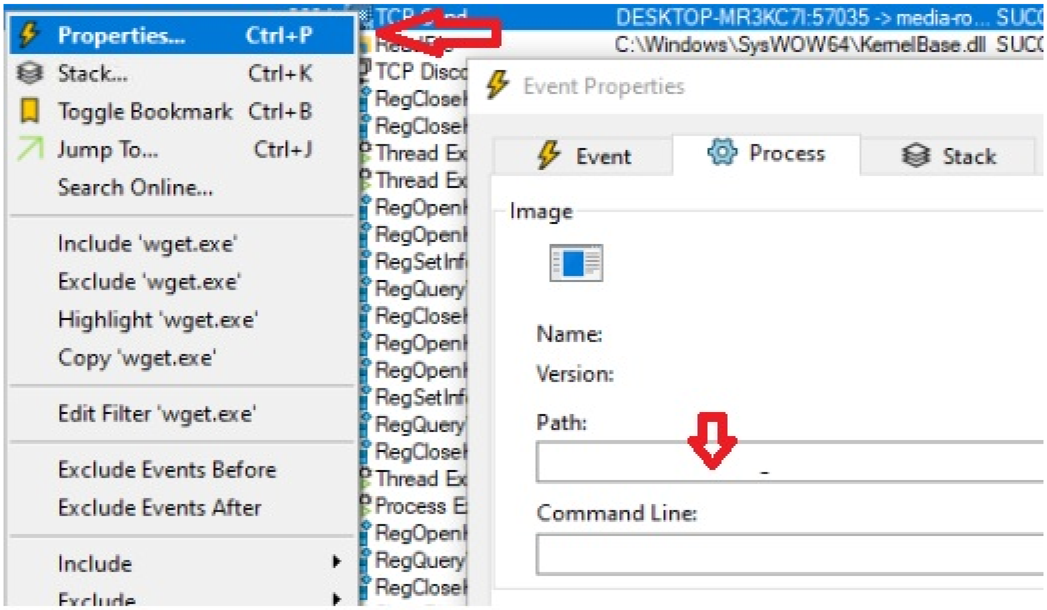
   - Unpack/Decrypt - VirtualAlloc VirtualProtect RtlMoveMemory
   - Ransomware - GetLogicalDrives GetDriveType FindFirstFile FindNextFile EncryptFile
   - Virus Infector - WriteFile SetFilePointer CreateFileMapping
   - Process Injector - GetTempPath CreateFile CopyFile
   - Backdoor - ReadFile WinHttpOpen

   In the following example, the *Operation* column displays example processes for a test sample notepad application.



Time ...	Process Name	PID	Operation	Path	Result	Detail
6:32:4...	notepad.exe	7780	RegQueryKey	HKCU	SUCCESS	Query: HandleTag...
6:32:4...	notepad.exe	7780	RegOpenKey	HKCU\Software\Microsoft\Office\16.0\...	SUCCESS	Desired Access: All...
6:32:4...	notepad.exe	7780	RegQueryValue	HKCU\SOFTWARE\Microsoft\Office\1...	NAME NOT FOUND	Length: 12
6:32:4...	notepad.exe	7780	RegQueryValue	HKCU\SOFTWARE\Microsoft\Office\1...	NAME NOT FOUND	Length: 144
6:32:4...	notepad.exe	7780	RegQueryValue	HKCU\SOFTWARE\Microsoft\Office\1...	NAME NOT FOUND	Length: 144
6:32:4...	notepad.exe	7780	CreateFile	C:\Users\ResearchDept\Desktop	SUCCESS	Desired Access: R...
6:32:4...	notepad.exe	7780	QueryBasicInformationFile	C:\Users\ResearchDept\Desktop	SUCCESS	CreationTime: 3/25...
6:32:4...	notepad.exe	7780	CloseFile	C:\Users\ResearchDept\Desktop	SUCCESS	
6:32:4...	notepad.exe	7780	CreateFile	C:\	SUCCESS	Desired Access: R...
6:32:4...	notepad.exe	7780	QueryDirectory	C:\Users	SUCCESS	FileInformationClas...
6:32:4...	notepad.exe	7780	RegQueryKey	HKLM	SUCCESS	Query: HandleTag...
6:32:4...	notepad.exe	7780	RegOpenKey	HKLM\Software\Microsoft\Windows\C...	SUCCESS	Desired Access: R...

5. Once you have confirmed the suspicious process, right-click the process, and select *Properties* to view the *File Path*.



6. Note the file path, and use Windows Explorer to locate the suspicious file.
7. In Windows Explorer, add the suspicious file to a ZIP archive with the password: *infected*.
8. Attach the ZIP archive to the FortiCare ticket for the FortiCare team to analyze, or email to submitvirus@fortinet.com.

Installing and using Autoruns to locate suspicious files

You can use the Autoruns utility to view all applications or programs within the host that automatically start.

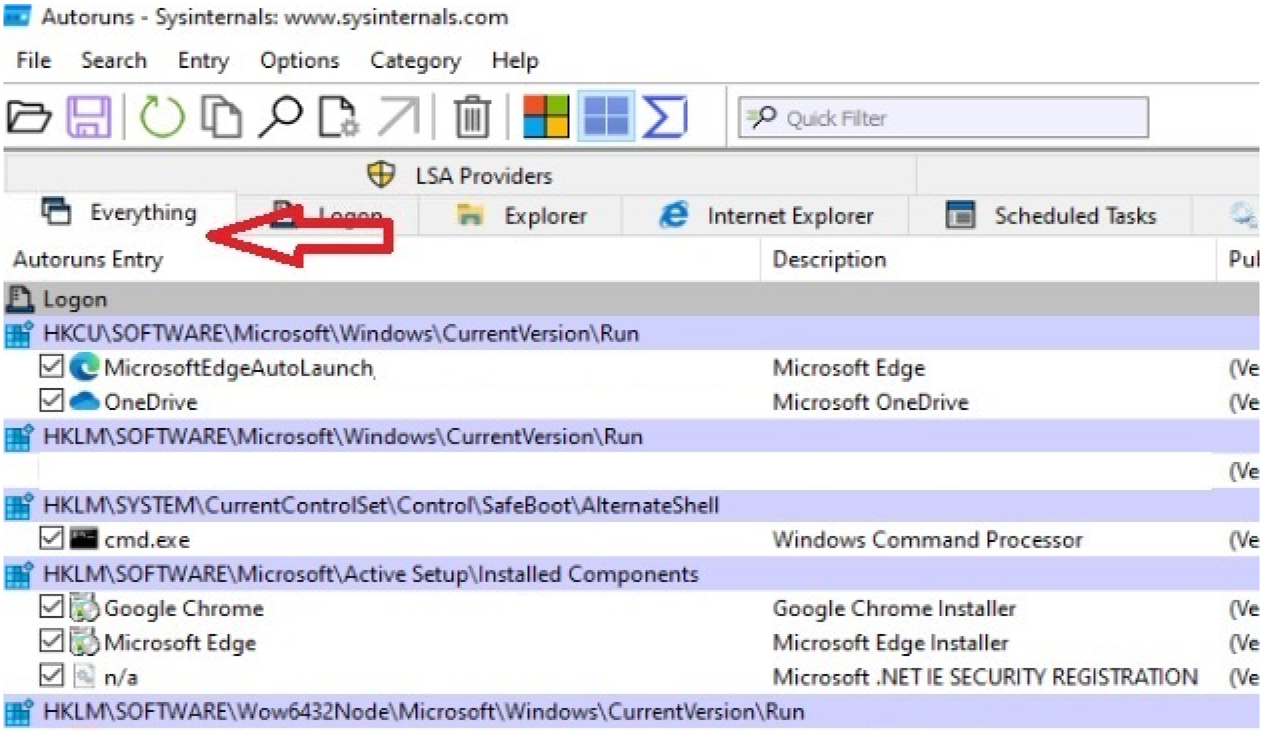
An application or program that uses the autorun feature isn't necessarily suspicious. Some clean or legitimate applications or programs can employ autorun. Nonetheless malware uses the autorun feature to ensure persistence upon system reboot.

To install Autoruns:

1. Download Autoruns from Microsoft at https://docs.microsoft.com/en-us/sysinternals/downloads/autoruns.
2. Install Autoruns.

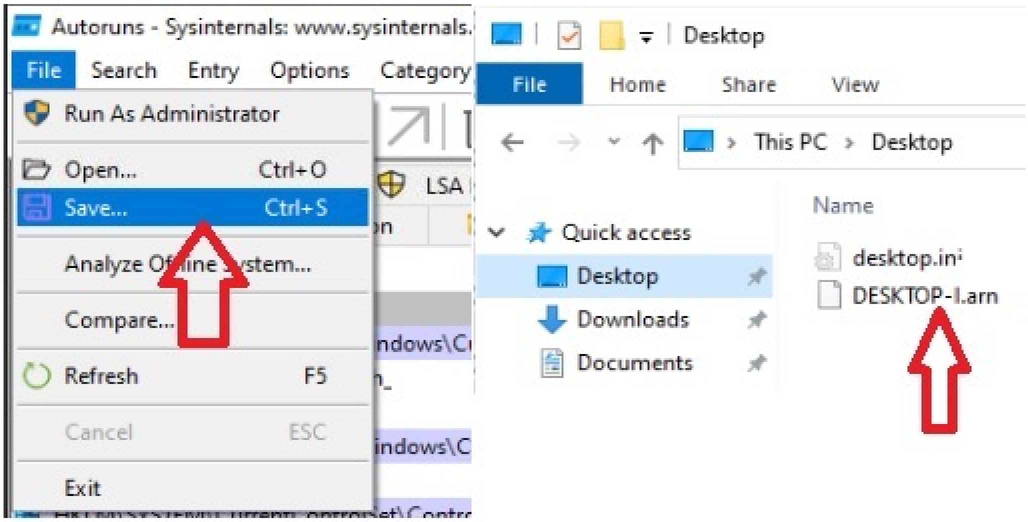
To use Autoruns to locate suspicious files:

1. Open the Autoruns utility, and go to the *Everything* tab to view the *Autoruns Entry* list.


Autoruns - Sysinternals: www.sysinternals.com
File Search Entry Options Category Help
Quick Filter
LSA Providers
Everything
Logon
Explorer
Internet Explorer
Scheduled Tasks

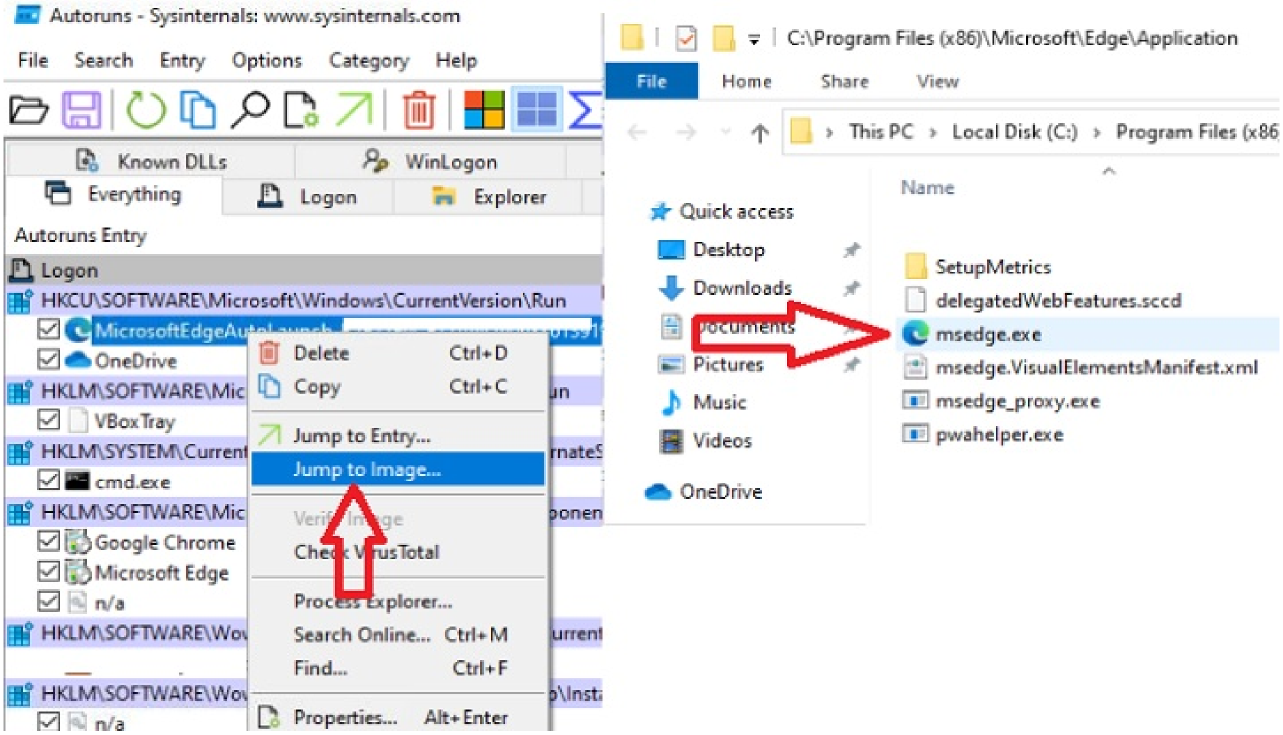
Autoruns Entry	Description	Pul
Logon		
HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
☑ MicrosoftEdgeAutoLaunch_	Microsoft Edge	(Ve
☑ OneDrive	Microsoft OneDrive	(Ve
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run		
		(Ve
HKLM\SYSTEM\CurrentControlSet\Control\SafeBoot\AlternateShell		
☑ cmd.exe	Windows Command Processor	(Ve
HKLM\SOFTWARE\Microsoft\Active Setup\Installed Components		
☑ Google Chrome	Google Chrome Installer	(Ve
☑ Microsoft Edge	Microsoft Edge Installer	(Ve
☑ n/a	Microsoft .NET IE SECURITY REGISTRATION	(Ve
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run		

2. Search for any unusual, suspicious entries in the *Autoruns Entry* list.
   A suspicious autorun entry can be any unfamiliar or unknown application or program that you or your system administrator may not be aware of. Usually the entry in the list indicates the name of the application currently running.
3. If you cannot determine a suspicious entry in the *Autoruns Entry* list, save an Autoruns file:
   a. Go to *File* > *Save*.
      Autorun generates and saves a file with an *.arn* extension. The following example shows the *DESKTOP-I.arn* file:



   b. Attach the log text file to the FortiCare ticket.
   c. Skip the remaining steps in the procedure.

4. If you locate a suspicious entry in the *Autoruns Entry* list, right click the process, and select *Jump to Image..* to go to the file location.
   The following example shows how to use the *Autoruns Entry* list to locate a sample test file for Microsoft Edge.



5. In Windows Explorer, add the suspicious file to a ZIP archive with the password: *infected*.
6. Attach the ZIP archive to the FortiCare ticket for the FortiCare team to analyze, or email to submitvirus@fortinet.com.

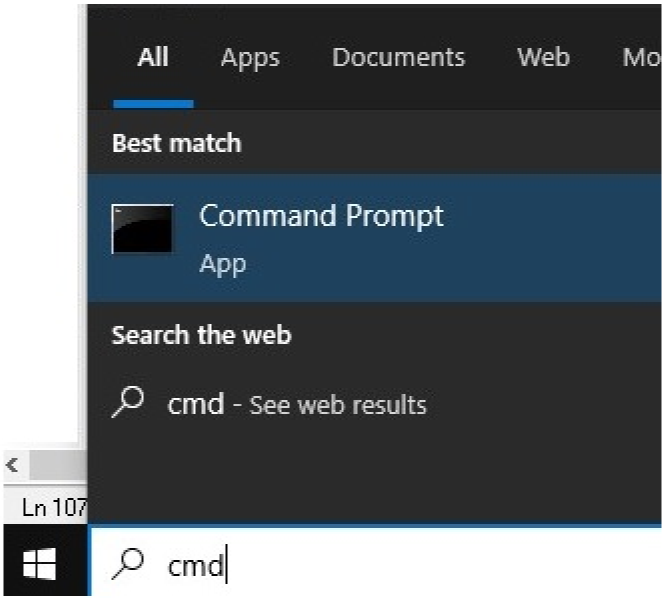
Revealing hidden, suspicious files

Sometimes suspicious files are hidden from view in Windows Explorer. You can use this procedure to display hidden files.

This procedure presumes that you have already identified the suspicious file or process.

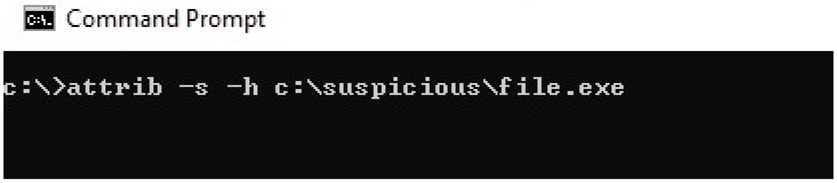
To reveal hidden, suspicious files:

1. Press `Win+R`, type *cmd*, and press `Enter`.



   The *Command Prompt* window is displayed.

2. At the prompt, enter `attrib -s -h` followed by the `<File_Path_of_Suspicious_File>`, and press `Enter`. For example, enter `attrib -s -h C:\suspicious\file.exe`.



```
c:\>attrib -s -h c:\suspicious\file.exe
```

   The file is unhidden.

3. In Windows Explorer, add the suspicious file to a ZIP archive with the password: *infected*.
4. Attach the ZIP archive to the FortiCare ticket for the FortiCare team to analyze, or email to submitvirus@fortinet.com.

Ending tasks or killing running processes to enable copying of suspicious files

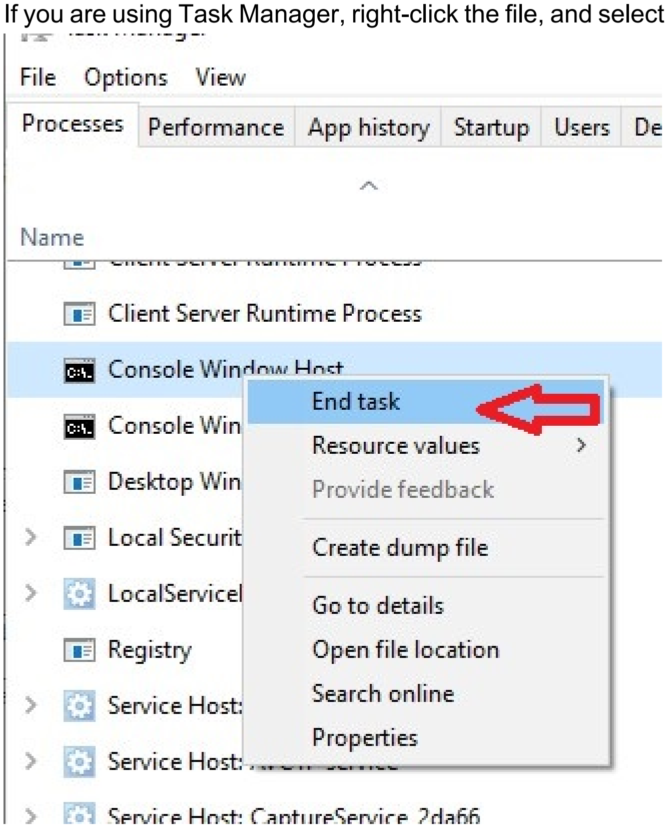
When the suspicious sample file is locked by a running process, you cannot obtain the file. This topic describes how to use the following tools to end the task or kill the running process, so you can copy the file.

- Windows Task Manager
- Process Explorer
- Resource Monitor

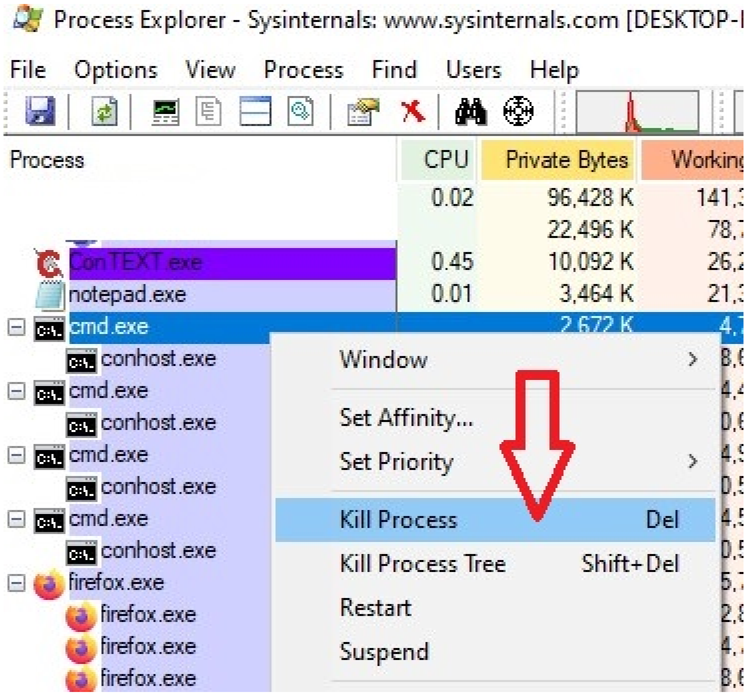
This procedure presumes that you have already identified the suspicious file or process.

To end tasks or kill running processes:

1. Open Task Manager or Process Explorer.
2. In the list, search for the process that is using the file.
3. End or kill the process:
   - If you are using Task Manager, right-click the file, and select *End Task*.

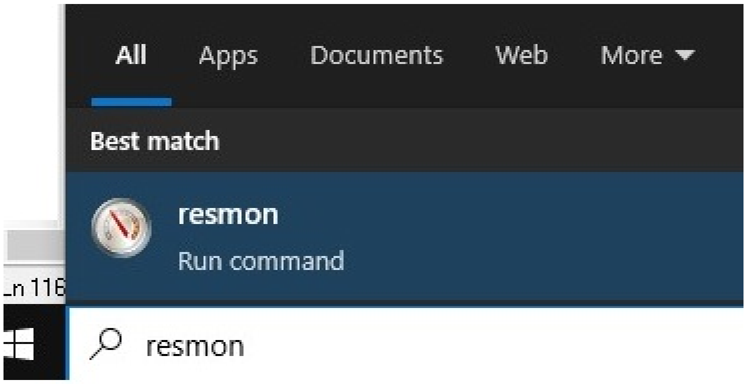


- If you are using Process Explorer, right-click the file and select *Kill Process*.


Process Explorer - Sysinternals: www.sysinternals.com [DESKTOP-I
File Options View Process Find Users Help
Window
Set Affinity...
Set Priority
Kill Process Del
Kill Process Tree Shift+Del
Restart
Suspend

Process	CPU	Private Bytes	Working
	0.02	96,428 K	141,3
		22,496 K	78,7
ConTEXT.exe	0.45	10,092 K	26,2
notepad.exe	0.01	3,464 K	21,3
cmd.exe		2,672 K	4,7
conhost.exe			8,6
cmd.exe			4,4
conhost.exe			0,6
cmd.exe			4,9
conhost.exe			0,5
cmd.exe			4,5
conhost.exe			0,5
firefox.exe			5,7
firefox.exe			2,8
firefox.exe			4,7
firefox.exe			8,6

4. If you cannot find the suspicious process by using Windows Task Manager or Process Explorer, try using Resource Monitor:
   a. Press `Win+R`, enter *resmon*, and press `Enter` to open Resource Monitor.

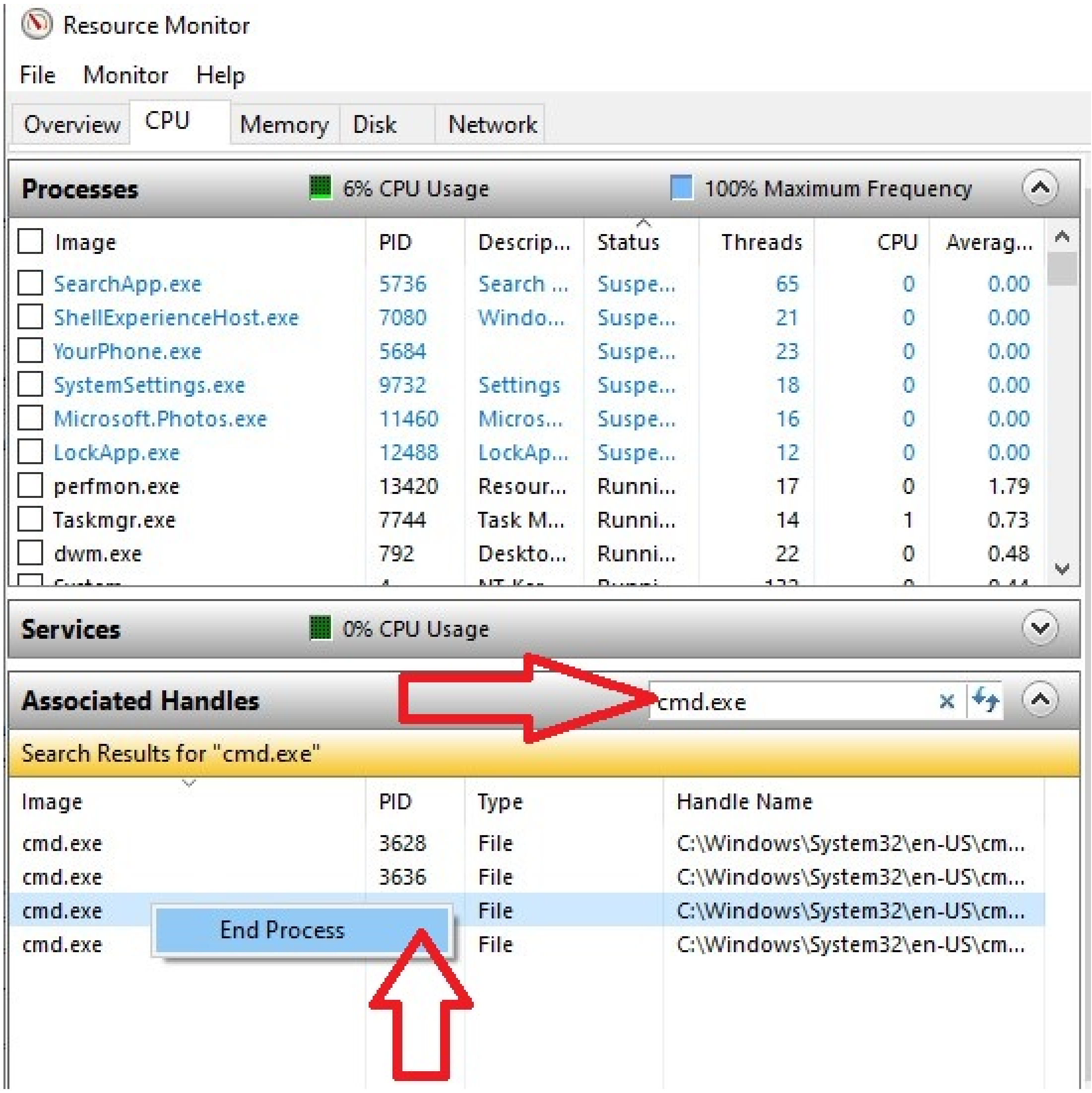


   The Resource Monitor window is displayed.

   b. Go to the *CPU* tab.

   c. In the *Associated Handles* section, enter the filename in the *Search* box, and press `Enter`.
   The process is displayed.

   d. In the *Search Results* list, right-click the process, and select *End Process*.
   In the following example, a process called *cmd.exe* is ended.



Processes 🟩 6% CPU Usage 🟦 100% Maximum Frequency

□ Image	PID	Descrip...	Status	Threads	CPU	Averag...
□ SearchApp.exe	5736	Search ...	Suspe...	65	0	0.00
□ ShellExperienceHost.exe	7080	Windo...	Suspe...	21	0	0.00
□ YourPhone.exe	5684		Suspe...	23	0	0.00
□ SystemSettings.exe	9732	Settings	Suspe...	18	0	0.00
□ Microsoft.Photos.exe	11460	Micros...	Suspe...	16	0	0.00
□ LockApp.exe	12488	LockAp...	Suspe...	12	0	0.00
□ perfmon.exe	13420	Resour...	Runni...	17	0	1.79
□ Taskmgr.exe	7744	Task M...	Runni...	14	1	0.73
□ dwm.exe	792	Deskto...	Runni...	22	0	0.48

Services 🟩 0% CPU Usage

Associated Handles cmd.exe

Search Results for "cmd.exe"

Image	PID	Type	Handle Name
cmd.exe	3628	File	C:\Windows\System32\en-US\cm...
cmd.exe	3636	File	C:\Windows\System32\en-US\cm...
cmd.exe		File	C:\Windows\System32\en-US\cm...
cmd.exe		File	C:\Windows\System32\en-US\cm...

5. In Windows Explorer, add the suspicious file to a ZIP archive with the password: *infected*.
6. Attach the ZIP archive to the FortiCare ticket for the FortiCare team to analyze, or email to submitvirus@fortinet.com.

Change Log

Date	Change Description
2022-05-26	Initial release.