Malware Analysis

If you were to inspect several malware samples in the wild, a typical pattern arises, making analysing other samples easier with experience. Knowing these common behaviours gives us an idea of what to look for on the defensive side, such as:

- **Network connections** - Malware tends to establish either external network connections or internal connections. External connections allow remote access or for downloading staged payloads from a threat actors' infrastructure. Meanwhile, internal connections allow for lateral movement, a technique used to extend access to other hosts or applications within the network.

- **Registry key modifications** - Malware typically uses registry keys to establish persistence, a technique used by threat actors to discreetly maintain long-term access to a system despite disruptions. A good example is Registry Run Keys, which allows binaries to be automatically executed when a user logs in or the machine boots up.

- **File manipulations** - Malware also tends to download (one of the common reasons to establish network connections) or create new files needed for its successful execution.

Given this knowledge, we can expect the possible behaviour of malware during an investigation.

===

Two methods of malware analysis:

1) Static Analysis

Static Analysis is a way of analysing a malware sample without executing the code. This method mainly focuses on profiling the binary with its readable information, such as its properties, program flow and strings. Given the limitation of not executing it, sometimes this method gives insufficient information, which is why we resort to Dynamic Analysis.

Profiling Executables through Static Analysis:

We can use a tool called Detect It Easy and a tool called CAPA to conduct static analysis.

1. **Detect It Easy (DIE)**

This tool provides information about the file, such as its architecture, significant headers, packer used, and strings. In this task, we will only utilise the basic functionalities of Detect It Easy to gain the basic information needed to analyse the binary. If you want to learn more about this tool, you may refer to this link.

Upon opening, we will immediately discover the binary's architecture, and the executable packer used.
Packing malware is a common technique used by malware developers to compress, obfuscate or encrypt the binary. With this, contents such as significant strings and headers will not be immediately visible to Static Analysis Tools.

You may test this information by doing the following:
- View the strings from Detect It Easy, which shows an overwhelming number of strings that are not that significant for investigation.
- Note: Strings are pieces of text inside a binary, often containing information such as IP addresses, URLs, or file names used by the malicious program.

----

2. **CAPA**

CAPA detects capabilities in executable files. May it be for the installation of a service, invocation of network connections, registry modifications and such.

----

2) Dynamic Analysis

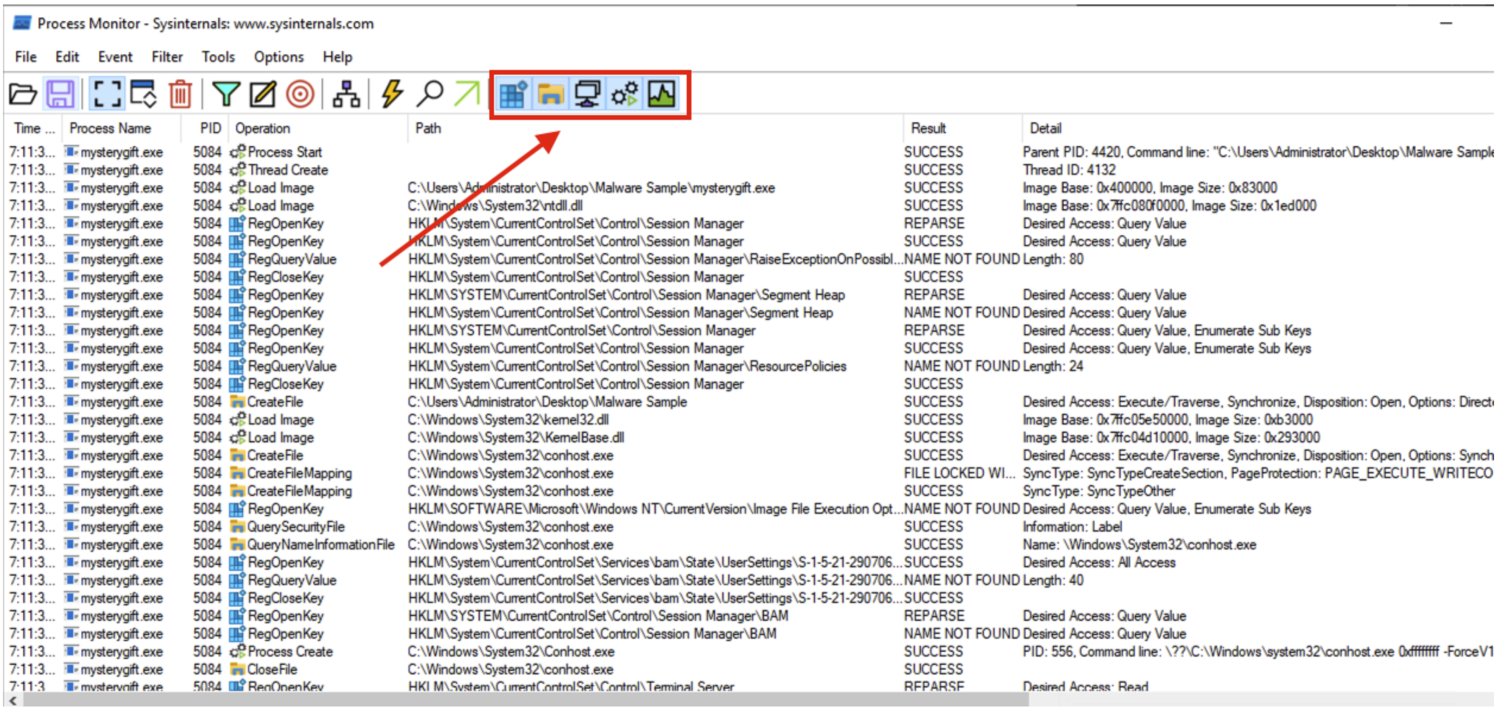
Dynamic Analysis mainly focuses on understanding the malware by executing it in a safe environment, such as a Sandbox. By doing this, you will see the malware live in action, its exact behaviour, and how it infects the environment.

Deep-dive into Dynamic Malware Analysis:

ProcMon, or Process Monitor, is a Windows tool that shows real-time registry, file system, and process/thread activity. You can learn more about it here.

ProcMon has a panel that can filter the following, as highlighted in the image below (in sequence):

- Show Registry Activity
- Show File System Activity
- Show Network Activity
- Show Process and Thread Activity
- Show Profiling Events



Time ...	Process Name	PID	Operation	Path	Result	Detail
7:11:3...	mysterygift.exe	5084	Process Start		SUCCESS	Parent PID: 4420, Command line: "C:\Users\Administrator\Desktop\Malware Sample
7:11:3...	mysterygift.exe	5084	Thread Create		SUCCESS	Thread ID: 4132
7:11:3...	mysterygift.exe	5084	Load Image	C:\Users\Administrator\Desktop\Malware Sample\mysterygift.exe	SUCCESS	Image Base: 0x400000, Image Size: 0x83000
7:11:3...	mysterygift.exe	5084	Load Image	C:\Windows\System32\ntdll.dll	SUCCESS	Image Base: 0x7ffc080f0000, Image Size: 0x1ed000
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
7:11:3...	mysterygift.exe	5084	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\RaiseExceptionOnPossibl...	NAME NOT FOUND	Length: 80
7:11:3...	mysterygift.exe	5084	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Segment Heap	REPARSE	Desired Access: Query Value
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\Segment Heap	NAME NOT FOUND	Desired Access: Query Value
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager	REPARSE	Desired Access: Query Value, Enumerate Sub Keys
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value, Enumerate Sub Keys
7:11:3...	mysterygift.exe	5084	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\ResourcePolicies	NAME NOT FOUND	Length: 24
7:11:3...	mysterygift.exe	5084	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
7:11:3...	mysterygift.exe	5084	CreateFile	C:\Users\Administrator\Desktop\Malware Sample	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Direct
7:11:3...	mysterygift.exe	5084	Load Image	C:\Windows\System32\kernel32.dll	SUCCESS	Image Base: 0x7ffc05e50000, Image Size: 0xb3000
7:11:3...	mysterygift.exe	5084	Load Image	C:\Windows\System32\KernelBase.dll	SUCCESS	Image Base: 0x7ffc04d10000, Image Size: 0x293000
7:11:3...	mysterygift.exe	5084	CreateFile	C:\Windows\System32\conhost.exe	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Disposition: Open, Options: Synch
7:11:3...	mysterygift.exe	5084	CreateFileMapping	C:\Windows\System32\conhost.exe	FILE LOCKED WI...	SyncType: SyncTypeCreateSection, PageProtection: PAGE_EXECUTE_WRITECO
7:11:3...	mysterygift.exe	5084	CreateFileMapping	C:\Windows\System32\conhost.exe	SUCCESS	SyncType: SyncTypeOther
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Image File Execution Opt...	NAME NOT FOUND	Desired Access: Query Value, Enumerate Sub Keys
7:11:3...	mysterygift.exe	5084	QuerySecurityFile	C:\Windows\System32\conhost.exe	SUCCESS	Information: Label
7:11:3...	mysterygift.exe	5084	QueryNameInformationFile	C:\Windows\System32\conhost.exe	SUCCESS	Name: \Windows\System32\conhost.exe
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-290706...	SUCCESS	Desired Access: All Access
7:11:3...	mysterygift.exe	5084	RegQueryValue	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-290706...	NAME NOT FOUND	Length: 40
7:11:3...	mysterygift.exe	5084	RegCloseKey	HKLM\System\CurrentControlSet\Services\bam\State\UserSettings\S-1-5-21-290706...	SUCCESS	
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\BAM	REPARSE	Desired Access: Query Value
7:11:3...	mysterygift.exe	5084	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager\BAM	NAME NOT FOUND	Desired Access: Query Value
7:11:3...	mysterygift.exe	5084	Process Create	C:\Windows\System32\Conhost.exe	SUCCESS	PID: 556, Command line: \??\C:\Windows\system32\conhost.exe 0xffffffff -ForceV1
7:11:3...	mysterygift.exe	5084	CloseFile	C:\Windows\System32\conhost.exe	SUCCESS	
7:11:3	mysterygift.exe	5084	RegOpenKey	HKLM\System\CurrentControlSet\Control\Terminal Server	REPARSE	Desired Access: Read

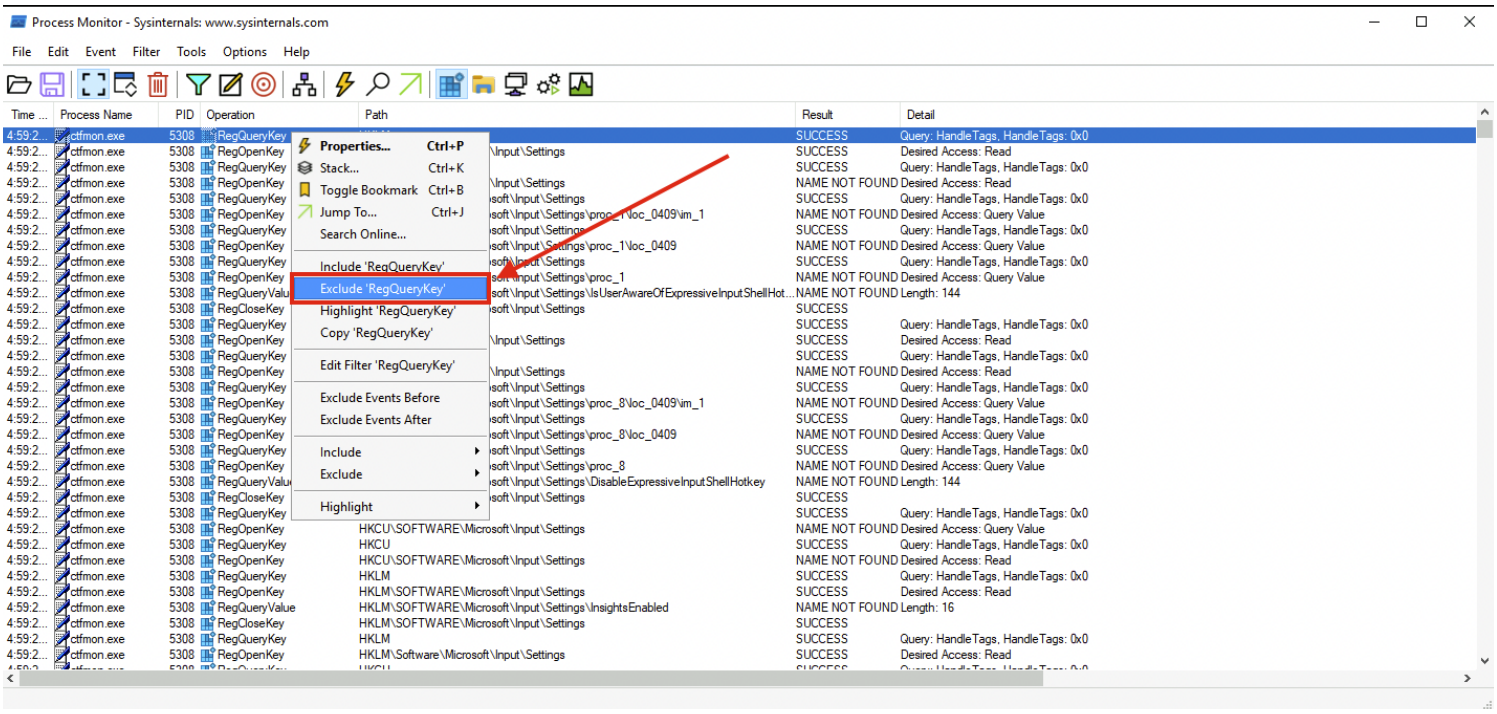
With these filters, we will focus on the first three; Registry, File System and Network. As discussed above, malware tends to do the following; **Registry Modification**, **File Modification and Network Connections**. Let's start investigating them one by one.

----

1. *Registry Modification*

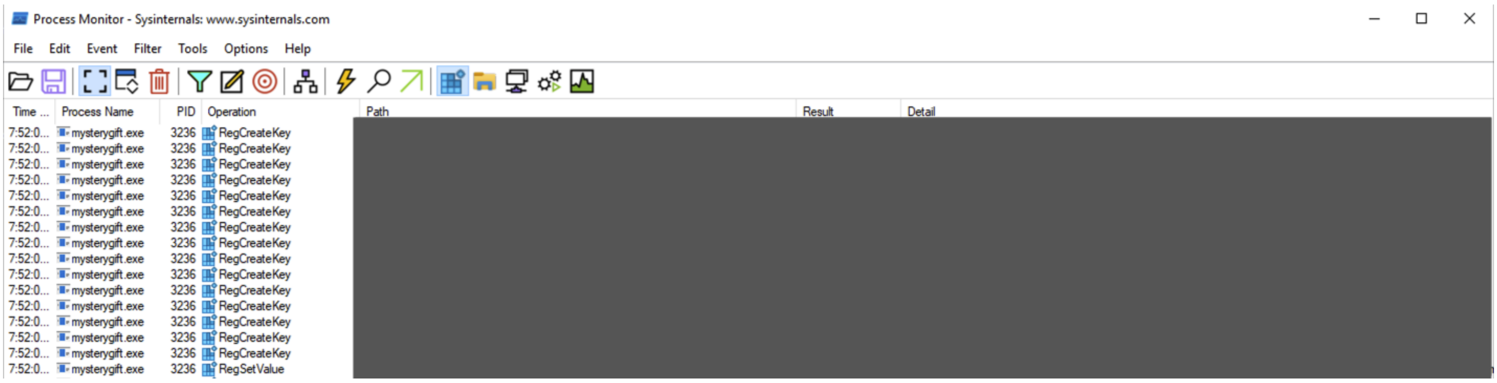
First, we want to determine if any significant Registry Modifications are executed by the binary, which is one of the expected behaviours introduced in this task.
To do this, unclick all filters and only choose **Show Registry Activity**. The results still give several results so let's add a filter by finding all Registry Key Creations and Modifications. Remove the following Operations by right-clicking an entry from the Operation column and choosing **Exclude '<operation (e.g. RegQueryKey)>'** similar to the image below:
Exclude these 4:

- RegOpenKey
- RegQueryValue
- RegQueryKey
- RegCloseKey



Time ...	Process Name	PID	Operation	Path	Result	Detail
4:59:2...	ctfmon.exe	5308	RegQueryKey		SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	\Input\Settings	SUCCESS	Desired Access: Read
4:59:2...	ctfmon.exe	5308	RegQueryKey		SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	\Input\Settings	NAME NOT FOUND	Desired Access: Read
4:59:2...	ctfmon.exe	5308	RegQueryKey	soft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	soft\Input\Settings\proc_1\loc_0409\im_1	NAME NOT FOUND	Desired Access: Query Value
4:59:2...	ctfmon.exe	5308	RegQueryKey	soft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	soft\Input\Settings\proc_1\loc_0409	NAME NOT FOUND	Desired Access: Query Value
4:59:2...	ctfmon.exe	5308	RegQueryKey	soft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	soft\Input\Settings\proc_1	NAME NOT FOUND	Desired Access: Query Value
4:59:2...	ctfmon.exe	5308	RegQueryValu	soft\Input\Settings\IsUserAwareOfExpressiveInputShellHot...	NAME NOT FOUND	Length: 144
4:59:2...	ctfmon.exe	5308	RegCloseKey	soft\Input\Settings	SUCCESS	
4:59:2...	ctfmon.exe	5308	RegQueryKey		SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	\Input\Settings	SUCCESS	Desired Access: Read
4:59:2...	ctfmon.exe	5308	RegQueryKey		SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	\Input\Settings	NAME NOT FOUND	Desired Access: Read
4:59:2...	ctfmon.exe	5308	RegQueryKey	soft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	soft\Input\Settings\proc_8\loc_0409\im_1	NAME NOT FOUND	Desired Access: Query Value
4:59:2...	ctfmon.exe	5308	RegQueryKey	soft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	soft\Input\Settings\proc_8\loc_0409	NAME NOT FOUND	Desired Access: Query Value
4:59:2...	ctfmon.exe	5308	RegQueryKey	soft\Input\Settings	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	soft\Input\Settings\proc_8	NAME NOT FOUND	Desired Access: Query Value
4:59:2...	ctfmon.exe	5308	RegQueryValu	soft\Input\Settings\DisableExpressiveInputShellHotkey	NAME NOT FOUND	Length: 144
4:59:2...	ctfmon.exe	5308	RegCloseKey	soft\Input\Settings	SUCCESS	
4:59:2...	ctfmon.exe	5308	RegQueryKey		SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Query Value
4:59:2...	ctfmon.exe	5308	RegQueryKey	HKCU	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	HKCU\SOFTWARE\Microsoft\Input\Settings	NAME NOT FOUND	Desired Access: Read
4:59:2...	ctfmon.exe	5308	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS	Desired Access: Read
4:59:2...	ctfmon.exe	5308	RegQueryValue	HKLM\SOFTWARE\Microsoft\Input\Settings\InsightsEnabled	NAME NOT FOUND	Length: 16
4:59:2...	ctfmon.exe	5308	RegCloseKey	HKLM\SOFTWARE\Microsoft\Input\Settings	SUCCESS	
4:59:2...	ctfmon.exe	5308	RegQueryKey	HKLM	SUCCESS	Query: HandleTags, HandleTags: 0x0
4:59:2...	ctfmon.exe	5308	RegOpenKey	HKLM\Software\Microsoft\Input\Settings	SUCCESS	Desired Access: Read

You may observe that only one Registry Key has both **RegCreateKey** and **RegSetValue**. This key is related to a persistence technique called **Registry Run Key Modification** and is commonly used by malware developers to install a backdoor. See screenshot Below:



Time ...	Process Name	PID	Operation	Path	Result	Detail
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegCreateKey	[redacted]	[redacted]	[redacted]
7:52:0...	mysterygift.exe	3236	RegSetValue	[redacted]	[redacted]	[redacted]

----

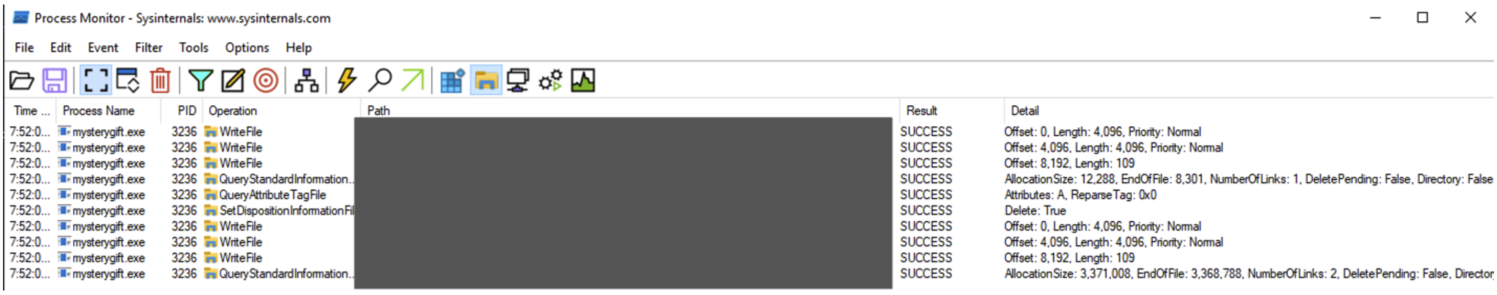
2. File Modification

Now, let's also determine if the malware sample executes File Creations. It may indicate that the malware drops prerequisite files for its successful execution.

Unclick all filters and choose the second filter - **Show File System Activity**. Again, the results are still numerous so let's add extra filters by focusing only on **File Write** events. Remove the following Operations again by right-clicking an entry from the Operation column and choosing **Exclude '<operation (e.g. CreateFile)>'**:

- CreateFile
- CreateFileMapping
- QuerySecurityFile
- QueryNameInformationFile
- QueryBasicInformationFile
- CloseFile
- ReadFile

The view from ProcMon should yield fewer results, similar to the image below:



Time ...	Process Name	PID	Operation	Path	Result	Detail
7:52:0...	mysterygift.exe	3236	WriteFile	[redacted]	SUCCESS	Offset: 0, Length: 4,096, Priority: Normal
7:52:0...	mysterygift.exe	3236	WriteFile	[redacted]	SUCCESS	Offset: 4,096, Length: 4,096, Priority: Normal
7:52:0...	mysterygift.exe	3236	WriteFile	[redacted]	SUCCESS	Offset: 8,192, Length: 109
7:52:0...	mysterygift.exe	3236	QueryStandardInformation...	[redacted]	SUCCESS	AllocationSize: 12,288, EndOfFile: 8,301, NumberOfLinks: 1, DeletePending: False, Directory: False
7:52:0...	mysterygift.exe	3236	QueryAttributeTagFile	[redacted]	SUCCESS	Attributes: A, ReparseTag: 0x0
7:52:0...	mysterygift.exe	3236	SetDispositionInformationFil	[redacted]	SUCCESS	Delete: True
7:52:0...	mysterygift.exe	3236	WriteFile	[redacted]	SUCCESS	Offset: 0, Length: 4,096, Priority: Normal
7:52:0...	mysterygift.exe	3236	WriteFile	[redacted]	SUCCESS	Offset: 4,096, Length: 4,096, Priority: Normal
7:52:0...	mysterygift.exe	3236	WriteFile	[redacted]	SUCCESS	Offset: 8,192, Length: 109
7:52:0...	mysterygift.exe	3236	QueryStandardInformation...	[redacted]	SUCCESS	AllocationSize: 3,371,008, EndOfFile: 3,368,788, NumberOfLinks: 2, DeletePending: False, Director

You may observe that two files are written under the **C:\Users\Administrator** directory. The first file is located in the user's **TEMP** directory, which is commonly used by malware to drop another file for its disposal. The other file is written in the **STARTUP** directory, also used for persistence via **Startup Folders**.

----

3. Network Connections

Lastly, let's confirm if the malware sample attempts to make a network connection. It may indicate that the malware communicates with external resources to download or establish remote access.

Unclick all filters and choose the third filter - **Show Network Activity**. Unlike the previous filters, the results are few and can be easily interpreted.

Please take note of domains or IP's requested by the malware, as we can use this information to investigate the rabbit hole further.
