# List of Sysmon Event IDs for Threat Hunting

## Features of Sysmon:

Sysmon monitors the following activities in a windows environment:

- ✓ Process creation (with full command line and hashes)
- ✓ Process termination
- ✓ Network connections
- ✓ File creation timestamps changes
- ✓ Driver/image loading
- ✓ Create remote threads
- ✓ Raw disk access
- ✓ Process memory access

## List of Sysmon Event IDs:

### Event ID 1: Process creation

The process creation event provides extended information about a newly created process. The full command line provides context on the process execution. The ProcessGUID field is a unique value for this process across a domain to make event correlation easier. The hash is a full hash of the file with the algorithms in the HashType field.

### Event ID 2: A process changed a file creation time

The change file creation time event is registered when a file creation time is explicitly modified by a process. This event helps tracking the real creation time of a file. Attackers may change the file creation time of a backdoor to make it look like it was installed with the operating system. Note that many processes legitimately change the creation time of a file; it does not necessarily indicate malicious activity.

### Event ID 3: Network connection

The network connection event logs TCP/UDP connections on the machine. It is disabled by default. Each connection is linked to a process through the ProcessId and ProcessGUID fields. The event also contains the source and destination host names IP addresses, port numbers and IPv6 status.

### Event ID 4: Sysmon service state changed

The service state change event reports the state of the Sysmon service (started or stopped).

### Event ID 5: Process terminated

The process terminates event reports when a process terminates. It provides the UtcTime, ProcessGuid and ProcessId of the process.

#### Event ID 6: Driver loaded

The driver loaded events provides information about a driver being loaded on the system. The configured hashes are provided as well as signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading.

#### Event ID 7: Image loaded

The image loaded event logs when a module is loaded in a specific process. This event is disabled by default and needs to be configured with the –l option. It indicates the process in which the module is loaded, hashes and signature information. The signature is created asynchronously for performance reasons and indicates if the file was removed after loading. This event should be configured carefully, as monitoring all image load events will generate a large number of events.

#### Event ID 8: CreateRemoteThread

The CreateRemoteThread event detects when a process creates a thread in another process. This technique is used by malware to inject code and hide in other processes. The event indicates the source and target process. It gives information on the code that will be run in the new thread: StartAddress, StartModule and StartFunction. Note that StartModule and StartFunction fields are inferred, they might be empty if the starting address is outside loaded modules or known exported functions.

#### Event ID 9: RawAccessRead

The RawAccessRead event detects when a process conducts reading operations from the drive using the `\\.\` denotation. This technique is often used by malware for data exfiltration of files that are locked for reading, as well as to avoid file access auditing tools. The event indicates the source process and target device.

#### Event ID 10: ProcessAccess

The process accessed event reports when a process opens another process, an operation that's often followed by information queries or reading and writing the address space of the target process. This enables detection of hacking tools that read the memory contents of processes like Local Security Authority (Lsass.exe) in order to steal credentials for use in Pass-the-Hash attacks. Enabling it can generate significant amounts of logging if there are diagnostic utilities active that repeatedly open processes to query their state, so it generally should only be done so with filters that remove expected accesses.

#### Event ID 11: FileCreate

File create operations are logged when a file is created or overwritten. This event is useful for monitoring autostart locations, like the Startup folder, as well as temporary and download directories, which are common places malware drops during initial infection.

### Event ID 12: RegistryEvent (Object create and delete)

Registry key and value create and delete operations map to this event type, which can be useful for monitoring for changes to Registry autostart locations, or specific malware registry modifications.

Sysmon uses abbreviated versions of Registry root key names, with the following mappings:

EVENT ID 12: REGISTRYEVENT (OBJECT CREATE AND DELETE)Key nameAbbreviation`HKEY_LOCAL_MACHINEHKLMHKEY_USERSHKUHKEY_LOCAL_MACHINE\System\ControlSet00xHKLM\System\CurrentControlSetHKEY_LOCAL_MACHINE\ClassesHKCR`

### Event ID 13: RegistryEvent (Value Set)

This Registry event type identifies Registry value modifications. The event records the value written for Registry values of type DWORD and QWORD.

### Event ID 14: RegistryEvent (Key and Value Rename)

Registry key and value rename operations map to this event type, recording the new name of the key or value that was renamed.

### Event ID 15: FileCreateStreamHash

This event logs when a named file stream is created, and it generates events that log the hash of the contents of the file to which the stream is assigned (the unnamed stream), as well as the contents of the named stream. There are malware variants that drop their executables or configuration settings via browser downloads, and this event is aimed at capturing that based on the browser attaching a `Zone.Identifier` "mark of the web" stream.

### Event ID 16: ServiceConfigurationChange

This event logs changes in the Sysmon configuration — for example when the filtering rules are updated.

### Event ID 17: PipeEvent (Pipe Created)

This event generates when a named pipe is created. Malware often uses named pipes for interprocess communication.

### Event ID 18: PipeEvent (Pipe Connected)

This event logs when a named pipe connection is made between a client and a server.

### Event ID 19: WmiEvent (WmiEventFilter activity detected)

When a WMI event filter is registered, which is a method used by malware to execute, this event logs the WMI namespace, filter name and filter expression.

#### Event ID 20: WmiEvent (WmiEventConsumer activity detected)

This event logs the registration of WMI consumers, recording the consumer name, log, and destination.

#### Event ID 21: WmiEvent (WmiEventConsumerToFilter activity detected)

When a consumer binds to a filter, this event logs the consumer name and filter path.

#### Event ID 22: DNSEvent (DNS query)

This event is generated when a process executes a DNS query, whether the result is successful or fails, cached or not. The telemetry for this event was added for Windows 8.1 so it is not available on Windows 7 and earlier.

#### Event ID 23: FileDelete (File Delete archived)

A file was deleted. Additionally to logging the event, the deleted file is also saved in the `ArchiveDirectory` (which is `C:\Sysmon` by default). Under normal operating conditions this directory might grow to an unreasonable size - see event ID 26: `FileDeleteDetected` for similar behavior but without saving the deleted files.

#### Event ID 24: ClipboardChange (New content in the clipboard)

This event is generated when the system clipboard contents change.

#### Event ID 25: ProcessTampering (Process image change)

This event is generated when process hiding techniques such as “hollow” or “herpaderp” are being detected.

#### Event ID 255: Error

This event is generated when an error occurred within Sysmon. They can happen if the system is under heavy load and certain tasked could not be performed or a bug exists in the Sysmon service.

## References:


https://docs.microsoft.com/en-us/sysinternals/downloads/sysmon

https://github.com/mrezagerami