Event IDs

> Randy Franklin Smith's Ultimate Windows Security
>
> Welcome to my February Patch Tuesday. Today Microsoft released updates for 73 vulnerabilities and an additional 33 updates since the previous Patch Tuesday for a total of 106 updates this month. Of these we have two zero-days to highlight first.
>
> https://www.ultimatewindowssecurity.com/

Event ID 4907, which signifies an audit policy change.

Windows System Logs:

- Event ID 1074 `(System Shutdown/Restart)`: This event log indicates when and why the system was shut down or restarted. By monitoring these events, you can determine if there are unexpected shutdowns or restarts, potentially revealing malicious activity such as malware infection or unauthorized user access.
- Event ID 6005 `(The Event log service was started)`: This event log marks the time when the Event Log Service was started. This is an important record, as it can signify a system boot-up, providing a starting point for investigating system performance or potential security incidents around that period. It can also be used to detect unauthorized system reboots.

- Event ID 6006 `(The Event log service was stopped)`: This event log signifies the moment when the Event Log Service was stopped. It is typically seen when the system is shutting down. Abnormal or unexpected occurrences of this event could point to intentional service disruption for covering illicit activities.
- Event ID 6013 `(Windows uptime)`: This event occurs once a day and shows the uptime of the system in seconds. A shorter than expected uptime could mean the system has been rebooted, which could signify a potential intrusion or unauthorized activities on the system.
- Event ID 7040 `(Service status change)`: This event indicates a change in service startup type, which could be from manual to automatic or vice versa. If a crucial service's startup type is changed, it could be a sign of system tampering.

1. **Windows Security Logs**
    - Event ID 1102 `(The audit log was cleared)`: Clearing the audit log is often a sign of an attempt to remove evidence of an intrusion or malicious activity.
    - Event ID 1116 `(Antivirus malware detection)`: This event is particularly important because it logs when Defender detects a malware. A surge in these events could indicate a targeted attack or widespread malware infection.
    - Event ID 1118 `(Antivirus remediation activity has started)`: This event signifies that Defender has begun the process of removing or quarantining detected malware. It's important to monitor these events to ensure that remediation activities are successful.
    - Event ID 1119 `(Antivirus remediation activity has succeeded)`: This event signifies that the remediation process for detected malware has been successful. Regular monitoring of these events will help ensure that identified threats are effectively neutralized.
    - Event ID 1120 `(Antivirus remediation activity has failed)`: This event is the counterpart to 1119 and indicates that the remediation process has failed. These events should be closely monitored and addressed immediately to ensure threats are effectively neutralized.

- Event ID 4624 `(Successful Logon)`: This event records successful logon events. This information is vital for establishing normal user behavior. Abnormal behavior, such as logon attempts at odd hours or from different locations, could signify a potential security threat.
- Event ID 4625 `(Failed Logon)`: This event logs failed logon attempts. Multiple failed logon attempts could signify a brute-force attack in progress.
- Event ID 4648 `(A logon was attempted using explicit credentials)`: This event is triggered when a user logs on with explicit credentials to run a program. Anomalies in these logon events could indicate lateral movement within a network, which is a common technique used by attackers.
- Event ID 4656 `(A handle to an object was requested)`: This event is triggered when a handle to an object (like a file, registry key, or process) is requested. This can be a useful event for detecting attempts to access sensitive resources.
- Event ID 4672 `(Special Privileges Assigned to a New Logon)`: This event is logged whenever an account logs on with super user privileges. Tracking these events helps to ensure that super user privileges are not being abused or used maliciously.
- Event ID 4698 `(A scheduled task was created)`: This event is triggered when a scheduled task is created. Monitoring this event can help you detect persistence mechanisms, as attackers often use scheduled tasks to maintain access and run malicious code.
- Event ID 4700 & Event ID 4701 `(A scheduled task was enabled/disabled)`: This records the enabling or disabling of a scheduled task. Scheduled tasks are often manipulated by attackers for persistence or to run malicious code, thus these logs can provide valuable insight into suspicious activities.
- Event ID 4702 `(A scheduled task was updated)`: Similar to 4698, this event is triggered when a scheduled task is updated. Monitoring these updates can help detect changes that may signify malicious intent.
- Event ID 4719 `(System audit policy was changed)`: This event records changes to the audit policy on a computer. It could be a sign that someone is trying

to cover their tracks by turning off auditing or changing what events get audited.

- Event ID 4738 `(A user account was changed)`: This event records any changes made to user accounts, including changes to privileges, group memberships, and account settings. Unexpected account changes can be a sign of account takeover or insider threats.
- Event ID 4771 `(Kerberos pre-authentication failed)`: This event is similar to 4625 (failed logon) but specifically for Kerberos authentication. An unusual amount of these logs could indicate an attacker attempting to brute force your Kerberos service.
- Event ID 4776 `(The domain controller attempted to validate the credentials for an account)`: This event helps track both successful and failed attempts at credential validation by the domain controller. Multiple failures could suggest a brute-force attack.
- Event ID 5001 `(Antivirus real-time protection configuration has changed)`: This event indicates that the real-time protection settings of Defender have been modified. Unauthorized changes could indicate an attempt to disable or undermine the functionality of Defender.
- Event ID 5140 `(A network share object was accessed)`: This event is logged whenever a network share is accessed. This can be critical in identifying unauthorized access to network shares.
- Event ID 5142 `(A network share object was added)`: This event signifies the creation of a new network share. Unauthorized network shares could be used to exfiltrate data or spread malware across a network.
- Event ID 5145 `(A network share object was checked to see whether client can be granted desired access)`: This event indicates that someone attempted to access a network share. Frequent checks of this sort might indicate a user or a malware trying to map out the network shares for future exploits.
- Event ID 5157 `(The Windows Filtering Platform has blocked a connection)`: This is logged when the Windows Filtering Platform blocks a connection attempt. This can be helpful for identifying malicious traffic on your network.

- Event ID 7045 `(A service was installed in the system)`: A sudden appearance of unknown services might suggest malware installation, as many types of malware install themselves as services.

Events

On Vista and higher, events are stored in `Applications and Services Logs/Microsoft/Windows/Sysmon/Operational`, and on older systems events are written to the `System` event log. Event timestamps are in UTC standard time.

The following are examples of each event type that Sysmon generates.

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 terminate 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 significant amount of logging.

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:

Expand table

Key name	Abbreviation
`HKEY_LOCAL_MACHINE`	`HKLM`
`HKEY_USERS`	`HKU`
`HKEY_LOCAL_MACHINE\System\ControlSet00x`	`HKLM\System\CurrentControlSet`
`HKEY_LOCAL_MACHINE\Classes`	`HKCR`

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 26: FileDeleteDetected (File Delete logged)

A file was deleted.

Event ID 27: FileBlockExecutable

This event is generated when Sysmon detects and blocks the creation of executable files (PE format).

Event ID 28: FileBlockShredding

This event is generated when Sysmon detects and blocks file shredding from tools such as SDelete.

Event ID 29: FileExecutableDetected

This event is generated when Sysmon detects the creation of a new executable file (PE format).

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 tasks could not be performed or a bug exists in the Sysmon service, or even if certain security and integrity conditions are not met

DLL DETECT WITH SYSMON:

To detect a DLL hijack, we need to focus on `Event Type 7`, which corresponds to module load events.

Let's explore these IOCs:

1. "calc.exe", originally located in System32, should not be found in a writable directory. Therefore, a copy of "calc.exe" in a writable directory serves as an IOC, as it should always reside in System32 or potentially Syswow64.
2. "WININET.dll", originally located in System32, should not be loaded outside of System32 by calc.exe. If instances of "WININET.dll" loading occur outside of System32 with "calc.exe" as the parent process, it indicates a DLL hijack within calc.exe. While caution is necessary when alerting on all instances of "WININET.dll" loading outside of System32 (as some applications may package specific DLL versions for stability), in the case of "calc.exe", we can confidently assert a hijack due to the DLL's unchanging name, which attackers cannot modify to evade detection.
3. The original "WININET.dll" is Microsoft-signed, while our injected DLL remains unsigned.

These three powerful IOCs provide an effective means of detecting a DLL hijack involving calc.exe. It's important to note that while Sysmon and event logs offer valuable telemetry for hunting and creating alert rules, they are not the sole sources of information.

- **Event ID 1:** Process Creation - Tracks when a process is started, including the command line that initiated the process. This is critical for identifying malicious processes or commands used by attackers.
- **Event ID 3:** Network Connection - Monitors attempts to connect to a remote host, which can be pivotal in detecting data exfiltration attempts or command and control (C&C) communication.
- **Event ID 7:** Image Loaded - Logs when a DLL is loaded into a process, which is useful for detecting the use of malicious payloads or code injection techniques.
- ***Event ID 22*** *is for DNSQuery*