

# Registry keys Deleted (Apparently)

- HKLM\System\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational{5770385f-c22a-43e0-bf4c-06f5698ffbd9}
- HKLM\System\CurrentControlSet\Control\WMI\Security\08dd09cd-9050-5a49-02f8-46fd443360a8
- HKLM\System\CurrentControlSet\Control\WMI\Autologger\EventLog-Microsoft-Windows-Sysmon-Operational
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Channels\Microsoft-Windows-Sysmon/Operational
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers{5770385f-c22a-43e0-bf4c-06f5698ffbd9}\ChannelReferences\0
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers{5770385f-c22a-43e0-bf4c-06f5698ffbd9}\ChannelReferences
- HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers{5770385f-c22a-43e0-bf4c-06f5698ffbd9}

# Access Right/Mask

DELETE 0x10000, %%1537 The right to delete the object.

# Enabling Registry Audit

auditpol.exe /set /subcategory:"Registry" /success:enable /failure:enable

# Creating Audit Rule (SACL) - Proof of Concept for one Key

```
git clone https://github.com/OTRF/Set-AuditRule
cd Set-AuditRule/
import-module Set-AuditRule.ps1
Set-AuditRule -RegistryPath 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\WINEVT\Publishers\{5770385f-c22a-43
```

# Monitor

## Windows Security Auditing Channel

Windows Security 4657 (Modification of Registry) Windows Security 4663 (Attempt was made to access an object) (Type: Key) ( TaskCategory: Registry) Windows Security 4660 (An object Was Deleted) (TaskCategory: Registry)

# SIGMA

```
title: Sysmon Channel Reference Deletion
id: 18beca67-ab3e-4ee3-ba7a-a46ca8d7d0cc
```

```
status: experimental
description: Potential threat actor tampering with Sysmon manifest and eventually disabling it
references:
  - https://twitter.com/Flangvik/status/1283054508084473861
  - https://twitter.com/SecurityJosh/status/1283027365770276866
  - https://securityjosh.github.io/2020/04/23/Mute-Sysmon.html
author: Roberto Rodriguez (Cyb3rWard0g), OTR (Open Threat Research)
date: 2020/07/14
tags:
    - attack.defense_evasion
    - attack.t1112
logsource:
    product: windows
    service: security
detection:
    selection1:
        EventID: 4657
        ObjectName|contains:
            - 'WINEVT\Publishers\{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'
            - 'WINEVT\Channels\Microsoft-Windows-Sysmon/Operational'
        ObjectValueName: 'Enabled'
        NewValue: '0'
    selection2:
        EventID: 4663
        ObjectName|contains:
            - 'WINEVT\Publishers\{5770385f-c22a-43e0-bf4c-06f5698ffbd9}'
            - 'WINEVT\Channels\Microsoft-Windows-Sysmon/Operational'
        AccessMask: 0x10000
    condition: selection1 or selection 2
falsepositives:
    - unknown
level: critical
```