**Security** Event IDs of Interest

**youtube.com/13cubed**

****

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **4624** | An account was successfully logged on. (**See Logon Type Codes**) |
| **4625** | An account failed to log on. |
| **4634** | An account was logged off. |
| **4647** | User initiated logoff. (In place of 4634 for Interactive and RemoteInteractive logons) |
| **4648** | A logon was attempted using explicit credentials. (RunAs) |
| **4672** | Special privileges assigned to new logon. (Admin login) |
| **4776** | The domain controller attempted to validate the credentials for an account. (DC) |
| **4768** | A Kerberos authentication ticket (TGT) was requested. |
| **4769** | A Kerberos service ticket was requested. |
| **4771** | Kerberos pre-authentication failed. |
| **4720** | A user account was created. |
| **4722** | A user account was enabled. |
| **4688** | A new process has been created. (If audited; some Windows processes logged by default) |
| **4698** | A scheduled task was created. (If audited) |
| **4798** | A user's local group membership was enumerated. |
| **4799** | A security-enabled local group membership was enumerated. |
| **5140** | A network share object was accessed. |
| **5145** | A network share object was checked to see whether client can be granted desired access. |
| **1102** | The audit log was cleared. (Security) |

# Logon Type Codes

**youtube.com/13cubed**

****

|  |  |
| --- | --- |
| **Type** | **Description** |
| **2** | Console |
| **3** | Network |
| **4** | Batch (Scheduled Tasks) |
| **5** | Windows Services |
| **7** | Screen Lock/Unlock |
| **8** | Network (Cleartext Logon) |
| **9** | Alternate Credentials Specified (RunAs) |
| **10** | Remote Interactive (RDP) |
| **11** | Cached Credentials (e.g., Offline DC) |
| **12** | Cached Remote Interactive (RDP, similar to Type 10) |
| **13** | Cached Unlock (Similar to Type 7) |

**System** Event IDs of Interest

**youtube.com/13cubed**

****

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **7045** | A new service was installed in the system. (4697 in Security) |
| **7034** | The *x* service terminated unexpectedly. It has done this *y* time(s). |
| **7009** | A timeout was reached (*x* milliseconds) while waiting for the *y* service to connect. |
| **104** | The *x* log file was cleared. (**Will show System, Application, and other logs cleared**) |

**Application** Event IDs of Interest

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **\*1000** | Application Error |
| **\*1002** | Application Hang |

\*Remember, third-party software (like Antivirus) can also write to this log!

**Application (ESENT Provider)** Event IDs of Interest

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **216** | A database location change was detected. |
| **325** | The database engine created a new database. |
| **326** | The database engine attached a database. |
| **327** | The database engine detached a database. |

**Windows-PowerShell** Event IDs of Interest

**youtube.com/13cubed**

****

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **400** | Engine state is changed from None to Available. |
| **600** | Provider "*x*" is Started. |

**Microsoft-Windows-PowerShell/Operational** Event IDs of Interest

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **\*4104** | 4104, Creating Scriptblock text (1 of 1): (Scriptblock Logging) |

\*Enabled by default in PowerShell v5 and later for scripts identified as potentially malicious, logged as warnings

**Microsoft-Windows-TaskScheduler/Operational** Event IDs of Interest

**youtube.com/13cubed**

****

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **106** | The user *x* registered the Task Scheduler task *y*. (New Scheduled Task) |
| **141** | User *x* deleted Task Scheduler task *y*. |
| **100** | Task Scheduler started the *x* instance of the *y* task for user *z*. |
| **102** | Task Scheduler successfully finished the *x* instance of the *y* task for user *z*. |

**Microsoft-Windows-Windows Defender/Operational** Event IDs of Interest

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **1116** | The antimalware platform detected malware or other potentially unwanted software. |
| **1117** | The antimalware platform performed an action to protect your system from malware or other potentially unwanted software. |

# Microsoft-Windows-TerminalServicesLocalSessionManager/Operational

Event IDs of Interest

**youtube.com/13cubed**

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **21** | Remote Desktop Services: Session logon succeeded: |
| **22** | Remote Desktop Services: Shell start notification received: |
| **23** | Remote Desktop Services: Session logoff succeeded: |
| **24** | Remote Desktop Services: Session has been disconnected: |
| **25** | Remote Desktop Services: Session reconnection succeeded: |

**Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational** Event IDs of Interest

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **\*1149** | Remote Desktop Services: User authentication succeeded: |

\*This is BEFORE user authentication and does NOT indicate successful authentication; only a successful NETWORK connection

**Microsoft-Windows-TerminalServices-RDPClient/Operational** Event IDs of Interest

|  |  |
| --- | --- |
| **Event ID** | **Description** |
| **\*1029** | Base64(SHA256(UserName)) is = *HASH* |

\*Created on the computer INITIATING the connection (i.e., the SOURCE); contains a HASH of the username used



**Version 1.1**

**See the 13Cubed** [**RDP Event Log Forensics**](https://www.13cubed.com/downloads/rdp_flowchart.pdf) **flowchart for additional details.**